PROCEEDINGS OF THE AFRICAN CYBER CITIZENSHIP CONFERENCE 2015 (ACCC2015)

2-3 November 2015
Port Elizabeth
South Africa

Editor:

J.F. Van Niekerk

Publisher:
Nelson Mandela Metropolitan University
PO Box 77000
Port Elizabeth
6031

Proceedings published at
http://accconference.nmmu.ac.za

ISBN: 978-1-920508-67-8

TO WHOM IT MAY CONCERN

The full papers for the African Cyber Citizenship Conference 2015 were refereed by a double-blind reviewing process according to South Africa's Department of Higher Education and Training (DHET) refereeing standards. Before accepting a paper, authors were to include the corrections as stated by the peer reviewers. Of the 36 full papers received, 14 were accepted for the Proceedings (acceptance rate: 39%).

Papers were reviewed according to the following criteria:

- Relevancy of the paper to the Cyber-based theme
- Originality and Innovativeness of the research
- Quality of Academic writing and Argument
- Appropriateness and Quality of Literature sources used

The program committee reflected the inter-disciplinary nature of the conference and consisted of international experts in the fields of Information Technology, Law, Psychology, Management, and Education.

Prof. Johan van Niekerk
The Program Chair: ACCC2015

School of ICT
Nelson Mandela Metropolitan University
South Africa
Port Elizabeth

Cell: +27 76 251 7684
Tel: +27 41 504 3048
Email: johan.vanniekerk@nmmu.ac.za

Program Committee ACCC 2015

Johan van Niekerk	johanvn@nmmu.ac.za	Nelson Mandela Metropolitan University
Karen Renaud	karen.renaud@glasgow.ac.uk	University of Glasgow
Steven Furnell	sfurnell@plymouth.ac.uk	Plymouth University
Anne Karen Seip	annikken@online.no	Finanstilsynet
Elmarie Kritzinger	kritze@unisa.ac.za	UNISA
Nathan Clarke	nclarke@plymouth.ac.uk	Plymouth University
Frans Marx	Frans.Marx@nmmu.ac.za	NMMU
Pedro Veiga	pmveiga@fc.ul.pt	University of Lisbon
Marijke Coetzee	marijkec@uj.ac.za	University of Johannesburg
Liezel Cilliers	liezelcilliers@yahoo.com	Department of Health
Matt Bishop	mabishop@ucdavis.edu	University of California at Davis
Carlos Rieder	carlos.rieder@isec.ch	isec ag
Miroslava Cernochova	miroslava.cernochova@pedf.cuni.cz	Charles University in Prague, Faculty of Education
Christoph Kreitz	kreitz@cs.uni-potsdam.de	Cornell University / University of Potsdam
Adele Da Veiga	dveiga@unisa.ac.za	Unisa
Kerry-Lynn Thomson	Kerry-Lynn.Thomson@nmmu.ac.za	Nelson Mandela Metropolitan University
Nader Sohrabi Safa	Nader.SohrabiSafa@nmmu.ac.za	Nelson Mandela Metropolitan University
Lynn Futcher	lynn.futcher@nmmu.ac.za	Nelson Mandela Metropolitan University
Reinhardt Botha	ReinhardtA.Botha@nmmu.ac.za	Nelson Mandela Metropolitan University

Table of Contents – Peer reviewed papers

Proceedings of the African Cyber Citizenship Conference 2015
Port Elizabeth, 2-3 November 2015 (http://accconference.nmmu.ac.za)
ISBN: 978-1-920508-67-8

The interplay of cyberspaces, sympathy and self-creation: Bullying as an ideology of anti-compassion

Belinda Du Plooy
Nelson Mandela Metropolitan University
belinda.duplooy@nmmu.ac.za

Abstract

Electronic/cyberspaces undeniably have previously inconceivable practical and immediate use-value, but also carry with them great ironies and paradoxes that have become indistinguishable parts of contemporary postmodern and posthuman self- and community management. It also provides new mediums through which ideology can be manifested and challenged. Cyberspace provides previously unprecedented arenas for the creation and expression of the self, on the one hand, and intersubjectivity and the extension of the self to others, on the other hand, with the ensuing dangers. Cyberspace provides a new self-perpetuating, immediate and constantly innovating playing field for old games - new ways of doing very old things, as Badenhorst (2011) astutely notes. This paper serves as an initial and introductory conceptual exploration for points of metatextual and metadiscursive convergence, aiming for a dialectical and dialogical engagement with, specifically, the concepts of ideology, cyberspace, sympathy/compassion, self-creation and bullying in contemporary human (often technologically mediated) experiences.

Keywords

cyberspace, bullying, compassion, sympathy, individualism, humanitarianism, ideology, anti-compassion

1. Introduction

Ronald Barnett (1998, 2000a, 2000b, 2000c) accurately describes contemporary human existence as “supercomplex”, with technology contributing greatly to these expanding complexities. It is an indisputable fact that contemporary communication technology has changed human existence in an extremely short span of time. At the controversial forefront of this change today is the internet, social networking, virtual gaming and various real-time instant-messaging applications and sites. Despite the very recent advent of these forms of communication and the extensive public and scholarly critiques around security, safety and the potential vulnerability of the users of these techno-medias, the active engagement within these spaces seem to flourish and expand daily. Electronic/cyberspaces undeniably have previously inconceivable practical and immediate use-value, but also carry with them great ironies and paradoxes that have become indistinguishable parts of contemporary postmodern and posthuman (Braidotti, 2013) self- and community management. Sherry Turkle’s book title Alone Together (2011) maybe best describes the ironic paradox of human techno-mediated existence. Consequently, technology and cyberspaces also provide new mediums through which various ideologies and counter-ideologies can be manifested and challenged.

Cyberspace provides previously unprecedented arenas for the creation and expression of the self, on the one hand, and intersubjectivity and the extension of the self to others, on the other hand, with the ensuing dangers. Concepts such as virtual communities, networked space and cyberprofiling have migrated to common daily experience for many people, with extension to both affective sides of the positive/negative spectrum. We are cautioned to be cybersmart, cybersecure and responsible cybercitizens. Indeed, cyberspace creates liminal spaces of new types of civic (and civil – consider, for example, the neologism ‘nettiquette’) engagement, quite literally thresholds or portals between people, environments and experiences where polar categories such as in/out, us/them, self/other, real/virtual, good/bad and right/wrong and historical, cultural and political ‘big truths’ (or ideologies) are constantly, if often unintentionally and even violently, renegotiated and interrogated by the users of these technologies. This, of course, in itself is not new, but cyberspace provides a new self-perpetuating, immediate and constantly innovating playing field for old games - new ways of doing very old things, as Charmain Badenhorst (2011) astutely notes.

However, at the heart of human existence (irrespective of its complexities and how these are mediated) is still the basic concept of human interpersonal engagement or interaction, as articulated in Roman Jakobson’s (1995) original semiotic communication model: the sharing or sending of information and experience, through contexts, codes and channels, for whatever range of purposes, by one person with or to another/others and the return exchange of related information or experience. John Caputo (1993:252) expresses this contemporary “hermeneutical anxiety” - the perennial existential human questions about being oneself with others in meaningful ways - when he asks: “[W]ho are we now, at this particular moment of our historical continuum ... Who are we high-tech, late capitalist, mobile, post-Enlightenment ...

postmodernists? And how can we be otherwise?”.

It is in this interrogation of our possibilities for “being otherwise” that Caputo’s work resonates with critiques of power and ideology, particularly from theorist from/of psychology, psychoanalysis and social psychology. This paper serves as an initial and introductory conceptual exploration for points of metatextual and metadiscursive convergence, aiming for a dialectical and dialogical engagement with, specifically, the concepts of ideology, cyberspace, sympathy/compassion, self-creation and bullying in contemporary human (often technologically mediated) experiences. The discourses mentioned in this paper are not posited as the only resonant emerging and converging strands of thought on these topics and the paper aims to invite the continued conversation, with more and different iterations on the themes introduced here.

2. Cyberbullying

The golden thread of mutual relevance, for the purpose of this paper, that connects the discourses mentioned here is the concept of bullying, its prevalence in cyberspace and how it constructs itself at the nexus of converging ideologies and cultural structures around individualism and altruism, humanitarianism and egoism, self-construction and communalism. For the purpose of this paper I subscribe to a broad definition of cyberbullying as a form of abusive behavior, perpetrated by one or more persons through electronic means or mediation on one or more other persons who feel that they cannot defend themselves, often with the support of bystanders who may or may not actively participate in the abusive action, often resulting in what can be called mobbing (Leymann, 1990). I furthermore think of cyberbullying (like other more traditional forms of bullying) as a discursive form of anti-compassion, in opposition to the recent reemergence of a popular focus on compassion discourses (Armstrong, 2008, 2009, 2011; Lampert, 2011), coinciding with what is now called the 'affective turn' of the mid-twentieth century: the popular and scholarly prioritizing and legitimizing of social, cultural and interpersonal politics, and the concomitant ideological constructedness and responsiveness, of human emotions and feelings (Athanasiou, Hantzaroula & Yannakopolos, 2008; Clough, 2008; Clough & Halley, 2007; La Caze & Lloyd, 2011). (Other recent examples of anti-compassion, which fall outside of the scope of this specific paper, would be the rise in fundamentalist violence and pornography, both greatly enabled by cybertechnologies.)

Cyberbullying is often associated with abuse-related terminologies, such as defamation, harassment, discrimination, offensive, vulgar, derogatory and aggressive behavior (Burton & Mutongwize, 2009; Belsey, 2005; Willard, 2003). The bully, in all spaces and forms, succeeds in her/his intent to harm another by two means: controlling the narrative and creating a hostile environment. It is clear how cyberspace potentially enables these type of actions, due to its immediacy, lack of screening and security, anonymity, reliance on trust and communal non-personal activity (what can become mobbing, a form of psychological terror (Leymann, 1990)). But bullying is most often not controlled by legislation or policies, though this is changing, as the world adapts to the new challenges created by technology. Because of its general accessibility – for example, according to Fine (2008:11) 99% of South Africans have access to mobile communication - cyberbullying is reported to constitute "a quarter to a third of traditional bullying" (Burton & Mutongwizo, 2009) and can take a variety of forms, such as online fights or 'flaming', impersonation or identity theft, 'outing' of secrets, gossip and relational violence, ostracism, stalking, sexting and the unobtrusive recording and then publicly sharing of recorded information ('happy slapping' is popular among children; with the repeated sharing of images aptly called 'going viral') (Burton & Mutongwize, 2009).

One of the common fault lines of bullying and anti-bullying theory and practices alike is the assumption that it is 'child-like' or 'childish' behavior and it is often wrongly relegated to the school playground with patronizing and dismissive attitudes of 'mere horse-play'. The increasingly recognized escalating epidemic of workplace bullying (Namie & Namie, 2000, 2011; Babiak & Hare, 2006) and the serious consequences to health and life demand more sophisticated interpretations of bullying, both among children and adults.

Within these dynamics cyberspace is increasingly emerging as the very serious metaphorical 'playground', for adults and children alike, where the highly complex socio-political dynamics of bullying are enacted. Cyberbullying is a particularly malignant form of abuse because it is easily accessible, often anonymous, carries few if any consequences or punitive results, entails no interpersonal contact and thus little or no reading of physical social cues, actively enables actions of disinhibition, dehumanization and public humiliation (Burton & Mutongwize, 2009; Limber, 2009) and is virally cumulative in nature: due to its accessibility and visibility not only the specific targets are victimized, but by implication secondary victimization and traumatization happen whenever one person witnesses the victimization of another and knows 'it could have been me'. Consequently, the United States Centre for Disease Control indicates a 50% increase in internet users reporting online victimization in the five years from 2000 to 2005 (Burton & Mutongwize, 2009; Hertz & David-Ferdon, 2008). Of particular importance is the fact that online bullying, with its relational and anonymous aspects, is seen as an increasing problem in girls and women as abusers, while a correlating relationship has been found to exist "between those who experience cyberaggression and those who perpetrate it" (Burton & Mutongwize, 2009), proving how the lines between previously distinct categories (abusers and victims) have become blurred with the potentialities of relational, automatic, immediate, anonymous and adaptable initiation and retaliation of cyberviolence.

3. Ideology and cyberspace

Psychoanalytic philosopher Slavoj Žižek, in the 2012 film The Pervert's Guide to Ideology (Fiennes, 2012) says "when we think we escape ideology in our dreams; that is when we are in ideology" [my emphasis]. Cyberspace is possibly the most complex example of postmodern and posthuman ideological dream worlds, as it creates imaginary and virtual landscapes previously unimaginable to us. As Žižek (Fiennes, 2012) explains, “fantasies are the central things our ideologies are made of”, in particular “the fantasy of myself as desired by others”. In cyberspace self-creation becomes a possibility in ways that are impossible anywhere else. But it is a two-sided sword of both subjectivation (creation of the self as subject, in Foucaultian terms, through technologies of the self) and subjection (of the self to the scrutiny, opinion and governance of/by others through discursive apparatuses) – even subjugation, if the opinions and gazes of the scrutinizing others become the exclusive means through which the self is constructed. It also creates others of varying forms, as all ideological tools are wont to do. The latter two (subjugation and othering) are part of the danger associated with cyberbullying, when the influence of governing forces of the other on the self, or the self on the other, become uncontrolled and uncontrollable, and, most dangerously, uncritically internalized.

Žižek (Fiennes, 2012) explains ideology as glasses that we put on that distort our view and in order to see our ideologies for what they are (discursive constructs instead of essential or monolithic ‘truths’), we have to take off the glasses through critical engagement with our ideologies. For Michel Foucault this would mean the skeptical freedom (Rajchman, 1985:3-4) of “a doubting attitude [a]s a culturally available option” (Hammer, 2005:124); or what John Rollins calls “holding your beliefs lightly” (Crucified Identities, youtube.com). Cyberspace represents potentially both, at times, the glasses of ideology and the painful removal of the glasses, at other times. Some of the most prevalent interconnected ideological stands of cyberdiscourses today relate to the myths, fantasies and narratives (“free-floating elements that combine to form ideology” and that serve to “fixate imagination and mobilize us” (Žižek in Fiennes, 2012)) that are connected to social networks and communities, cyberactivism and social movements, the new millennial humanitarianism (and its deeply complex relationship with consumerism), self-construction and its relationship to the liberal ideals of freedom, autonomy and non-conformism, and social and interpersonal violence.

Cyberspace is an arena in which many old ideologies have been re-engineered and whole new ones have been created. It also enables, what Foucault calls, heterotopic experiences and spaces where individual and social crises and deviations are constructed and deconstructed (Foucault, 1984:4). These always necessarily imply resistance of some kind, even if merely imaginary, and are therefore politicized experiences and places where the dual aspects of repressive and productive power operate simultaneously. Foucault describes this as the “joint, mixed experience” (1984:4) of contemporary pluralistic existence: the “simultaneously mythic and real contestation of the space in which we live” (1984:4). This implies a constant, active and dynamic engagement with constructions and representations of the self and the other.

Foucault (1984:4) describes this mirror-like experience of “hetertopic anxiety” as follows: “I discover my absence from the place where I am since I see myself over there. Starting from this gaze that is, as it were, directed towards me, from the ground of this virtual space that is on the other side of the glass, I come back towards myself; I begin again to direct my eyes toward myself and to reconstitute myself where I am". Žižek also warns that "it hurts to step out of ideology [because] we enjoy our ideology" (as mentioned above, ideology is, after all, the playing field of our desires and pleasures, in the psychoanalytical sense) and he cautions that stepping out of ideology demands "opening the abyss of suspicion" (Fiennes, 2012). It would be redundant to elaborate here, and to this audience, on either the vulnerabilities created by cyberspace, its potential for empowerment, or the potential practical dangers inherent in the negotiating of vulnerabilities and empowerment. These dynamic interactions between discourses produce iterative sites of ideological power struggles and violence (sometimes virtual, sometimes real) and constantly interrogate "[the] relationship between what we do, what we are obliged to do, what we are allowed to do, what we are forbidden to do ... and what we are allowed, forbidden, or obliged to say" (Foucault, 1988a:8).

It is in this way that ideologies through discourse produce 'truths', but it is also through discourse that the constructed truths of ideologies can be resisted and dismantled. Thus Foucault, shortly before his death in

1984, defended his skeptical position as follows: "My point is not that everything is bad, but that everything is dangerous, which is not exactly the same as bad. If everything is dangerous, then we always have something to do. So my position leads not to apathy, but to a hyper- and pessimistic activism" (Foucault in Grimshaw, 1993:56). Considering that Foucault did not have any experience of cyberspace as we do today, his words seem eerily and ironically prophetic, when read in the context of the cybersecurity crises of today, ranging from the grooming of children by abusers, identity fraud and confidence scams, the leaking of (inter)national security information, the threat to personal privacy and the violence mediated via cyberspaces.

The ironic paradox of individualism and humanitarianism: neo-colonialism in globalized cyberspaces

As early as the 1830's Alexis De Tocqueville commented on the interplay between cultural forces - or ideologies, though he did not use this term - of individualism and humanitarianism in America. In his twovolume socio-political analysis of American society, Democracy in America (1835 and 1840), De Tocqueville depicted American democracy as unique and called it "exceptional", which gave rise to the term "American exceptionalism" that is still widely used to criticize American foreign policy. Since the American ideological paradigm has largely come to define the

Westernized imagination of contemporary time, the questions that De Tocqueville, and subsequent theorists on the topic, raise have implications that reach further than just the physical borders of the United States. Cyberspace, as the progeny of Silicone Valley, can therefore arguably be called a form of American neo-colonialism (which has transcended itself through what is commonly called globalization), constituting structures and systems within which one has to, and outside of which one increasingly cannot, negotiate the very mundane practices and minutiae of everyday life. De Tocqueville‘s analysis was an antecedent of the idea of American individualism, founded on the ideals of liberty, equality and a dual concern for the individual and the community, which would come to distinguish American social and political discourses. This kind of individualism is based on the values of non-conformism, freedom and individual autonomy as a basic right; competition and the related idea that hard work will be rewarded and will lead to success; and a definitive commitment to self-interest whether in the realm of financial success, material comforts, bodily pleasure or psychological and emotional wellbeing. (De Tocqueville warned that despotism and egotism were potential dangers of the New World democracy.) The American imagination is teeming with images of real and fictitious heroes and characters who embody these ideals, with the most recent being the entrepreneurs of Wall Street and Silicon Valley, such as Steve Jobs, Steve Wozniak, Bill Gates, Donald Trump and Richard Branson. (Though being English, Branson conforms entirely to the American ideal of a pioneering self-made man, which is a recurring theme in the American imagination.)

But paradoxically at the same time the historical American imagination is filled with the traditions and ideals of altruism and charity, to such an extent that co-operation, generosity, helpfulness and neighbourliness are likewise staples of American fictional and historical mythologies and narratives, such as those associated with Thanksgiving (with full acknowledgement of the politically-loaded historical context of colonial exploitation).

Robert Wuthnow‘s studies during the last decade of the twentieth century have shown that eighty million Americans do volunteer work of some kind to help others in ways that hold no benefit for themselves: 45% of American adults are involved in some kind of volunteer activities, with approximately twenty-billion hours of service being donated annually, and 73% of the American public feel that helping people in need is very important while 63% feel that giving one‘s time to do so was essential (Wuthnow, 1991:6-7). On the other hand there are hundreds of thousands of people who are not being cared for; the medical, educational, social service and penal systems are constantly being criticized for failing the public; and politicians on both sides of the party divide build election campaigns around promises of better social service and care. Wuthnow (1991:19-20) reports that 80% of Americans feel that self-interest and the lack of care for others is a serious problem and 63% of the respondents in his study felt that this is an increasing and continuing trend. Steve Salerno (2006:245) correctly says “American values, with their profound sympathy for the underdog, have always favoured victim assistance”, even if it only exists in the realm of the superficial.

Most significantly, Wuthnow recognizes that there has been a shift since the middle of the twentieth century in terms of the way people engage with the concept of compassion (coinciding, maybe coincidentally, with the explosion in communication technology). He traces this through the emphasis on political awareness and ideological revolution in the 1960s, through the “me-generation” of the 1970s, the “decade of greed” in the 1980s, and the “decade of freedom” in the 1990s (1991:18). Through these eras and into the hightech cyber/virtual twenty-first century, observers and critics of American culture have identified “both the resurgence of individualistic values and a redefinition of these values as dominant trends” (Wuthnow, 1991:18). This has happened to the extent that freedom “ceases to mean liberty in civil society and becomes a fetish” (Wuthnow, 1991:18). It would be redundant to elaborate on how this is manifested through contemporary mediums such as talk shows and reality television, Internet blogs, instant messaging applications and electronic social networks. However, similar arguments can be made for the contemporary fetishization and superficialization of traditional caring-ideals (for example, empathy, compassion, altruism, sympathy) and for what Chouliaraki (2012:1) calls the “theatricality of humanitarianism”: (particularly celebrity-based) humanitarianism as spectacle and as inauthentic aspirational discourse. The general consensus, as Wuthnow points out (1991:20), among critics and theorists is that individualism and altruism are antagonistic concepts and that helping others necessarily means sacrificing oneself: it is a case of me versus we. However, Wuthnow presents a different premise: he recognises the complexity and dynamic nature of compassion and suggests that “individualism and altruism appear to be combined in complex ways” (1991:21), not only in the same individual personality but also in society. Thus these are not extremes caught at opposing ends of a scale, but rather dynamic and interacting pluralities engaged in an agonistic relationship. Wuthnow‘s studies show that “being intensely committed to self-realisation and material pleasure did not seem to be incompatible with doing volunteer work … a slight positive relationship [exists] between these self-orientated values and placing importance on charitable activities. In other words, people who were the most individualistic were also the most likely to value doing things to help others” (Wuthnow, 1991:22). As Wuthnow’s findings imply, those who value the power to choose also value the power to choose to help others. Since caring is a behaviour of choice it is “a metaphor for our self-identity” (Wuthnow, 1991:83).

I believe that this is particularly evident in cyberspaces (I use the plural purposefully to indicate its potential and multivariate dimensions), where discourses of non-conformism, autonomy and freedom mix with those around social responsibility, compassion and humanitarianism and where the forces of self-creation and the forces of communalism meet in what often becomes a highly contested space that the individual must negotiate daily as part of increasingly interactive normative existence. Cyberbullying often manifests in these spaces as forms of contemporary hermeneutical and heterotopic anxiety (Caputo, 1993; Foucault, 1984).

4. Emotion work in cyberspace

José Casanova (2006:18) argues that there has always been the assumption that, with an increase in modernity, there is also an automatic and lamentable loss of community and communalism, what is referred to in German as Gemeinschaft, as opposed to mere society or Gesellschaft, which is largely based on individualism and ego-driven (Tönnies, 1887). However, volunteer congregations and communal philanthropy (especially prevalent and easily accessible through social networking and other cyberspaces) provide, for many people, a sense of such community, despite the postindustrial and urbanizing alienating effects of contemporary globalized living. Casanova calls these "imagined [secular] religious communities" or "civil religions" (2006:19) and predicts that they will continue to be prominent carriers of collective identities, but ongoing processes of globalisation are likely to enhance the re-emergence of the great "world religions" as globalized transnational imagined religious communities". Indeed, recent and ongoing developments in connection to the Arab Spring and Occupy social movements in, for example, Egypt, Libya and Syria serve as examples of this; as does the tragic events around 9/11, the recent Islamic State attacks on tourists in Tunisia and elsewhere and the activities of Boko Haram in Nigeria. As Myers warns "such initiatives as the Arab push for reform or the Occupy movement will ultimately fall short unless they are able to address structural change in the light of the new paradigm of interdependence" (Life Beyond War, charterforcompassion.org). Manuel Castells (2012) and Paul Hawken (2007) interrogate the potential structural changes required in these technologically mediated social movements, which Castells calls "networks of outrage and hope" and Hawken calls "the movement with no name". As Castells (2012:11) argue, and in keeping with Foucaultian theory, these symbolic spaces are transformed into public spaces, which then become political spaces, to be controlled and managed through systems and structures of governmentality: cyber-heterotopias, for example.

However, as much as the terms social movement and cyberspace imply a mass and non-embodied force or entity, they are constituted of smaller individual and personal actions. This involves what Arlie Russell Hochschild (1983) calls "emotional labour": the investment of feeling, personality and identity in the exchange of capital (either public/commercial or personal/private – these are not necessarily distinct or polar categories anymore). I believe capital here denotes not only economic capital, but also social capital. Building on the work of Sigmund Freud and Erving Goffman, Hochschild points out that emotions have

"signal functions" (1983:x) that are arrested when "private management of feeling is socially engineered and transformed into emotional labour" (1983:x). Hochschild uses the term "emotion work" (1983:7) to refer to "acts done in a private context where they have use value" (1983:7), thus the public enactment of feeling – like in cyberspaces such as chat rooms and social networking platforms. The significance of emotional labour (with either/both positive or/and negative results) and emotion work in relation to cyberspace is quite evident, particularly in relation to social networking and cyberactivism, but also to the more mundane individual interactions through instant messaging applications and chat rooms. Hochschild explains that "when elements of [an intricate private emotional] system are taken into the market [here read cyber] space and sold [exchanged] as human labour, they become stretched into standardized social forms … when emotional labour is put into the public market [cyber] space, it behaves like a commodity" (1983:13-14). As Žižek (Fiennes, 2012) notes, commenting on the ironic commodification of humanitarianism and 'good deeds' and its complex relationship with globalized consumerism: "capitalism has been the true revolutionizing force in the twentieth century, even as it only serves itself … revolution changes the social body, but the dreams remain the old dreams and [can] turn into the ultimate nightmare". Hochschild (1983:18) refers to the "relations" and "rules" that govern the public and social management of feelings, through surface acting (what one knows about oneself but hides from others) and deep acting (what one hides even from oneself, therefore making feigning unnecessary (Hochschild, 1983:33)). In his analysis of the banality of evil, The Lucifer Effect (2007), Phillip Zimbardo refers to these as "rules and roles" (2007:2012), relating in its apex form to bullying as political torture, such as the controversial events at Abu Grahib and Gauntanamo Bay. Zimbardo says: "When role behaviour and the adherence to rules are rewarded, irrespective of their ethical validity, the ego-defence mechanisms of compartmentalization and rationalization often kick in, usually as an attempt to eliminate cognitive dissonance, resulting in momentary blindness to the moral implications of one's actions" (Zimbardo, 2007:214, 220). The implications for aggression and violence in cyberspace are evident, with its inherent immediacy, anonymity and retaliatory nature. These rules then easily become the ideological myths and narratives by means of which life and relations are governed, that is the 'truths' that are told to justify actions and behavior. Ideologies are most successful when these relations are self-induced (Hochschild, 1983:35) through, what Foucault would call, self-surveillance and technologies of self (1988b), for which cyberspace provides ample opportunity, for individuals as well as communities.

5. An example case

In conclusion, I briefly refer to an example case in cyberspace where the complex and contested conflict of ideological discourses of self-construction and humanitarianism are particularly evident. Kaycee Nicole Swenson was a teenage leukemia sufferer who created and regularly posted for over two years on a web blog about her journey with cancer, until her death. The implications in terms of confessional self-revealing, humanitarian compassionate activism and inspirational self-storying are predictably familiar to most contemporary people with access to the latest communication technology. Sympathizers and supporters followed her postings and invested much time, energy and trust (thus emotion work, following Hochschild), as individuals and as a virtual support community, into the tragic unfolding life narrative of this young girl.

However, as Jordan (2005:200) explains, “the real revelation about Kaycee Nicole Swanson was that she had never been alive. She was a digital dream, a carefully constructed and maintained fictional persona affected by her “mother”, Debbie Swenson, a very real person living in a small Kansas town”. When the cyberhoax or cyberfraud, as it is variously called, was discovered the cybercommunity was understandably outraged at what was felt (emotion work, again – the exchange of feelings as commodities for some kind of reward) to be a betrayal of trust and the abuse of confidence. The rules and roles (following Zimbardo and Hochschild) of human engagement were perceived to have been broken, though no real person had been harmed or even involved.

The clash of ideological discourses between the freedom to constitute the self as an imagined and fluid identity (as the creator of the virtual person did) and the extension of the self to others in a caring community of trust (as the blog followers and sympathizers did) is representative of Foucault’s heterotopic anxiety and Žižek’s ideological pain, which we experience upon recognizing the dream state of fantasy and myth upon which we construct our identities and relationships with ourselves and others. Ideals and beliefs around authenticity and trust clashed with those about imagination and autonomy. The subsequent vilification, ostracizing and marginalization of the creator of the virtual identity in cyberspace was predictably vicious, with the inescapable surreal irony that the commentators were themselves assuming virtual identities, writing under pseudonyms, even as they were attacking Debbie Swenson for assuming a virtual identity. As Jordan (2005:208) notes, “the community’s view was that identity could be playful as long as it was also honest, and the Internet could be an ‘identity laboratory’ as long as everyone was informed and gave consent”. The ethical implications, from the perspective of ideology critique, is significant: who and what govern these rules and roles regarding what are acceptable forms of fantasy, myth and narrative; and, most importantly, can we assume any sense of trust and safety in the contested arena of cyberspace? The only possible answer to Caputo’s questions, “Who are ne now … and how can we be otherwise” (1993:252), is contained in Foucault’s vigilant attitude of “pessimistic activism” (in Grimshaw, 1993:56) and the skeptical freedom of a doubting attitude (Rajchman, 1985:3-4; Hammer, 2005:124).

6. Conclusion

This paper serves as an introductory exploration of the discursive theme of cyberbullying, in its broadest context, in relation to contemporary ideologies of cyber-based social networking, humanitarianism, selfconstruction and violence. As a particularly malignant form of violence, enabled by the inherent aspects of cyberspace (such as immediacy, anonymity, adaptability, relationality), bullying is fast becoming one of the arenas where the interaction of these discourses can best be contextualized and theorized. Further synthesis of existing work on these themes are encouraged and will lead to greater understanding of the dynamic nature of contemporary forms of ideological and practical violence, which may also lead to the construction of effective interventions to address the closely embedded social and cyber problems associated with contemporary technologically mediated human interaction.

7. References

Armstrong, K. 2008. TED Talks: Karen Armstrong Makes her TED Prize Wish: The Charter for Compassion. http://www.ted.com

Armstrong, K. 2009. TED Talks: Let's Revive the Golden Rule. TED Global.

http://www.ted.com

Armstrong, K. 2011. Twelve Steps to a Compassionate Life. London: The Bodley Head.

Athanasiou A, Hantzaroula P & Yannakopoulos K. 2008. Towards a new epistemology: The

'affective turn'. Historein Vol 8:1-16.

Babiak, P & Hare, R. 2006. Snakes in suits: When psychopaths go to work. New York: Harper Collins.

Badenhorst, C. 2011. Legal responses to cyberbullying and sexting in South Africa. Centre for Justice and Crime Prevention. Issue Paper No 10. August 2011.

Barnett, R. 1998. Supercomplexity and the university. Social Epistemology. 12(1):43-50.

Barnett. R. 2000a. Realising the university in the age of supercomplexity. Milton Keynes, UK: Society for Research into Higher Education and Open University Press.

Barnett, R. 2000b. University knowledge in an age of supercomplexity. Higher Education. 40(4):409- 422.

Barnett, R. 2000c. Supercomplexity and the curriculum. Studies in Higher Education. 25(3):255-265.

Belsey, B. 2005. Fair play at school – fair play in society towards a school without bullying! A manual for teachers and head teachers. Daphne project. http://www.cyberbullying.ca/facts-st.html In: Burton, P & Mutongwizo, T. 2009. Inescapable violence: Cyberbullying and electronic violence against young people in South Africa. Centre for Justice and Crime Prevention. Issue Paper No 8. December 2009.

Braidotti, R. 2013. The posthuman. Malden, Massachusetts: Polity Press.

Burton, P & Mutongwizo, T. 2009. Inescapable violence: Cyberbullying and electronic violence against young people in South Africa. Centre for Justice and Crime Prevention. Issue Paper No 8.

Caputo, J. 1993. On not knowing who we are: Madness, hermeneutics, and the night of truth in Foucault. In Caputo, J & M Yount (Eds). Foucault and the critique of institutions. Pennsylvania: The Pennsylvania State University Press. December 2009.

Casanova, J. 2006. Rethinking secularisation: A global comparative perspective. The Hedgehog Review. Spring & Summer, 7-22.

Castells, M. 2012. Networks of outrage and hope: Social movements in the internet age. Cambridge Polity Press.

Chouliaraki, L. 2012. The theatricality of humanitarianism: A critique of celebrity advocacy.

Communication and Critical/Cultural Studies. 9(1):1-21.

Clough P. 2008. The affective turn: Political economy, biomedia and bodies. Theory Culture & Society Sage Publications 25(1):1-22.

Clough P & Halley J (Eds). 2007. The affective turn. Durham North Carolina: Duke University Press. De Tocqueville, A. [1835] 1965. Democracy in America. New York: Harper & Row.

Fine, D. 2008. A beginner's guide to mobile communication. Integrat Mobile Aggregation Services. P 11.

http://www.integrat.co.za In: Burton, P & Mutongwizo, T. 2009. Inescapable violence: Cyber bullying and electronic violence against young people in South Africa. Centre for Justice and Crime Prevention. Issue Paper No 8. December 2009.

Foucault, M. 1984. Of Other Spaces: Utopias and Heterotopias. (Transl. J Miskowiec). In:

Architecture/Mouvement Continuité, 1-9.

Foucault, M. 1988a. The Minimalist Self: An Interview with Stephen Riggins, originally published In Ethos (1983). In: Kritzman, LD (Ed.). Michel Foucault: Politics, philosophy, culture: Interviews and other writings 1977-1984. New York and London: Routledge, 3-17.

Foucault, M. 1988b. Technologies of the self: A seminar with Michel Foucault. Martin, LH, Gutman, H & Hutton, PH (Eds). Amherst: University of Massachusetts Press.

Grimshaw, J. 1993. Practices of Freedom. In: Ramazanoglu, Caroline (Ed.). Up against Foucault: Explorations of some tensions between Foucault and feminism. London and New York: Routledge, 123-146.

Hawken, P. 2007. Blessed unrest: How the largest social movement in history is restoring grace, justice and beauty in the world. London: Penguin.

Hammer, O. 2005. New Age and the Discursive Construction of Community. Journal of Alternative Spiritualities and New Age Studies. 1:111-128.

Hochschild AR. 1983. The managed heart: the commercialisation of human feeling. Berkeley, California: University of California Press.

Hertz, MF & David-Ferdon, C. 2008. Electronic media and youth violence: A CDC Issue Brief for Educators and Caregivers. Atlanta, Centre for Disease Control.

Jakobson, R. 1995. On language. L Waugh & M Monville-Burston (Eds). Harvard University Press.

Jordan, JW. 2005. A virtual death and real dilemma: Identity, trust and community in cyberspace. Southern Communication Journal. 70(3):200-218.

Namie , G & Namie, R. 2000. The bully at work: What you can do to stop the hurt and reclaim your dignity on the job. Workplace Bullying Institute. Naperville, Illinois: Sourcebooks, Inc. Namie G & Namie, R. 2011. The bully-free workplace. New Jersey: John Wiley & Sons.

La Caze M & Lloyd HM. 2011. Editor's introduction: Philosophy and the 'affective turn'. Parrhesia. No 13:1-13.

Lampert, K. 2005. Traditions of Compassion – From Religious Duty to Social Activism. New York: Palgrove Macmillan: New York.

Leynamm, H. 1990. Mobbing and psychological terror at workplaces. Violence and Victims. Springer Publications. 5(2):119-126.

Limber, S. 2009. The challenge: A publication of the Office of Safe and Drug-free Schools.

http://www.thechallenge.org In: Burton, P & Mutongwizo, T. 2009. Inescapable violence: Cyber bullying and electronic violence against young people in South Africa. Centre for Justice and Crime Prevention. Issue Paper No 8. December 2009.

Rajchman, J. 1985. Michel Foucault: The freedom of philosophy. New York: Columbia University Press.

Rollins, P. Crucified Identities. 21 May 2013. Work of the People.

https://www.youtube.com/watch?v=e2_y_QM8yWw&list=PLAISstVxi5GnTugnTo9m8ewPA o WeO9Ox.

Salerno, S. 2006. SHAM: Self-help and actualization movement – How the gurus of the self-help movement make us helpless. London and Boston: Nicholas Breadley Publishing.

Tönnies, F. [1887] 1957. Community and Society. (Transl. CP Loomis.) East Lansing: Michigan State University Press.

Turkle, S. Alone together: Why we expect more from technology and less from each other. New York: Basic Books, Perseus Book Group.

Willard, N. 2003. Off-campus, harmful online student speech. Journal of School Violence. 1(2):66.

Wuthnow, R. 1991. Acts of compassion, caring for others and helping ourselves. Princeton, New Jersey: Princeton University Press.

Zimbardo, P. 2007. The Lucifer effect, how good people turn evil. London, Sydney, Auckland, Johannesburg Rider Books Random Books Publishing.

Fiennes, S. 2012. DVD. The pervert's guide to ideology. Scriptwriter: Žižek, S.

How students' relationships with their cellphones inform their experience of socialising online and offline

Ms Jessica Oosthuizen and Prof Charles Young
Psychology Department, Rhodes University
jessoosties@gmail.com, c.young@ru.ac.za

Abstract

This study explores the relationship that students have with their cellphones in order to understand how this device informs their social experience online and offline. Central to the design of the study is a "social media detox" for which the participants agreed to restrict their social media/cellphone use. The study employed the qualitative approach of interpretative phenomenological analysis to uncover key themes from in-depth interviews before and after the detox. Cellphones offer a sense of companionship that may deprive youth of opportunities for social development.

Keywords

social media, youth, cellphones, mobile phones, social development, cyberpsychology, identity

1. INTRODUCTION

The emergence of mobile digital technologies at the turn of the century has added a new dimension to the debate around the impact of human-computer interaction (Ahn, 2011; Palfrey & Gasser, 2010; Rosen, Cheever, & Carrier, 2012). Today's young people represent the first generation who have grown up surrounded by and immersed in these technologies and the term digital natives has been coined to describe them (Prensky, 2001). Cellphones have made it possible for young people to access social media platforms anywhere and at any time, which has given rise to a generation of young people with expectations of being 'always online' and 'always connected'(Subrahmanyam & Smahel, 2010; Turkle, 2011).

Heightened interest among young people towards social media platforms like Facebook have made them integral to the youth social experience (Ahn, 2011;

Baker & White, 2010). Baker and White (2010, p. 1591) conclude that social networking sites are ‘emerging as a primary tool for adolescent socialisation’. Furthermore, an increasing number of research studies report on young people’s preference for online social interactions instead of interactions face-to-face (Caplan, 2003, 2005; Casale, Tella, & Fioravanti, 2013; Pierce, 2009; Walsh, White, Cox, & Young, 2011).The reported perception among young people is that their involvement with social media platforms broadens their sense of community and subsequently gives them a sense of belonging (Lewis, Pea, & Rosen, 2010). In one study, Facebook was referred to as a ‘social lubricant’(Ellison, Steinfield, & Lampe, 2011, p. 873).

However, while there may be evidence to suggest the positive benefits of social media usage, many adolescents access these sites on their smartphones and there is increasing research that points towards the negative impact of excessive cellphone use. A study that focused on Problematic Mobile Phone Use (PU) showed that chronic stress, and depression scores are positively associated with PU score and emotional stability negatively related to PU score (Augner and Hacker, 2011 p.440). A recent study showed that ‘after five days interacting face-to-face without the use of any screen-based media, preteens’ recognition of nonverbal emotion cues improved significantly more than that of the control group for both facial expressions and videotaped scenes’ (Uhls, Michikyan, Morris, Garcia, Small, Zgourou,& Greenfield, 2014).

Social cognitive theory, which is the theoretical framework that informs the present study, suggests that personal agency occurs within broader social forces, where people are the products as well as the producers of their social systems (Bandura, 2001). From this perspective, it widely understood that social interactions have a central role in a young person’s social development (e.g., Bandura, 1990, 1999; Erikson, 1968). In particular, adolescence represents a unique developmental period during which young people ‘need to learn to navigate complex social situations despite strong competing feelings’ (Dahl, 2004, p. 18). The extent to which smartphone use enables or disables a young person’s capacity to navigate social situations and exercise their personal agency remains to be determined.

Many studies (e.g., Byun et al., 2009; Hall & Parsons, 2001; Huang & Leung, 2009; Young, 2009) refer to excessive and compulsive online behaviour as ‘addiction’. Boyd (2014, p. 83) argues that ‘addic¬tion rhetoric positions new technologies as devilish and teenagers as constitutionally incapable of having agency in response to the temp¬tations that surround them’. Similarly, one study points out that ‘current interest in smartphone addiction, however, focuses largely on negative outcomes, and there is a lack of discussion from the users’ perspective of the addiction’(Ahn & Jung, 2014, p. 2). This highlights the importance of this research which documents the young users’ perspective and explores the role of agency in understanding how they socialise online and offline.

The participants in this study are at the end of their adolescence. During late adolescence, individuals move away from identifying with a core group of friends or clique towards identifying with multiple peer groups and this loosening of peer bonds "coincides with a growing sense of autonomy" (Davis, 2012a, p. 1528). This study raises questions about whether or not heightened attachment towards a cellphone enables or disables a young person's capacity to develop agency in social situations.

Furthermore, since most of the available research in this field is conducted in the Global North, this study presents a unique South African perspective and draws attention to the demand for more local research. The total number of internet users South Africa is likely to increase at a 27.3% compound annual rate to reach 29.8 million in 2016 with South Africans mostly using their cellphones to access the internet (PricewaterhouseCoopers, 2012).

This study explores the relationship that young people have with their cellphone and how these devices – and the social media applications on this device – inform, influence and shape their experience of socialising with their peers. Since digital natives have little or no memory of what life was like before cellphones (Palfrey & Gasser (2010); Prensky (2001)), the detox presented the respondents of this study with the opportunity to reflect on their social behaviour with and without the presence of this device.

One of the strengths of this study is that it explores the respondents' relationship with their cellphone and the social media platforms they use to socialise. In this way, this study provides a more accurate reflection of how young people use their cellphones in real life rather than focusing on a single social media platform in isolation. Furthermore, since the field of digital technology is dynamic and constantly being innovated, the relevance of research studies that focus on a single social media platform is dependent on the longevity of that particular platform in the market (Subrahmanyam & Smahel, 2010). Thus, it is likely that this research will hold more value into the future.

2. METHOD

IPA is concerned with understanding the personal lived experience and uncovering the ordinary everyday experience and how it becomes an experience of importance in the mind of the participant (Smith, Larkin and Flowers, 2009). This approach aims to capture and explore the meanings that participants assign to their experiences. IPA involves a "double hermeneutic" (Smith and Osborn, 2003 in Smith et al., 2009, p. 35). This means that taking the participants' perspective is only one part of the analytic experience. In addition, the role of the researcher is to also offer an interpretative account of the participants' experiences. This approach will be useful to understanding how young people experience socialising online using their cellphone and offline through face-to-face interactions. Unlike most psychology which is 'nomothetic' and focused on population-level analysis, IPA is strongly influenced by idiography (Smith et al., 2009). With IPA, the focus is to understand the particular and to include a small purposively-selected homogenous sample for which the research will be meaningful (Smith et al., 2009). Smith (2004, p. 42) argues that "it is only possible to do the detailed, nuanced analysis associated with IPA on a small sample". This type of inquiry positions people's perspectives and experiences at the forefront of psychological study and in doing so, "reinforces the view that such 'personal' phenomena are an important part of psychology's subject-matter (Larkin, Watts, and Clifton, 2006, p. 118).

A common misconception about IPA is that it is a 'simply descriptive' methodology (Larkin et al., 2006). These authors argue that the reasons IPA is considered attractive to researchers – its accessibility, flexibility and applicability – are the same reasons why its critics question the value of its contribution to qualitative psychological research. They declare that "it is easy for flexibility to be mistaken for lack of rigour – and the subtlety and complexity of phenomenology's aims and origins are often overlooked" (Larkin et al., 2006, p. 103).

3. DATA COLLECTION

This study involved nine participants (ages 18–21) of different race and gender. Nine students participated in the focus groups and eight students participated in the individual interviews. All the participants were Rhodes University students who considered themselves to be "active users" (i.e. daily users) of a cellphone and social media platforms (e.g., Facebook, BBM, WhatsApp). The anonymity of each participant was maintained by providing each of them with an alias so that their identity was protected. The opportunity to participate in this study was advertised through emails, in lectures and on campus and participants were recruited in this way. The first phase of data collection involved focus groups to orientate participants to the study and to finalise the interview schedule for the individual interviews. Following the focus groups, eight participants were all interviewed twice; once before and once after the negotiated social media detox. According to Smith et al. (2009, p.52), before and after interviews are useful to achieve multiple perspectives which 'can help the IPA analyst develop a more detailed and multi-faceted account of that phenomenon'.

It should be noted that this is a relatively large sample for an IPA study as a sample size of three is considered the "default size" for a Masters-level study (Smith et al., 2009, p. 52). In terms of sample size and complexity of the design, this study goes beyond what Smith and colleagues (2009) consider being acceptable for a typical masters study. However, the sample size and complexity of the design study employed in this study was considered necessary to be able to adequately address the research aims.

4. THE SOCIAL MEDIA DETOX

The social media detox (“the detox”) required the respondents to voluntarily impose restrictions on their social media consumption habits for one or more days. A similar approach to the detox has been used in a study called ‘The World Unplugged’ (Moeller et al., 2012). The specific details of the detox in this study varied according to what each respondent decided for themselves in consultation with the researcher. The researcher did not insist on a particular format for the detox or instruct the respondent to structure their detox in a particular way. This approach enabled the respondent to take ownership of the detox process which was considered crucial to their participation and subsequent ability to contribute to this study. The researcher was also explicit about informing the participants that their involvement in this process did not involve any penalties for non-compliance.

5. DATA ANALYSIS

Analysis is a flexible, iterative process that starts with a detailed, line-by-line examination of one transcript until a degree of finality has been reached, before the analysis of subsequent cases. Once all cases had been analysed, a cross-case analysis was conducted to seek for connections across themes (Smith & Osborn, 2003; Smith et al., 2009).

6. RESULTS & DISCUSSION

In total six overlapping superordinate themes and several sub-themes emerged from the data collected during the first interviews before the detox. After participating in the social media detox, the participants were interviewed for a second time. A great deal of the data obtained from these interviews supported the findings from the first interviews. The novel findings were discussed and three overlapping superordinate themes emerged with several sub-themes. This paper discusses four superordinate themes from the first (before the detox) and second (after the detox) interviews.

Theme 1: Texting feels more natural than talking

A common characteristic observed among digital natives (recall Prensky (2001)) is that they have little memory of what their lives were like without access to cellphones. One respondent in this study described socialising on social media as ‘all we know’.

“For us we've been brought up in the era whereby socialising can mean virtual socialisation... As in people are now more likely to communicate virtually than they are to communicate personally... For us, that's all we know now.” [Thuli]

“I’m trying think what do I feel when I take my phone. That’s – I think what I’m trying describe is that, there’s not a particular feeling, you just, it just, it just happens, it’s just natural.” [Thabo]

Furthermore, respondents (see below) also described how their cellphone is ‘a part of you’ which highlights just how integral they perceive these devices to be in their lives. Cellphones have seemingly become entwined with their sense of self and normalised within their peer groups.

“[Being on your phone] it’s a norm, it’s something that happens; you do not even think about it. You do not even think that maybe I’m spending too much time with my phone, because it’s something that you grew up doing, so it’s just a part of you” [Gugu]

“.... in life we see everyone is [using a cellphone] so we are, sort of, socialised into it. I mean, we will, we’ll see that our friends are always on their phones and... So it becomes, because you on it all the time, it becomes something that you do not even realise you’re on all the time.” [Natalie]

This brings into question whether young people’s preference for online social interactions is a result of a conscious decision or whether it is a habit. The distinction between choice and habit is raised by Lindbladh and Lyttkens (2002). These authors (2002, p. 453) refer to habits as “repetitive and non-reflective behaviour”. This is distinct from choices whereby an individual makes a conscious decision.

“... we do not actually know why we [check our phone so often] ... it’s almost like – our muscles are so used to it… people get habits like for example someone might <um> always chew their fingernails or <um> play with their hair… And because we are on our phones so much, even when we do not have a purpose in going on our phone” [Natalie]

“I’m used to [checking my phone every minute] – It’s just like...you [are] blinking. You do not actually have control over that it just happens. [Like] you [are] breathing, you do not actually choose to, it just happens...you know like it’s a reflex.” [Gugu]

The respondents describe checking their cellphone with reference to bodily functions such as blinking, using muscles and breathing which illustrates just how integral their cellphone use is to their social lives. Furthermore, this draws attention to the fact that young people are seemingly unaware of the choices they make around using or not using social media.

Theme 2: “My cellphone is my comfort zone”

A ‘comfort zone’ refers to a behavioural state or position from which one struggles to escape for fear of the unknown (Ballach & Brede, 2011). The participants’ experiences reveal that their relationship with their cellphone provides a source of emotional comfort.

“Um... being socially active with my phone is much, much easier and is in my comfort zone...” [Thuli]

“I have my phone with me 24/7... I know I get too comfortable when it comes to me chatting [on my phone]... we just communicate everyday via social media... it's my comfort zone...” [Gugu]

It seems that while their cellphones are a source of comfort that allow the respondents to feel safer, using these devices also encourages the respondents to become ‘too comfortable’. Similarly, being on your cellphone creates a ‘safe place’.

“.. So for me, [being on your phone is] just a way so that I can get away from people or if I'm in a completely strange place where I do not know anyone at all, then I will be on my cellphone to create that safe place...” [Lucy]

The participants’ experiences it seems that their cellphones provide them with a form of protection from fears associated with the unknown, where the unknown is largely associated with interactions that take place offline or in ‘real life’.

“… [On social media] there’s no fear…Whereas, in real life the fear is always here for me. I think that’s the most important sort of distinction [between socialising on social media and in real life]...” [Thabo]

One of the respondents described how he resists having to spend time in his own company and his phone enables him to avoid confronting feelings of isolation because he is busy texting and checking messages from the time that he wakes up until he goes to sleep at night.

“...being alone is feeling isolated... maybe I just do not like my own company… I text until I go to sleep at night and when I wake up in the morning, first thing that I do is check all my messages. I feel a little empty if I do not have any...” [Josh]

Their cellphone is also used to protect the respondents from experiencing potential social embarrassment by avoiding ‘awkward vibes’.

“[If] I walked into a room and I felt awkward vibes I would definitely be on my phone, I’d find a spot to sit and I would be on my phone…” [Thabo]

“You first try and engage with everyone in the room and then it kind of feels like every word you’re putting out is contrived and it's like: “Oh god! This word is so forced!”…it’s almost like that feeling of you know: I’m digging myself deeper with every word I say. So I’m just going to shut the f**k up and sit down and text” [Josh]

The same respondent describes how he “slips into my phone” when such an awkward situation arises. Despite the small size of the device the respondent considers his cellphone a place of refuge or escape.

“Well, it's a device you're capable of using to better your situation of like 'I'm awkward right now, but I'm just going to slip into my phone” [Josh]

From the participants experiences it seems that all associations with social awkwardness were almost guaranteed to happen in the physical or offline context which seemed to reinforce the role of the cellphone as providing a source of protection and security. Thus, it is not surprising that they have come to rely on their cellphones in social situations. However, this raises important questions about their capacity to trust and or exercise their own personal agency during social interactions.

“...When it comes to talking to people, I rely more on my phone than myself.” [Gugu]

Theme 3: REALationships

The in-depth interview process prompted the respondents to think more deeply about their relationship with the device and how their experience of relating to people on this device compares to their experience of relating to people face-to-face:

"… People have so many layers, they're so complicated and everyone's got this aspect and that aspect and good and bad in their personality and you can't find that out on a phone so I would say that people are more interesting face-to-face." [Natalie]

Several decades ago, Mehrabian (1977) highlighted the importance of non-verbal communication in social interactions. Shilling (2012) refers to the 'enfleshment of social interactions' to emphasise the presence of the physical body in social interactions. In contrast to interactions taking place face-to-face, texting on a cellphone involves using words and emoticons to communicate. Kotlyar and Ariely (2013, p. 545) suggest that the 'limited capacity of text-based communication to convey nonverbal cues may lead to an impoverished personal interaction'.

"… You can have 150 BBM contacts but <pause> there's no one of that value to you in terms of <pause> like the real things in your life. Someone you can be completely honest with… about where you come from, about your actual life, about the things you are experiencing, about the pain you are experiencing." [Thabo]

"... You can't really "read" sarcasm on the internet – or sadness or happiness. You can use as many exclamation marks or ellipsis as you want to but it doesn't really show the person's feelings because they're hiding behind a screen" [Lucy]

After their detoxes, during their second interviews, the respondents reported how the experience of connecting face-to-face deepened their connection to their friends and they described how distinct this was from socialising through a cellphone:

"...a friend of mine; when we are talking on WhatsApp... we talk about just general things like: 'How was your day?'... But then [during the detox]…while we were chatting face-to-face –um – the fact that her mom is unemployed came out, the fact that her brother is not a nice person, whatever, came out... A lot of emotion actually came out of it, so I learned more about that person than when were on WhatsApp." [Gugu]

“...Before the detox… I thought you could survive without having to approach people [face-to-face] because I had the cushion of social media. But then now without social media, I actually realised that it's something that's actually vital...” [Thuli]

The experience of face-to-face conversations seemed to facilitate a connection that resulted in a deeper understanding of each other which seemed to be both surprising and satisfying to the respondents. Furthermore, the detox allowed the respondents to relate to their surroundings without the presence of their cellphones. In doing so, the respondents reported being able to relate to their environment in a way that was more meaningful to them.

“... [in order] to stay relevant on the social networks you have to be on your toes. You have to say something that's out of the ordinary or something that other people can relate to... [On social media] you can't say 'I'm in the library’.... But then now without [social media] I felt like I could just walk [around] without having to see and find things that I could post [online].” [Thuli]

Another respondent described how her detox experience allowed her to “look at the details of everything” because she was not “being sucked into” her cellphone:

“[During the detox] I gave myself a coffee and just [sat] outside under the tree, just like looking at everybody… I love looking at people… I love looking at the details of everything, I was looking at the trees... I wasn’t being sucked into [my cellphone]... there wasn’t anything that was on my mind at [that] moment, it was just nothing, it was just plain [and] it was just [taking in] the birds singing, the leaves falling and people talking...” [Lucy]

Theme 4: Me, My Cell & I

This section is called “Me, My Cell & I” as derived from the phrase: “Me, Myself and I” but unlike the latter, the emphasis here is on recognising oneself in relation to one’s cellphone. It seems that through their participation in the detox, the respondents became more aware of their relationship with this device. This experience seems to have also prompted them to recognise their personal agency in social situations. For some of the respondents this experience seemed to leave them feeling more empowered:

“[After the detox] I know I’m in control where I do not need to have Facebook open. I do not have to have the Twitter open. I can hide them and be perfectly content with going about my day...” [Max]

“[During the detox] I felt more in control. Because I think sometimes our phones can control us and not having it [meant] I was in control of my time management; my phone wasn’t a distraction...” [Natalie]

Another respondent described what it was like for her to reconnect with her own sense of self-control. She felt relief and that a burden had been lifted off her to know that her phone was not actually controlling her life.

“I feel relieved actually because now [after the detox] it's like a burden has been lifted off me... It means that I get some control back… I thought I was like powerless, like my phone is the one that decides what I'm doing in that moment. But [now after the detox] I feel if I cut down the amount of time I spend on social media then I'll be able to take some power back and I can actually be independent.” [Thuli]

Another respondent realised that she had unknowingly given her cellphone permission to control her life before the detox:

“I can do whatever I want to do because... my WhatsApp is not really controlling me. I am actually the one who is giving it permission to control me, in a way. So now I know that I can actually take control over it.” [Gugu]

One of the participants realised that Facebook creates a “safety net around me” which seemed to shift her understanding of her relationship with these platforms:

“...When I’m on – um – BBM or Facebook it kind of creates like this safety net around me so that people do not bug me...” [Lucy]

7. CONCLUSION

Throughout the first interviews the participants described how important their cellphones were to them because this device enables them to take charge, feel more in control and connect with each other more efficiently and effortlessly. In comparison, interacting face-to-face is associated with feeling awkward and feeling less in control of oneself in a social situation. Furthermore, the pervasive presence of cellphones in their lives has normalised the use of this device which reinforces their relationship and attachment to it. The findings from this study highlight the collective perception among the respondents that the source of their social autonomy comes mostly from outside of them – as attributed to their cellphone – rather than inside of them (as a function of their emotional intelligence or social skills, for example). It seems likely that the way in which young people relate to their phone relates to what Zizek (1998, p. 483) described as 'interpassivity' which is 'the exact obverse of interactivity'. This involves feeling that you are being active through another subject who does the activity for you. Since their cellphones have become 'a part of them' it's possible to understand why they are not aware that they have 'externalised' their source of social competency. This is compounded by their fears of experiencing awkwardness and discomfort in 'real life' (offline) encourage young people to use their cellphones as a prop, which results in them having less opportunity for social practice or information that would disconfirm the fear. Consequently, the fear of awkwardness is maintained or even strengthened.

The results of this study suggest that cellphone usage is potentially both useful and not useful to young people. Cellphone and social media use seems to be useful to young people for communicating efficiently, coordinating social arrangements, maintaining contact with friends and family who are not in close proximity and for providing them with a platform through which to broaden their network of friends. However, it is possible that cellphone and social media use is also not useful to them because it allows young people to avoid face-to-face interactions and side-step important developmental challenges as result. Thus, this study raises questions about how young people navigate and/or mediate between cellphone behaviour that is useful and not useful to them.

Self-awareness is fundamental to empowerment (Moeller, Powers, and Roberts, 2012). Insights from the second interviews – which took place after the detox – highlight the need for young people to become more self-aware of their cellphone use as a way of empowering themselves to make informed decisions about their social lives. Through their experience of participating in the detox and the in-depth interview process provided the respondents with the opportunity to critically reflect on the nature of their relationship with this device. This study suggests that the detox allowed the respondents to become more aware of their agency in social situations because they had chosen to restrict the use of their cellphone during this period. This raises important questions about how young people can be empowered to utilise their agency in terms of effecting behaviour change.

This research proposes that social fitness might be useful for interpreting how young people engage in offline and online contexts. No information in the available literature could be found to support this proposal which presents an opportunity for future research studies. Assessing how young people use the internet in terms of social fitness might be more useful than contextualising problematic behaviour in terms of behavioural addiction. In this way, social fitness might be a more appropriate term for understanding this behaviour because the emphasis is on one's capacity to socialise and being able to make informed decisions around one's social life rather than contextualising the internet itself as being similar to a drug addiction. Furthermore, the term "social fitness" recognises that young people are capable of having agency in response to how they mediate their online and offline social behaviour. With this in mind, it is possible that the use of the term social fitness is more useful to empowering young people rather than the term addiction which is often associated with relinquishing control.

8. REFERENCES

Ahn, J. (2011). The effect of social network sites on adolescents' social and academic development: Current theories and controversies. Journal of the American Society for Information Science and Technology, 62(8), 1435–1445. doi:10.1002/asi.21540

Ahn, J. & Jung Y. (2014). The common sense of dependence on smartphone: A comparison between digital natives and digital immigrants. New Media & Society, 1461444814554902. http://doi.org/10.1177/1461444814554902

Augner, C., & Hacker, G.W. (2012). Associations between problematic mobile phone use and psychological parameters in young adults. International Journal of Public Health, 57, 437–441. doi: 10.1007/s00038-011-0234-z

Bacchini, D., & Magliulo, F. (2003). Self-image and perceived self-efficacy during adolescence. Journal of Youth and Adolescence, 32(5), 337–349. doi:10.1023/A:1024969914672

Baker, R. K., & White, K. M. (2010). Predicting adolescents' use of social networking sites from an extended theory of planned behaviour perspective. Computers in Human Behavior, 26(6), 1591–1597. doi:10.1016/j.chb.2010.06.006

Ballach, S., & Brede, A. (2011). Get out of your comfort zone: The exercise book for your personal growth. [e-book]. Retrieved from http://www.amazon.com

Bandura, A. (1990). Perceived self-efficacy in the exercise of personal agency. Journal of Applied Sport Psychology, 2(2), 128–163. doi:10.1080/10413209008406426

Bandura, A. (2001). Social cognitive theory: An agentic perspective. Annual Review of Psychology, 52(1), 1-26.

Beyers, W., Goossens, L., Vansant, I., & Moors, E. (2003). A structural model of autonomy in middle and late adolescence: Connectedness, separation, detachment, and agency. Journal of Youth and Adolescence, 32(5), 351–365. doi:10.1023/A:1024922031510

Boyd, D. (2014). It's complicated: The social lives of networked teens [e-book]. Retrieved from http://www.danah.org/books/ItsComplicated.pdf

Byun, S., Ruffini, C., Mills, J. E., Douglas, A. C., Niang, M., Stepchenkova, S., … Blanton, M. (2009). Internet addiction: Metasynthesis of 1996–2006 quantitative research. CyberPsychology & Behavior, 12(2), 203–207. doi:10.1089/cpb.2008.0102

Cacioppo, J. T., Reis, H. T., & Zautra, A. J. (2011). Social resilience: The value of social fitness with an application to the military. American Psychologist, 66(1), 43–51. doi:10.1037/a0021419

Caplan, S. E. (2003). Preference for online social interaction a theory of problematic internet use and psychosocial well-being. Communication Research, 30(6), 625–648. doi:10.1177/0093650203257842

Caplan, S. E. (2005). A social skill account of problematic internet use. Journal of Communication, 55(4), 721–736. doi:10.1111/j.1460-2466.2005.tb03019.x

Casale, S., Tella, L., & Fioravanti, G. (2013). Preference for online social interactions among young people: Direct and indirect effects of emotional intelligence. Personality and Individual Differences, 54(4), 524–529. doi:10.1016/j.paid.2012.10.023

Dahl, R. E. (2004). Adolescent brain development: A period of vulnerabilities and opportunities. Annals of the New York Academy of Sciences, 1021(1), 1–22. doi:10.1196/annals.1308.001

Davis, K. (2012). Friendship 2.0: Adolescents’ experiences of belonging and self-disclosure online. Journal of Adolescence, 35(6), 1527–1536. doi:10.1016/j.adolescence.2012.02.013

Ellison, N. B., Steinfield, C., & Lampe, C. (2011). Connection strategies: Social capital implications of Facebook-enabled communication practices. New Media & Society, 13(6), 873–892. doi:10.1177/1461444810385389

Erikson, E. H. (1968). Identity: Youth and crisis [e-book]. Retrieved from http://books.google.co.za/

Greydanus, D. E., & Bashe, P. (2003). American Academy of Paediatrics: Caring for your teenager

[e-book]. Retrieved from http://www.amazon.com

Hall, A. S., & Parsons, J. (2001). Internet addiction: College student case study using best practices in Cognitive Behavior Therapy. Journal of Mental Health Counseling, 23(4), 312–327.

Henderson, L., & Zimbardo, P. (2005). The Shyness Home Page (from The Shyness Institute, Palo Alto, California). Retrieved from http://www.shyness.com/encyclopedia.html

Huang, H., & Leung, L. (2009). Instant messaging addiction among teenagers in China: Shyness, alienation, and academic performance decrement. CyberPsychology & Behavior, 12(6), 675–679. doi:10.1089/cpb.2009.0060

Kotlyar, I., & Ariely, D. (2013). The effect of nonverbal cues on relationship formation. Computers in Human Behavior, 29(3), 544–551. doi:10.1016/j.chb.2012.11.020

Larkin, M., Watts, S., & Clifton, E. (2006). Giving voice and making sense in interpretative phenomenological analysis. Qualitative Research in Psychology, 3(2), 102–120. doi:10.1191/1478088706qp062oa

Lewis, S., Pea, R., & Rosen, J. (2010). Beyond participation to co-creation of meaning: Mobile social media in generative learning communities. Social Science Information, 49(3), 351–369. doi:10.1177/0539018410370726

Lindbladh, E., & Lyttkens, C. H. (2002). Habit versus choice: the process of decision-making in health-related behaviour. Social Science & Medicine, 55(3), 451–465. doi:10.1016/S0277-9536(01)00180-0

Madell, D. E., & Muncer, S. J. (2007). Control over social interactions: An important reason for young people’s use of the internet and mobile phones for communication? CyberPsychology & Behavior, 10(1), 137–140. doi:10.1089/cpb.2006.9980

Mehrabian, A. (1977). Nonverbal Communication [e-book]. Retrieved from http://books.google.co.za/books

Moeller, S., Powers, E., & Roberts, J. (2012). The world unplugged and 24 hours without media: Media literacy to develop self-awareness regarding media. Communicar, 39(20), 45–52. doi:10.3916/C39-2012-02-04

Palfrey, J., & Gasser, U. (2010). Born Digital: Understanding the First Generation of Digital Natives [e-book]. Retrieved from http://books.google.co.za/

Pierce, T. (2009). Social anxiety and technology: Face-to-face communication versus technological communication among teens. Computers in Human Behavior, 25(6), 1367–1372. doi:10.1016/j.chb.2009.06.003

Prensky, M. (2001). Digital natives, digital immigrants: Part 1. On the Horizon, 9(5), 1–6. doi:10.1108/10748120110424816

PricewaterhouseCoopers. (2012, September). South African entertainment and media outlook: 2012-2016. Retrieved from http://www.pwc.co.za/en/publications/entertainment-and-media-outlook.jhtml

Rosen, L. D., Cheever, N. A., & Carrier, L. M. (2012). iDisorder: Understanding our obsession with technology and overcoming its hold on us. New York, NY: Palgrave Macmillan.

Scott, S. (2006). The medicalisation of shyness: From social misfits to social fitness. Sociology of Health & Illness, 28(2), 133–153. doi:10.1111/j.1467-9566.2006.00485.x

Shilling, C. (2012). The body and social theory [e-book]. Retrieved from http://books.google.co.za/books

Smith, J. A. (2004). Reflecting on the development of interpretative phenomenological analysis and its contribution to qualitative research in psychology. Qualitative Research in Psychology, 1(1), 39–54. doi:10.1191/1478088704qp004oa

Smith, J.A. & Osborn, M. (2003). Interpretative phenomenological analysis. In J.A. Smith (Ed.), Qualitative Psychology: A Practical Guide to Methods. London: Sage.

Smith, J. A., Larkin, M., & Flowers, P. (2009). Interpretative phenomenological analysis: Theory, method and research. London, UK: SAGE Publications Ltd.

Subrahmanyam, K., & Smahel, D. (2010). Digital youth: The role of media in development [e-book]. Retrieved from http://books.google.co.za/books

Turkle, S. (2011). Alone together: Why we expect more from technology and less from each other. New York, NY, USA: Basic Books.

Uhls, Y.T., Michikyan, M., Morris, J., Garcia, D., Small, G.W., Zgourou, E. & Greenfield, P.M. (2014). Five days at outdoor education camp without screens improves preteen skills with nonverbal emotion cues. Computers in Human Behavior, 39, 387-392.

Walsh, S. P., White, K. M., Cox, S., & Young, R. M. (2011). Keeping in constant touch: The predictors of young Australians' mobile phone involvement. Computers in Human Behavior, 27(1), 333–342. doi:10.1016/j.chb.2010.08.011

Young, K. (2009). Internet addiction: Diagnosis and treatment considerations. Journal of Contemporary Psychotherapy, 39(4), 241–246. doi:10.1007/s10879-009-9120-x

Zizek, S. (1998). Cyberspace, or, how to traverse the fantasy in the Age of the Retreat of the Big Other. Public Culture, 10(3), 483–513. doi:10.1215/08992363-10-3-483

Romantic Love in Virtual Space: A Literature Review

Ms. T. Lambert, Prof. G. Howcroft and Prof. C. Hoelson

Department of Psychology, Nelson Mandela Metropolitan University, PO Box 77 000, Port Elizabeth, 6031.

e-mail: tania.lambert@nmmu.ac.za

Abstract

The global popularity of the internet has led to a significant increase in romantic relationships that are initiated online. This trend is also noted in the South African context where online relationships are becoming more prevalent. Research findings indicate that people do experience meaningful online romantic relationships and that high levels of intimacy are often experienced online. The article reviews the experience of romantic love relationships in the virtual context. Both international and national literature was reviewed. The findings indicate that levels of intimacy are often higher in online relationships than face-to-face (FTF) relationships. It is suggested that the characteristics of Computer Mediated Communication (CMC) contribute to higher self-disclosure ultimately leading to higher levels of intimacy. Another important finding was that in the virtual context, unlike in FTF relationships, intimacy develops before feelings of passion develop.

Keywords

Intimacy, Romantic relationships, Self-disclosure, Virtual space

1. Introduction

The arena for finding an intimate partner has changed significantly in the 21st century. The internet has become a popular and vital part of how people seek intimate relationships. The popularity of this medium as a way of seeking intimate relationships could be explained by considering various characteristics of the medium. For instance, the internet permits relationship formation without the barriers of gating features present in real life barriers (Gibbs, Ellison & Heino, 2006) such as physical appearance, shyness and social anxiety (Bargh, McKenna & Fitzsimons, 2002). Research findings suggest that social cues are imbedded in text rather than in body language and physical appearance (Whitty & Gavin, 2001) leading to the abovementioned features becoming less apparent (Ben-Ze'ev, 2004). Another important characteristic of this medium is that individuals involved in online relationships remain to a certain extent anonymous (Bargh, McKenna & Fitzsimons, 2002; Whitty & Gavin, 2001). The benefits of Computer mediated communication

(CMC) such as anonymity, flexibility and multiple interaction allow socially anxious or lonely people to be socially rewarded by online communication without being overly conscious while at the same time guarding their self-image (Peter, Valkenburg & Schouten, 2005). Chak and Leung (2004) argued that because of the perceived control over online communication people prefer to use this medium to meet their social and intimacy needs.

Another possible explanation for the increase in online relationship formation is the increase in global usage of the internet. According to the International Telecommunications Union (ITU, 2015), internet usage in Africa has risen from 2.4% of the population in the year 2005 to 20.7% in 2015. In more developed countries the usage is much higher, for example, 77.6% of the European population has access to the internet. Research conducted in 2009 found that more than twice as much marriages occurred between people who met online than those who met in bars, clubs and other social events combined (Baily, 2010). These statistics suggests that people do experience meaningful online romantic relationships and that these relationships often lead to face to face (FTF) relationships. This notion is supported by research findings which indicate that high levels of intimacy are often experienced in the virtual context, people find these relationships meaningful and high levels of relationship satisfaction is reported. Therefore, these relationships often lead to FTF relationships (Cooper & Sportolari, 1997; Whitty, 2008; Zaczek & Bonn, 2006).

2. Concept Definitions

Romantic Love

For the purpose of the proposed study, Sternberg's (1986) Triangular Theory of Love will be used to conceptualize romantic love. According to Sternberg (1986) love within the context of interpersonal relationships consists of three different components namely: intimacy, passion and commitment. It is argued that an individual's experience of love depends on the strength and combination of these three components. Romantic love derives from a combination of the intimacy and passion components (Sternberg, 1986).

Intimacy

Intimacy is often defined as a multifaceted concept that builds as the relationship develops over time (Baumeister & Bratslavsky, 1999). Sternberg (1986) broadly defined intimacy as people's perceptions of connectedness, (psychological) closeness and bondedness within a relationship. It is important to note that intimacy is reliant on the level of self-disclosure that occurs between individuals. High self-disclosure is almost a necessary prerequisite for effective online relationships (Franzoi, 1996; Verderber & Verderber, 2008).

Passion

Passion is defined as drives that lead to romance, longing for a person, physical attraction, sexual consummation and related phenomenon in love relationships (Sternberg, 1986). Passion involves physiological arousal which is not dependent on how long you have known a person (Baumeister & Bratslavsky, 1999) and normally develops before intimacy develops (Louw & Louw, 2011).

Virtual relationships

For the context of this research online/virtual relationships refer to relationships initiated and/or maintained though Computer mediator communication (CMC). CMC is defined as any communicative transaction that occurs by using two or more electronic devices (Ahern, Peck & Laycock, 1992).

Offline/Face to Face (FTF) Relationships

Offline/FTF relationships are described as social interaction carried out without any mediating technology (David, Crowley & Mitchell, 1994). FTF relationships are also often referred to as "relationships in the real life context".

3. Research Aim

The aim of this study is to explore how individuals experience romantic love in virtual space by means of a systematic review. Therefore the research question of the study is: "How do individuals experience romantic love in virtual space?"

4. Research Methodology

The method that the reviewer used is the basic principles of a systematic review. The data that the reviewer sampled were articles in scholarly journals, books, theses and computerized databases. The reviewer used both quantitative and qualitative studies. Both international and national search strategies were employed. The reviewer used certain criteria to select relevant articles. All articles needed to contain information about how people experience romantic love relationships in virtual space. Literature focusing on the components of romantic love (intimacy and passion) was also included.

5. Findings and Discussion

In an attempt to answer the research question (how do people experience romantic love in virtual space?) two major themes emerged: the experience of intimacy in virtual space and the experience of passion in virtual space. Within each of the major themes subthemes emerged which will be discussed in more detail.

Intimacy in virtual space

Sub-themes included the following: compensating for the lack of social cues; the disinhibiting effect of anonymity; self-disclosure and the development of intimacy; and self-presentation in cyberspace. The findings will be discussed according to these themes.

Compensating for the lack of social cues

The Social information processing theory suggests that despite the characteristic lack of cues found in the nonverbal communication of online interactions, there are many other ways for people to create and process personal information (Walther, 1992). It is argued that relationships grow only to the extent that parties first gain information about each other and use that information to form interpersonal impressions of each other. Research found that, proportionately, CMC partners ask more questions and disclose more about themselves than do their face-to-face counterparts. The Social information processing theory suggests that the absence of nonverbal information will necessitates greater self-disclosure since information that can be visually ascertained needs to be communicated verbally online (Walther, 1992).

Furthermore, research findings suggest that in the virtual environment social cues are imbedded in text rather than in body language and physical appearance (Whitty & Gavin, 2001). These cues can be quite extensive and include language, style of writing, the use of emoticons, length of messages, timing and speed of writing (Doring, 2002; Ellison, Heino & Gibbs, 2006). It is argued that all of the abovementioned cues important in the development and experience of intimacy. For example, the use of words is especially powerful (Wildermuth & Vogl-Bauer, 2007). Endearing words could create a sense of caring and connectedness which fosters the development of intimacy. Longer messages could be possible be perceived as an indicator of interest. Similarly, quick response time could be perceived as an indicator of caring.

The obstacles to communicate caused by lack of interpersonal interaction in online relationships are also overcome by the use of other means of communicating behaviours that suggest intimacy, such as the use of emoticons (pictures used to depict and explain expressions and emotions). Research indicate that the use of emoticons positively influence the development of online relationships (Utz, 2000; Walther & D'Addario, 2001) and specifically the experience of intimacy (Anderson & Emmers-Sommer, 2006). For example, emotions such as smiley faces could create a friendly atmosphere which aids in developing their feelings towards each other by attracting attention and showing interest (Doring, 2002).

The disinhibiting effect of anonymity

According to Walther (1996) CMC is more intimate and surpasses the level of emotion of FTF interaction. Wysocki (1998) supported this notion, suggesting that online relationships progress far more intimately and quickly than FTF relationship partly because of the degree of anonymity but also because of the heightened level of self-disclosure. It is argued that in the virtual environment barriers of judgement and disapproval are eliminated allowing for increased self-disclosure. Therefore private information is revealed sooner in an online relationship which leads to feelings of closeness earlier in the relationship (Bonebrake, 2002; McKenna, Green & Gleason, 2002; Merkle & Richardson, 2000). Likewise, it is argued that online relationships also tend to develop at a faster rate than FTF relationships due to the notion that the social awkwardness of FTF interactions are removed. Whitty and Gavin (2001) stated that computer users report less self- consciousness and awareness of being socially evaluated which facilitates more intimate self-revelation. This is echoed by the research conducted by Anderson (2005) where individuals reported positives about their online relationships. Participants stated that the distance actually aided in increased levels of intimacy since relational partners are disinhibited and felt freer to be themselves. In addition, Merkle and Richardson (2000) stated that anonymity provides a level of psychological comfort that increases the amount of self-disclosure shared with the other person.

The greater anonymity in online relationships produces higher levels of intimacy and closeness (McKenna, Green & Gleason, 2002). In fact, it is argued by some researchers, such as Wang and Chang (2010) that anonymity, offered by online interactions, might be the greatest factor leading to higher levels of intimacy. They claimed that anonymity might trigger self-disclosure with only a moderate amount of self-disclosure risk. In addition, Merkle and Richardson (2000) stated that anonymity provides a level of psychological comfort that increases the amount of self-disclosure shared with the other person.

Self-disclosure and the development of intimacy

SNS's promote self-disclosure (Christofides, Muise, & Desmarais, 2012), but sharing information on SNS's can have social ramifications. For, example, Bazarova (2012) found that in the context of Facebook highly personal self-disclosure, is perceived as inappropriate, making the discloser seem unlikable. However, as previously discussed, self-disclosure generally increases and mutual self-disclosure plays a very significant role in the development of intimacy. It is important to note that extent to which the self-disclosure is mutual will determine the level of intimacy experienced by partners (Brehm, 1992). This reciprocal nature of the online relationship nurtures a feeling of dependence, support and understanding (Rietchard, 2007). The Uncertainty reduction theory claims that one of the major goals of relationship development, especially during the initial stages of a relationship, is to reduce the uncertainty between two partners (Berger & Calabrese, 1975). According to May and Tenzek (2011) individuals who participate in online dating sites may in fact engage in interactive behaviour and seek confirmatory information sooner than those who engage in FTF dating. Wood and Molema (2010) found that individuals who are seeking a relationship are more likely to self-disclose personal information, opinions, views and relationship statuses. This perceived usefulness of selfdisclosure, may lead to a positive attitude towards online self-disclosure. A positive attitude towards self-disclosure, in turn, has been found to be related to intention to disclose (Chang & Chen, 2014).

In an experimental study, Antheunis and Valkenburg (2007) randomly assigned 81 cross-sexed dyads into text only CMC, visual CMC or FTF groups. Participants were asked to rate the amount of partner disclosure on five intimate topics. The findings indicated significant greater CMC disclosure. Likewise, Bruss and Hill (2010) found that participants involved in online communication reported higher levels of personal self-disclosure and perceived partner self-disclosure compared to the group that interacted FTF. Van Staden (2010) confirms the notion that individuals' perceived intimacy and self-disclosure develops at a faster pace online than offline relationships. In this study respondents reported less social anxiety, greater trust and feelings of safety when engaging in online relationships. These above-mentioned studies commonly show that self-disclosure plays an essential role in the developing relationships by promoting trust, commitment and intimacy between romantic partners.

It should be noted that self-disclosure is not a one-dimensional construct, but rather can be assessed by quantity and quality of self-disclosure (Park, Jin & Jin, 2011). Researchers agree that an increased degree of intimacy is experienced in virtual space as it develops more quickly and intensely due to heightened frequency of interaction. Park, Jin and Jin (2011) conducted a study that examined the association between self-disclosure and intimacy in the context of Facebook and found that more and frequent interactions facilitated intimacy. Previous research indicated that the frequency of CMC between online partners affects their perceptions of one another (Walther, 1996). More specifically, Anderson and Emmers-Sommer (2006) found that amount of communication time had a greater impact on perceptions than the length of the relationship.

According to Gibbs, Ellison and Lai (2011) the frequency of contact is important in the development of attraction and establishing intimacy as constant contact between people causes positive responses to one another. This will ultimately lead to couples sharing more personal information with one another which leads to higher levels of intimacy. However, it must be noted that it is not only the quality if the conversation, but also the quality of the conversations escalating to different rates of intimacy (Fox & Warber, 2013; Wildermuth &Vogl-Bauer, 2007).

Self-presentation in Virtual Space

Walther (2005) acknowledges that the development of intimate relationships relies very much upon both partner's levels of self-disclosure as well as intensity of selfdisclosure. However, he also highlights other important factors that play a role. It is suggested that close relationships also develop from the sender's ability to carefully present him- or herself by editing messages before sending them, as well as the receiver's predisposition to form idealistic attributions about the partner (Fox & Warber, 2013; Walther)

The Hyperpersonal CMC model suggests CMC can become hyperpersonal because it surpasses FTF interactions (Walther, 1996). CMC allow message senders a multitude of communicative advantages over traditional FTF interaction. Compared to ordinary FTF situations, a hyperpersonal message sender has a greater ability to strategically develop and edit self-presentation. Therefore a person could create a selective and optimized presentation of one's self to others. Hyperpersonal communication is more socially desirable than individuals tend to experience in parallel FTF interaction and therefore will ultimately enhance experiences of intimacy. The Hyperpersonal CMC theory explains the exaggerated intimacy formed online as a result of the idealised perception of the partner (Walther, 1996). In FTF interaction we meet the potential partner on a regular basis and gradually we accommodate our mental image to reality. However, in online relationships people fall in love with a mental image they have constructed for themselves (Dunbar, 2012).

According to Robinson (2007) what an individual believes is another's perception of his or her appearance or behaviour occurs mainly as an imaginative process. An emotional response is based on what an individual would imagine to be perceived judgment from another, in this context an online romantic partner. A person seeks to convey a certain identity, through interaction, that is in agreement with the expectations of his/her romantic partner. A new and fitting (and potentially desirable) persona is therefore constructed in light of others' perceived expectations (Robinson, 2007). In the virtual context this newly created persona, or cyber-self, therefore becomes both the object and the subject of interaction. By perceiving another's presence, the individual presents him or herself according to the imagined expectations of his/her partner. According to Marwick and Boyd (2010) the imagined audience, in this case the romantic partner, is kept in mind when choosing what information, and in what style, to post on Social Networking Sites (SNS).

Passion in Virtual Space

As stated before, in FTF relationships most people fall in love due to physical attributes of their partners, and then that love is strengthened (or weakened) as further information is revealed. However, in online relationships where selfdisclosure is greater and hence intimacy is significant and occurs early in relationships, most people get to know each other before passion develops. According to Ben-Ze'ev (2004) online relationships in a sense mark the return to a traditional order of falling in love. As in arranged marriages online romantic love is the product of a process in which two people come to know each other before developing feelings of passion and therefore this manner of falling in love in virtual space may greatly enhance the quality of the bond between the partners. People often testify about the great intensity of their virtual love relationships – many of them indicating that they have never felt this intensity for someone before (Ben-Ze'ev, 2004).

It is commonly believed that the lack of physical contact in virtual romantic relationships will significantly hinder the experience and development of passion. It is hypothesised that due to this belief research conducted on online romantic love relationships fails to investigate how people experience passion online. However, Cooper, McLoughlin and Campbell (2000) argue that the lack of physical attributes and contact enhances other factors such as rapport, mutual self-disclosing and similarity, thus promoting erotic connections that stem from emotional intimacy rather than ‘lustful attraction’. Other researchers, such as Cooper and Sportolati (1997) shared this position by stating that the development of rapport, mutual selfdisclosure, and the empathic understanding of the other are involved in an intensifying and deepening of the connection leading to an erotic attraction to the person. It is hypothesised (by the present researcher) that the belief that physical proximity is integral to the development of passion prohibits research conducted on the online experience of passion. Up to date, passion as a component of romantic love is neglected in research studies pertaining to relationships in virtual space.

6. Conclusion

The findings suggest that the experience of romantic love in virtual space differs from traditional face to face relationships, but can be equality rewarding and satisfying. In fact, levels of intimacy are often higher in virtual relationships than in FTF relationships. In the context of virtual space, cues such as language, writing style, and the use of emoticons plays a significant role in the development and experience of intimacy. In a sense these cues compensate for the absence of FTF cues such as body language and physical appearance. Furthermore, it is suggested that the characteristics of CMC, contribute to higher self-disclosure. For, example the disinhibiting effect of anonymity facilitates more frequent and deeper levels of selfdisclosure. In addition, the ability to edit and develop self- presentation contributes to higher self-disclosure ultimately leading to higher levels of intimacy. Another important finding was that in the virtual context, unlike in FTF relationships, intimacy develops before feelings of passion develop. More specifically, in the virtual environment passion stems from emotional intimacy.

7. Recommendations for Further Studies

Many myths and negative impression still exist regarding online relationships. As such, future studies should aim to contribute to the development of the understanding of individual's significant experiences of online relationships. More specifically, indepth qualitative studies are needed to explore the richness of this phenomenon. These studies will be especially significant for the field of Cyber Psychology. At a practical level the creation of awareness surrounding the topic of online relationships can influence client treatment plans in a positive manner. As therapists may have their own perceptions of the dynamics surrounding online relationships, further research may assist them in clarifying and appropriately treating relationship concerns.

8. References

Ahern, T. C., Peck, K., & Laycock, M. (1992). The effects of teacher discourse in computer Mediated discussion. Journal of Educational Computing Research, 8(3), 291-309.

Anderson, T. L. (2005). Relationships among internet attitudes, internet use, romantic beliefs, And perceptions of online romantic relationships. Cyberpsychology & Behaviour, 8, 521-531.

Anderson, T.L., & Emmers-Sommer, T.M. (2006). Predictors of relationship satisfaction in Online romantic relationships. Communication Studies, 57(2), 153-172.

Antheunis, M. L., & Valkenburg, P. M. (2007). Computer-mediated communication an Interpersonal attraction: an experimental test of two explanatory hypotheses. Cyberpsychology & Behaviour.

Bailey. C. M. (2010). Recent trends: Online dating. Retrieved on August 30, 2012, http://cp.match.com/cppp/media/CMB_Study.pdf

Bargh, J. A., McKenna, K. Y., & Fitzsimons, G. M. (2002). Can you see the real me? activation and expression of the "true self" on the internet. Journal of Social Issues, 58(33-49), 105.

Barraket, J., & Henry-Waring, M.S. (2008). Dating & Intimacy in the 21st Century: The Use of Online Dating Sites in Australia. International Journal of Emerging Technologies and Society, 6, 14-33.

Baumeister, R. F., & Bratslavsky, E. (1999). Passion,intimacy, and time: Passionate love as a function of change in intimacy. Personality and Social PsychologyReview, 3, 49–67.

Bazarova, N. N. (2012). Public intimacy: Disclosure interpretation and social judgments on Facebook. Journal of Communication, 62, 815–832.

Ben-Ze'ev, A. (2004). Love online: Emotions on the internet. Cambridge, UK: Cambridge University Press.

Berger, C. R., & Calabrese, R. J. (1975). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. Human Communications Research, 1, 99-112.

Bonebrake, K. (2002).College students' internet use, relationship formation and personality correlates. Cyber Psychology & Behaviour, 5(6), 551-557.

Bruss, O., & Hill, J. (2010). Tell me more: Online versus face-to-face communication and self-disclosure. Psi Chi Journal of Undergraduate Research, 15(1), 3-6.

Chak, K., & Leung, L. (2004). Shyness and locus of control as predictors of Internet addiction and Internet use. Cyberpsychology & Behavior, 7(5), 559–570.

Cheng, D. K. Chan & G. H. (2004). Comparison of Offline and Online Friendship Qualities at Different Stages of Relationship Development. Journal of Social and Personal Relationships 21(3), 305–320.

Christofides, E., Muise, A., & Desmarais, S. (2012). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? CyberPsychology & Behavior, 12, 341–345.

Cohen, S., & Wills, T. A. (1985). Stress, social support, and the buffering hypothesis. Psychological Bulletin, 98, 310–357.

Cohen, S. (2004). Social relationships and health. American Psychologist, 59, 676–684

Cooper, A., Galbreath, N., & Becker, M. (2004). Sex on the Internet: Furthering our

understanding of men with online sexual problems. Psychology of Addictive Behaviors, 18(3), 223-230

Cooper, A., McLoughlin, I.P. & Campbell, K.M. (2000) Sexuality in cyberspace: Update forthe 21st Century. CyberPsychology & Behavior, 3(4), 521-536.

Cooper, A., & Sportolati, L. (1997) Romance in cyberspace: Understanding online attraction. Journal of Sex Education Therapy. 22, 7–14.

Doring, N. (2002). Studying Online-Love and Cyber-Romance. In B. Batinic, U. –D. Reips & M. Bosnjak (Eds.), Online Social Sciences (pp. 333-356). Seattle, Toronto, Switzerland, Germany: Hogrefe & Huber Publishers.

Dunbar, R. (2012). The Science of Love and Betrayel. London, UK: Faber and Faber Ltd.

Ellison, N., Heino, R., & Gibbs, J. (2006). Managing impressions online: Self-Presentation processes in the online dating environment. Journal of Computer-MediatedCommunication,

11(2).

Fox, J., & Warber, K.M. (2013). Romantic Relationship development in the age of Facebook:

Anexploratory study of emerging adults' perceptions, motives, and behaviours. Cyberpsychology, Behaviour, And Social Networking, 16(1), 3-7.

Franzoi, S. L. (1996). Social Psychology. California, CA: Brown & Benchmark.

Gibbs, J. L., Ellison, N. B., & Heino, R. D. (2006). Self-presentation in online personals: The role of anticipated future interaction, self-disclosure, and perceived success in internet dating. Communication Research, 33, 152-177.

Gibbs, J. L., Ellison, N. B., & Lai, C. (2011). First Comes Love, Then Comes Google: An Investigation of Uncertainty Reduction Strategies and Self-disclosure in Online Dating. Communication Research 38(1), 70-100.

Hardie, E., Buzwell, S. (2006). Finding Love Online: The Nature and Frequency of Australian Adults' Internet Relationships, 1-14.

International Telocommucations Union (ITU). (2015). Percentage of individuals using the internet.

Louw, D.P., & Louw, A. (2011). Adult Development and Ageing. Bloemfontein, SA:Psychology Publications.

Marwick, A. E. & Boyd, D. (2010). I tweet honestly, I tweet passionately: Twitter users context collapse, and the imagined audience. New Media & Society, 1–20.

May, A. & Tenzek, K.E. (2011). Seeking Mrs. Right: Uncertainty Reduction in Online Surrogacy Ads. Qualitative Research Reports in Communication, 12 (1), 27-33.

McKenna, K. Y., & Bargh, J. A. (2000). Plan 9 from cyberspace: The implications of the Internet for personality and social psychology. Personality and Social Psychology Review, 4, 57-75.

McKenna, K. Y., Green, A. S., & Gleason, M. E. (2002). Relationship formation on the Internet: What's the big attraction? Journal of Social Issues, 58, 9-31, 113

Merkle, E., & Richardson, R. (2000). Digital dating and virtual relating: Conceptualizing computer mediated romantic relationships. Family Relations, 49, 187-203.

Nosko, A., Wood, E. & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. Computers in Human Behavior 26, 406–418.

Park, N., Jin, B. & Jin, S. A. (2011). Effects of self-disclosure on relational intimacy in Facebook.Computers in Human Behavior, 27, 1974–1983.

Peter, J., Valkenburg, P., & Schouten, A. P. (2005). Developing a model of adolescent friendship formation on the Internet. Cyberpsychology & Behavior,8(5), 423–430.

Rietchard, C. (2007). Online dating in a South African Context: A Psychological Study of the Persona Profile. (Unpublished masters dissertation). The University of Pretoria, South Africa.

Robinson, L. (2007). The cyberself: the self-ing project goes online, symbolic interaction in the digitalage. New Media & Society, 9(1), 93–110.

Sternberg, R. J. (1986). A triangular theory of love. Psychological Review, 93, 119–135.

Thurlow, C., Lengel, L. & Tomic, A. (2004). Computer mediated communication: Social interaction and the internet. London, UK: Sage

Valkenburg, P., Peter, J., & Schouten, A. P. (2006). Friend networking sites and their relationship to adolescents well-being and social self-esteem. Cyberpsychology & Behavior, 9(5), 584–590.

Van Staden, P. (2010). Exploring self-concept and social identity in the context of online intimate relationships. (Unpublished masters dissertation). Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.

Verderber, R. F., & Verderber, K. S. (2008). Communicate!. California, CA: Thomson Wadsworth.

Walther, J.B. (1992). Interpersonal effects in computer-mediated interaction: A relational perspective. Communication Research 19,52–90.

Walther, J.B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. Communication Research, 23, 3-43.

Wang, C., & Chang, Y. (2010). Cyber relationship motives: scale development and validation. Social behaviour and personality, 38(3), 289-300.

Wildermuth, S.M., & Vogl-Bauer, S. (2007). We met on the net: Exploring the perceptions of online romantic relationship participants. Southern Communication Journal, 72(3), 211-227.

Whitty, M. T., & Gavin, J. (2001). Age/sex/location: Uncovering the social cues in the development of online relationships. CyberPsychology & Behavior, 4, 623-630.

Whitty, M.T. (2008). Liberating or debilitating? An examination of romantic relationships, sexual relationships and friendships on the net. Computers in Human Behavior, 24, 1837-1850

Wysocki, D. K. (1998). Let your fingers do the talking sex on an adult chat-line. Sexualities, 1, 425–452.

Zaczek, D., & Bonn, M. (2006). Online friendships: Their prevalence and quality. New Voices in Psychology, 2(1), 83-107.

The Extent to which Privacy Legislation of the European Union and South Africa Addresses the 2013 OECD Guidelines

P.Dala and H.S.Venter
Department of Computer Science, University of Pretoria, Pretoria, South Africa
e-mail: xprittishx@gmail.com and hventer@cs.up.ac.za

Abstract

Privacy entails controlling the use and access to place, location and personal information. The value of personal information has increased significantly due to the advent of the information age and with it, the occurrence of the most prevalent crime of the new millennium known as “identity theft”. Largely as a response to ever increasing use of personal information, the Organisation for Economic Co-operation and Development (OECD) adopted guidelines on trans-border data flows and the protection of privacy. These guidelines included eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) to govern the preservation of privacy and trans-border flow of personal data. The European Union adopted the Data Protection Directive (also known as Directive 95/46/EC) of 1995 to protect the personal information of individuals within European Union member states. In South Africa, privacy legislation in the form of the Protection of Personal Information (POPI) Act was signed into law on 26 November 2013. The POPI Act promotes the protection of personal information by public and private institutions and specifies the minimum requirements which include eight conditions for lawful processing of personal information. To date, an analysis to ascertain the extent to which the European Union and South African privacy legislation addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy including the eight privacy principles, has not been undertaken. Hence, this paper aims to initiate such an analysis, with particular focus on the extent to which the European Union’s Data Protection Directive and the South African POPI Act addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, including the eight privacy principles. In addition, similarities and differences were identified between the Data Protection Directive (1995) and the POPI Act (2013) as a result of the analysis.

Keywords

Protection of personal information, POPI Act, Data protection directive, OECD privacy principles

1. Introduction

The currency of the digital world and oil of the Internet is personal data (Kuneva, 2009). Personal data can be bought, sold and traded creating economic value (Ali et al. 2013). Hence, global risks identified by the World Economic Forum (2014) include data loss as a result of data fraud as a major risk within the technology domain. This is due to the advent of the information age which has presented new challenges in terms of preserving personal information (Saunders and Zucker, 1999).

Privacy entails controlling the use and access to place, location and personal information (Moore, 2008). The value of personal information has increased significantly due to the advent of the information age (Saunders and Zucker, 1999) and this has subsequently resulted in the most prevalent crime of the new millennium known as identity theft (Hoar, 2001). This rampant form of crime according to the Information Systems Audit and Control Association (ISACA) (2014) largely occurs when criminals electronically break into information systems (such as those owned by organisations) to gain access to databases, which allows them to steal personal information such as financial account numbers, addresses or identity numbers.

As a result, the protection of personal information aims to protect individuals against identity theft and offers wide-ranging organisational benefits such as the protection of an organisation’s brand, image and reputation, enhancing the credibility of an organisation as well as promoting consumer confidence and goodwill (Titus, 2011).

The Organisation for Economic Co-operation and Development (OECD) (1980 and 2013) adopted guidelines on trans-border data flows and the protection of privacy. The guidelines included eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) to govern the preservation of privacy and trans-border flow of personal data.

Privacy legislation in the European Union took the form of the Data Protection Directive (also known as Directive 95/46/EC) of 1995, which aimed to protect the personal information of individuals within European Union member states.

The South African privacy legislation response to protect personal information was in the form of the Protection of Personal Information (POPI) Bill first published for comment in 2005 (Stein, 2012). After undergoing numerous reviews, the POPI Bill (2009) was finally enacted and signed into law on 26 November 2013 as the Protection of Personal Information (POPI) Act (2013).

The extent to which the European Union and South African privacy legislation addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, which includes the eight privacy principles, has not been explored. Hence, this paper aims to analyse the extent to which the European Union Data Protection Directive and the South African POPI Act addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, which includes the eight privacy principles. Thus, the contribution of this paper is to provide a comparison of specific privacy legislation in relation to the 2013 OECD guidelines, instead of comparing privacy legislation of specific countries or regions to each other, which has been conducted by several researchers such as Botha et al. (2015) and Dowling (2009).

This paper is one of a series of papers that aim to provide an understanding of the POPI Act as well as:

a framework of security safeguards for confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, which has been completed and submitted.

the extent to which the European Union and South African privacy legislation addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, including eight privacy principles, which is this paper.

the current state of security safeguards within South African institutions, in relation to electronic personal information, to achieve compliance to Condition Seven of the POPI Act, which is a forthcoming paper; and

a model of operation to guide the implementation of the security safeguards, as required by Condition Seven of the POPI Act, which is a forthcoming paper.

The paper is structured as follows: Section 2 provides a background of the OECD guidelines on trans-border data flows and the protection of privacy as well as the European Union and South African privacy legislation. Section 3 analyses the extent to which the European Union Data Protection Directive and the South African POPI Act addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, which includes the eight privacy principles. Section 4 provides a critical evaluation of the analysis. Section 5 concludes the paper and also presents future work.

2. Background

This section provides a background of the Organisation for Economic Co-operation and Development (OECD) guidelines on trans-border data flows and the protection of privacy as well as the European Union and South African privacy legislation.

OECD Guidelines on Trans-Border Data Flows and the Protection of Privacy

In 1980, the OECD adopted guidelines on trans-border data flows and the protection of privacy. At that stage, the major drivers for these guidelines were the threats associated with privacy due to the ever increasing use of personal information and the impact restrictions on the flow of information will have on the global economy (OECD, 2011). As a result, the guidelines included eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) to govern the preservation of privacy and trans-border flow of personal data (OECD, 1980). These guidelines were recommended to OECD member states to be applied to all personal data by both public and private institutions [OECD, 1980 and Kirby, 2011).

The guidelines on trans-border data flows and the protection of privacy were revised by the OECD in 2013. Major drivers for the revision of the guidelines according to Kuner (2011), was due to increased globalisation of the world economy, growing economic importance of data processing, ubiquity of data transfers over the Internet, greater direct involvement in trans-border data flows, the changing role of geography and the growing risk to the privacy of individuals.

The eight privacy principles prescribed within the guidelines by the OECD in 1980 remained unchanged in the 2013 revision (Kuschewsky, 2014). However, the revised guidelines by OECD (2013) placed greater focus on implementing accountability, the basic principles of international application in terms of free flow and legitimate restrictions, national implementation as well as international co-operation and interoperability.

European Union Data Protection Directive

Privacy legislation in the European Union takes the form of the Data Protection Directive (also known as Directive 95/46/EC) of 1995.

The purpose of the Data Protection Directive (1995) as outlined in article 1 is to ensure that, “member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data”. In addition, the free flow of personal data between member states is encouraged as long as privacy is preserved.

Article 2 of the Data Protection Directive of 1995 defines personal data as, “any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

The protection of personal data as promoted by the Data Protection Directive (1995) is applicable to European Union member states. However, each European Union member state enacts their own privacy laws based on the Data Protection Directive (1995) which consists of 34 articles within 7 chapters.

The Data Protection Directive (1995) is not a regulation and this has allowed European Union member states to inconsistently interpret and apply the Directive within their own enacted privacy legislation (Lynch, 2013). For example, chapter 3 of the Directive makes provision for judicial remedies, liability and sanctions, however the conditions, actual penalties and enforcement in the event of a breach of personal information differs for each European Union member state.

As a result, in 2012 the European Commission proposed that the Data Protection Directive (1995) be replaced by the General Data Protection Regulation (2012). This proposal marked a paradigm shift from “directive” to “regulation” that sought to provide a single data protection law applicable to all European Union member states, thus preventing the need for individual privacy legislation by each European Union member state. According to Greens (2015), it is envisaged that the General Data Protection Regulation will be adopted by the end of 2015 and will be followed by a two year transition period to allow European Union member states to comply, followed by enforcement of the regulation.

South African Protection of Personal Information Act

South African privacy legislation took the form of the Protection of Personal Information (POPI) Bill, first published for comment in 2005 (Stein, 2012). After undergoing numerous reviews, the POPI Bill was finally enacted and signed into law on 26 November 2013 as the Protection of Personal Information (POPI) Act, with the purpose clearly outlined within section 2 (2013).

Section 1 of the POPI Act (2013) defines personal information as, “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.”

The protection of personal information as promoted by the POPI Act (2013) is applicable to public and private institutions in South Africa. In order to lawfully process personal information the South African public and private institutions need to comply with the minimum requirements of the POPI Act (2013), specified within 12 chapters including 8 conditions.

Although the POPI Act was signed into law on 26 November 2013 the enforcement date of POPI Act is still to be announced. However, the "Transitional arrangements" section of the POPI Act (2013) contained in chapter 11 specifies that within 1 year, compliance to the Act should be achieved by public and private institutions in South Africa, unless exemptions which are gazetted are granted. In the event of such exemption, however, the time granted to comply may not exceed 3 years.

An external Information Regulator has to be established in terms of section 39 of the POPI Act (2013) to promote, enforce and monitor compliance to the POPI Act. According to Michalsons (2014), in the event that compliance to the POPI Act is not achieved, members of the South African public and private institutions may be fined up to 10 million rand, face imprisonment not exceeding 10 years or receive a combination of a fine and imprisonment. Furthermore, institutions may suffer reputational damage, lose customers and may have to pay out millions in damages due to civil class action (Michalsons, 2014).

3. Analysis of the European Union and South African privacy legislation in relation to the 2013 OECD guidelines

This section analyses the extent to which the European Union Data Protection Directive (1995) and the South African Protection of Personal Information (POPI) Act (2013) address the 2013 Organisation for Economic Co-operation and Development (OECD) guidelines on trans-border data flows and the protection of privacy.

The analysis uses the eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) as well as the additional focus areas (implementing accountability, basic principles of international application in terms of free flow and legitimate restrictions, national implementation and international co-operation and interoperability) of the 2013 OECD guidelines on trans-border data flows and the protection of privacy, as the basis for comparison. The analysis is reflected in table 1 below, which provides the extent to which the European Union Data Protection Directive (1995) and South African POPI Act (2013) addresses the 2013 OECD guidelines.

No.	Description of the 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the European Union Data Protection Directive of 1995	Requirement addressed by the South African Protection of Personal Information Act

No.	Description of the 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the European Union Data Protection Directive of 1995	Requirement addressed by the South African Protection of Personal Information Act
1	Collection limitation principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 5 and 6).	Yes - Chapter 3: Conditions for lawful processing of personal information (Conditions 2, 3 and 4).
2	Data quality principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Article 6).	Yes - Chapter 3: Conditions for lawful processing of personal information (Condition 5).
3	Purpose specification principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 6, 7, 8, 9, 10 and 11).	Yes - Chapter 3: Conditions for lawful processing of personal information (Conditions 3 and 4).
4	Use limitation principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 6, 7, 8, 9, 10, 11, 20 and 21).	Yes - Chapter 3: Conditions for lawful processing of personal information (Conditions 2, 3 and 4) and Chapter 6: Prior authorisation.
5	Security safeguards principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 16 and 17).	Yes - Chapter 3: Conditions for lawful processing of personal information (Condition 7).
6	Openness principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 12 and 13).	Yes - Chapter 3: Conditions for lawful processing of personal information (Condition 6).
7	Individual participation principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 14 and 15).	Yes - Chapter 3: Conditions for lawful processing of personal information (Condition 8).
8	Accountability	Yes - Chapter 1: General provisions (Article 4) and	Yes - Chapter 3: Conditions for lawful processing of

No.	Description of the 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the European Union Data Protection Directive of 1995	Requirement addressed by the South African Protection of Personal Information Act
	principle	Chapter 2: General rules on the lawfulness of the processing of personal data (Article 6).	personal information (Condition 1).
9	Implementing accountability: Privacy management programme	No - Specific reference is not made to a privacy management programme.	No - Specific reference is not made to a privacy management programme. However, chapter 11 makes reference to an administrative fine being enforced in the event of failure to conduct a risk assessment and maintain good policies, procedures and practices to protect personal information.
10	Implementing accountability: Privacy enforcement authorities	Yes - Chapter 6: Supervisory authority and working party on the protection of individuals with regard to the processing of personal data (Article 28).	Yes - Chapter 5: Information regulator.
11	Implementing accountability: Data security breach notification	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Article 18).	Yes - Chapter 3: Conditions for lawful processing of personal information (Condition 7).
12	Basic principles of international application in terms of free flow and legitimate restrictions: Trans-border flows of personal data	Yes - Chapter 4: Transfer of personal data to third countries (Articles 25 and 26).	Yes - Chapter 9: Trans-border information flows.
13	National implementation	No - The European Union Data Protection Directive is not a regulation, it is a directive. As a result, Chapter 1: Article 4 states	Yes - The Protection of Personal Information Act is applicable to all public and private institutions in South Africa. At this stage the Act

No.	Description of the 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the European Union Data Protection Directive of 1995	Requirement addressed by the South African Protection of Personal Information Act
		that each member state shall apply the national provisions it adopts pursuant to the directive.	was signed into law on 26 November 2013. The enforcement date for the POPI Act is still to be announced. Thereafter, a one year transition period will apply to allow all public and private institutions in South Africa to comply with the POPI Act, after which enforcement will be monitored by the Information Regulator.
14	International co-operation and interoperability	Yes - Chapter 4: Transfer of personal data to third countries (Articles 25 and 26).	Yes - Chapter 5: Information regulator (co-operating on a national and international basis with other persons and bodies concerned with the protection of personal information).

Table 1: Extent to which the European Union Data Protection Directive (1995) and the South African Protection of Personal Information Act (2013) addresses the 2013 OECD guidelines (2013)

4. Critical evaluation of the analysis of the European Union and South African privacy legislation in relation to the 2013 OECD guidelines

This section provides a critical evaluation of the analysis performed in section three of this paper, to ascertain the extent to which the European Union Data Protection Directive (1995) and the South African Protection of Personal Information (POPI) Act (2013) addresses the 2013 Organisation for Economic Co-operation and Development (OECD) guidelines on trans-border data flows and the protection of privacy, which includes eight privacy principles.

The European Union Data Protection Directive (1995) addresses the eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) from the 2013 OECD guidelines on trans-border data flows and the protection of privacy. However, the Directive does not make reference to a privacy management programme. In terms of implementing accountability an adequate privacy management programme has to be defined and implemented and be subject to review from a privacy enforcement authority. The programme includes providing notice to the privacy enforcement authority in the event of a breach of personal data. In addition, the Directive does not address the national implementation requirement as it is not a regulation but a directive.

In terms of the South African POPI Act (2013), the 2013 OECD guidelines on trans-border data flows and the protection of privacy, including the eight privacy principles are addressed. The only exception is that no specific reference is made to a privacy management programme within the POPI Act. However, the POPI Act does make reference to an administrative fine being enforced in the event of failure to conduct a risk assessment and maintain good policies, procedures and practices to protect personal information. Furthermore, a privacy enforcement authority in the form of the Information Regulator is required by the POPI Act to monitor enforcement and receive notifications relating to breaches of personal data.

Furthermore, similarities and differences were noted between the Data Protection Directive (1995) and the POPI Act (2013) as a result of the analysis performed in section three of this paper. Firstly, all eight privacy principles specified by the OECD (2013) are addressed by both the Data Protection Directive (1995) and POPI Act (2013). Secondly, the Data Protection Directive (1995) and POPI Act (2013) both do not make provision for a privacy management programme. The major difference between the Data Protection Directive (1995) and the POPI Act (2013) is that the POPI Act is enforceable compared to the Data Protection Directive which is not enforceable. The Data Protection Directive (1995) is not enforceable as it is not a regulation, but is viewed as a guideline to serve as a frame of reference for European

Union member states when developing their own privacy legislation, which becomes enforceable within that member state once enacted.

5. Conclusion and future work

In this paper the 2013 Organisation for Economic Co-operation and Development (OECD) guidelines on trans-border data flows and the protection of privacy, which includes eight privacy principles as well as the European Union Data Protection Directive (1995) and the South African Protection of Personal Information (POPI) Act (2013) were explored.

This gave rise to an analysis of the European Union and South African privacy legislation in relation to the 2013 OECD guidelines. The analysis was followed by a critical evaluation that identified the extent to which the Data Protection Directive (1995) and the POPI Act (2013) address the 2013 OECD guidelines on trans-border data flows and the protection of privacy. In addition, the critical evaluation identified similarities and differences between the Data Protection Directive (1995) and the POPI Act (2013).

In terms of future work, the current state of security safeguards within South African institutions, in relation to electronic personal information, to achieve compliance to Condition Seven of the POPI Act (2013) will be explored. In addition, a model of operation will be proposed to guide the implementation of the security safeguards to ensure confidentiality and integrity of electronic personal information stored, processed and transmitted, as required by Condition Seven of the POPI Act (2013).

6. References

Ali, A., Eggers, W.D., Hamill, R. and Hersey, J. (2013), “Data as the New Currency - Government’s Role in Facilitating the Exchange”, Deloitte Review, Issue 13, p.19.

Botha, J., Eloff, M.M. and Swart, I. (2015), “Evaluation of Online Resources on the Implementation of the Protection of Personal Information Act in South Africa”, Proceedings of the 10th International Conference on Cyber Warfare and Security, Kruger National Park, South Africa, 24-25 March 2015, p.41.

Dowling Jr, D.C. (2009), “International Data Protection and Privacy Law”, White Case, pp.2-33, http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf, (Accessed 27 June 2015).

European Parliament. (1995), “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data”, Official Journal of the European Communities, Vol.1, No. 281, pp.31-50.

European Parliament. (2012), “Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)”, pp. 1-99, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, (Accessed 29 June 2015).

Greens, J.P.A. (2015), “EU General Data Protection Regulation State of Play and 10 Main Issues”, p.1, http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf, (Accessed 29 June 2015).

Hoar, S.B. (2001), “Identity Theft: The Crime of the New Millennium”, Oregon Law Review, Vol.80, No.4, p.1423.

Information Systems Audit and Control Association (ISACA). (2014), “Risk to Entities Regarding Data Breaches - Lessons from a Brief Case Study”, Information Systems Audit and Control Association (ISACA) Journal, Vol.2, p.14.

Kirby, M. (2011), “The History, Achievement and Future of the 1980 OECD Guidelines on Privacy”, International Data Privacy Law, Vol.1, No.1, p.6.

Kuner, C. (2011), “Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present and Future”, OECD Digital Economy Papers, No.187, pp.10-11.

Kuneva, M. (2009), “Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling”, p.2, http://europa.eu/rapid/press-release_SPEECH-09-156_en.pdf, (Accessed 27 June 2015).

Kuschewsky, M. (2014), “The New Privacy Guidelines of the OECD: What Changes for Businesses?”, Journal of European Competition Law & Practice, Vol.5, No.3, p.147.

Lynch, L. (2013), “EU Data Protection’s Paradigm Shift: From Directive to Regulation”, p.2, http://www.ey.com/Publication/vwLUAssets/EU_Data_Protections_Paradigm_Shift_From_Drective_to_Regulation/$FILE/EU%20Data%20Protections%20Paradigm%20Shift%20From%20Directive%20to%20Regulation.pdf, (Accessed 29 June 2015).

Michalsons. (2014), “Protection of Personal Information Act - POPI”, http://www.michalsons.co.za/protection-of-personal-information-act-popi/11105, (Accessed 27 June 2015).

Moore, A.D. (2008), “Defining Privacy”, Journal of Social Philosophy, Vol.39, No.3, p.425.

Organisation for Economic Co-operation and Development (OECD). (1980), “OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data - Annex to the recommendation of the Council of 23 September 1980”, pp.1-4.

Organisation for Economic Co-operation and Development (OECD). (2011), “Thirty Years After The OECD Privacy Guidelines”, p.10.

Organisation for Economic Co-operation and Development (OECD). (2013), “OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data”, pp.1-154.

Republic of South Africa. (2009), “Protection of Personal Information (POPI) Bill”, Cape Town and Pretoria: Government Printer, pp.1-50.

Republic of South Africa. (2013), “Protection of Personal Information (POPI) Act (Act 4 of 2013)”, Cape Town: Government Printer, No.37067, pp.2-146.

Saunders, K.M. and Zucker, B. (1999), “Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act”, International Review of Law, Computers & Technology, Vol.13, No.2, p.183.

Stein, P. (2012), “South Africa’s EU-style Data Protection Law”, Without Prejudice, Vol.12, Issue 10, pp.48-49.

Titus. (2011), “Protecting Personally Identifiable Information (PII) with Classification and Content Inspection”, Titus White Paper, p.5.

World Economic Forum (WEF). (2014), “Global Risks 2014”, Insight Report, 9th Edition, pp.12-13, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, (Accessed 27

June 2015).

Social networking as both a cause for concern and a window for hope - A focus on child online protection in Namibia.

Attlee M. Gamundani1, Isaac Nhamu2, Fungai Bhunu-Shava3, Mercy Bere4

Polytechnic of Namibia transforming into Namibia University of Science & Technology
School of Computing & Informatics,
Computer Science Department.
(agamundani1, inhamu2, fbshava3, mbere4)@ polytechnic.edu.na

Abstract

The interconnectedness of communication channels availed through various social platforms has presented a unique socialisation platform. The complexity of such social communication networks have grown and presented a new dimension towards security concerns within the cyberspace. On the positive end, such web of connections has enabled sharing of ideas and information effortlessly. Bringing the child to such a mixed environment presents a set of demanding and critical issues to deal with in the cyberspace. The motivation to look at social networking was purely driven by the wide use that it enjoys mostly among the “dot-com” generation. With such intense use, where limits are not defined, there is need to explore the extent to which such a special group of users are exposed to and how much risks they are exposed to and how much know-how they have as to ensure their own safety. This research will employ a qualitative research approach to solicit some of the potential traits among the youth as active users of social networking platforms. Similar related work carried out will be analysed using the desktop approach, based on the findings, an action based solution will be proposed to deploy awareness and equipping of such users. It is envisaged that social networking platforms can be used to avail positive solutions in a faster way to some of the challenges that utilise the very same platform to perpetrate the ills that needs attention, especially with a focus on Child Online Protection (COP).

Keywords

Social, Cyberspace, Child, “Dot –com”, Online, Networking.

1. Background

The complexity of social communication networks have grown and presented a new set of challenges that has marred the cyberspace with a unique set of crimes. Online predators that prey on naive children through their pervasive behaviours are rampant (Wolak, J.et al, 2008). Internet sex crimes involving adults and juveniles are no longer surprising pieces of news as relationships are being developed online resulting in open seduction of underage teenagers (Wolak, J.et al, 2008).

A social network site enables individuals to construct web based profiles that are visible to the public. The developed web based services positions the very users in a situation where they are able to interact with those they share connections and the extended connections created by their established connections too (Lindamood, J. et al, 2009). The build-up of these connections vary from one site to another, hence there is no universal design for such networks (O'Keeffe, G.S. et al, 2011).

The content that facebook profiles contain includes photos, dating preferences, birthdays, etc. Since the launch of the facebook platform, profiles can also display third-party gadgets. (Felt, A., & Evans, D., 2008). With such content enabled, it makes the task of predators much easy in as far as accessing their victims' profiles is concerned. It is very easy to quickly create a profile of a person through social networking inputs. Social networks meet a unique need by allowing users to articulate and make visible their social networks (O'Keeffe, G.S. et al, 2011). This explains why the complexity of the networks that are ultimately created as a result of the web of connections are quite complex to assimilate hence increasing the vulnerabilities thereof.

What also constitute a social network can typically be explained in light of any website that allows social interaction as espoused by (O'Keeffe, G.S. et al, 2011), where mention is alluded to such social networking sites as facebook, My Space, Twitter, gaming sites and virtual worlds such as club Penguin, Sims as well as video sites such as YouTube and blogs. There is quite a diverse of such sites and their exponential growth is quite alarming. The usage of such platforms since their inception has witnessed the integration by users into their daily practices as supported by (O'Keeffe, G.S. et al, 2011). There have been some side effects on the health side of such integrated usage, as coined by (O'Keeffe, G.S. et al, 2011), "Facebook depression," however the focus of this paper is to look at the effects such integration have on children's lifestyle on the cyberspace.

Purposefully looking at the motivation behind the growth and existence of social network platforms there are six functions as expounded by (Richter, A., & Koch, M, 2008), namely:- (1) Identity management(2) Expert finding (3) Context awareness (4) Contact management (5) Network awareness (6) Exchange. Such functionalities as the authors explained facilitate the modularisation and integration into specific application domains. This paper will harness part of that concept to look at the positive side social networking platforms could be harnessed on, to aid awareness of the weakness and lookouts aspects of the social platforms.

The following section will hint on some of the user traits that contribute either directly or indirectly to the subsequent attacks via social network platforms, followed by a section that focuses on scenarios where social networking has been used as either a vehicle to ignite child abuses online or having been used as a vehicle for awareness for some of the lookouts on purported child online cases. Informed by the case scenarios, the next section will detail the potential modalities that could be extended to ensure child online threats are brought to the fore effortlessly, especially harnessing the wide usability that it enjoys among the affected user groups. An explanation on how we propose the use of social networking as a tool for advancing solutions towards child online protection challenges will be done before the concluding remarks and future research insights.

2. “Dot-com” generation- user traits

There are varied and dynamic uses of social networking platforms by the 21st child dubbed the “dot-com” generation. This section has focused on identifying those and solicit possible traits that could be capitalised to bring awareness of some of the practices, they might be neglecting as they un-endlessly explore the cyberspace horizons. Considering the observation by (Kornblum, J., 2005), on the entertainment use of social networking by teens, which online predators utilise to stalk their victims. A worrying development is reported of young girls who have been molested by strangers they meet on social networking sites (Kornblum,J., 2005). The profiling capability offered by social networking platforms makes it easy for fishing victims by gender and age.

The teens are sometimes their own enemies on social platforms as they occasionally fabricate details of what they post on the sites as rightly presented by (Bahrampour , T., & Aratani,L.,2006) in the statement, “Increasingly, many teenagers feel pressured to show themselves doing more risqué things, even if they are not actually doing them.” Such behaviours put their fellow colleagues into serious dangers. They will experiment with certain behaviours and forced to create strange relationships for the sake of appealing to their colleagues in the name of competition and a sense of belonging. As supported by (Barnes, S. B., 2006), the need for social networking sites to heighten awareness even on privacy issues, cannot be underestimated especially with teens outpouring their intimate thoughts publicly.

In a study done by (Ellison, N. B., 2007), where focus was on identifying motivation for cyber-bullying and online harassment of teenagers in the United states, the observation that having social networking site membership is not the predictor of online abuse for teenagers is a hint towards a different behavioural user traits. As alluded by (Ellison, N. B, 2007) those demographic and behavioural characteristics of teenagers are stronger predictors of online abuse based on their findings. From this, we can postulate that, there are unpredictable online behaviours teenagers have and it will not be easy to handle such traits, hence an open room for further research.

To explain the extent of negligence to security requirements by youth (Ellison, N. B, 2007), reference to the following various other authors makes it clear as presented by (Acquisti, A., & Gross, R., 2006) that there is often a disconnect between students' desire to protect privacy and their behaviours, a theme that is also explored by (Stutzman, F., 2006) in a survey of Facebook users and the description of the "privacy paradox" that occurs when teens are not aware of the public nature of the Internet (Barnes, S.B. , 2006). The bottom line is the fact that the teenage users may not be concerned with doing a due diligence on the platforms they use but glued on the capabilities such platforms can avail to them. It will own dawn to them when they are in danger, hence awareness is key to ensure responsible social networking behaviours amongst the youth.

A more escalating user trait among the teenagers is the excessive overreliance on social platforms. During the inception of social networking platforms (Benniger, J.R.,1987) described how mass media has gradually replaced interpersonal communication as a socializing force. What is alarming even to date is that teenagers are relating more to friends they meet online than close family in their physical spaces, in turn social networking is now defining youth culture where they can now explore themselves and share cultural artefacts (Jenkins, H. & Boyd, D., 2006). Precisely teenagers are now living in virtual environments most of their everyday lives depending of their access levels to the internet.

3. Social networking case studies

Social networking can have both positive and negative effects on its users. This section dwells on some of the positive and negative issues social networking has on children. This will be a showcase of scenarios where social networking was used as flame that ignites positive action and feelings in children and also in areas where social networking is used as a vehicle to ignite child abuses online.

A Texas college survey of 2603 students found that there was a positive relationship between the use of Facebook and student's life satisfaction, political participation, social trust and civic engagement (Valenzuela, S. et. al. ,2009). Although, in another survey it was discovered that Facebook use only helps in maintaining existing offline relationships instead of building new ones (Ellison, N.B., et.al., 2007). This same study also confirms that use of SNS increases student's psychological well-being which is a great benefit to those students with low self-esteem. This study also saw strong relationship between Facebook use and bridging social capital.

472 Facebook groups related to concussion which is defined as temporary unconsciousness or confusion and other symptoms caused by a blow on the head were screened by three researchers using a specifically developed coding scheme to

examine demographic information and the purpose of the posting. In the main part, individuals utilised the Facebook group to relate personal experiences of concussion (65%), although it was also used to seek (8%) or offer advice (2%). This study highlights the evolving nature of healthcare support in the twenty-first century and the rich information present relating to concussion on SNSs such as Facebook. (Ahmed, O. H.,et. al, P, 2010).

SNS seriously poses privacy concerns especially when young users are concerned (George,A., 2006; Kornblum, J. & Marklein, M.B., 2006). Some of the concerns are:

Some of the information on SNS like hometown and date of birth on SNS might be used to reconstruct private information like social security numbers (Ellison, N. B., 2007)

Students do not want to share everything about themselves but they do not realise that the information they are sharing on Facebook is in public space (Barnes, S. B.,2006).

Schools and potential employers can also access the information the students post on SNS (Barnes, S. B.,2006).

Another concern of using SNS is that they expose children to unwanted sexual solicitation. In addition children are asked to divulge personal sexual information and do something sexual. Children are also exposed to internet harassment (Ybarra, M. L., & Mitchell, K. J. (2008). Internet harassment which might be in the form of cyberbullying is also prevalent as is shown by a study on 2186 students were 30% report that they have either been victims, perpetrators or both of cyberbullied (Sengupta, A., & Chaudhuri, A., 2011).

4. Social networking as an awareness platform

This section will detail the potential modalities that could be extended to ensure child online threats are brought to the fore effortlessly, especially harnessing the wide usability that it enjoys among the affected user group. The SNS can also be used to promote secure behaviour among the children by sharing information on threats and best practices using social tools.

Security solutions have moved from focusing on technology as a solution to the use component through awareness, training and education. Among the tools used to enhance user awareness are visual aids, videos, cartoons, etc. According to (Byron, T., 2008) better awareness of risk doesn’t certainly restrain children’s adventurous behaviour as they are naturally inquisitive. Children always seek to explore, defy boundary, learn new things, and conquer new heights. However recommended strategies to address online risks should focus on influencing behaviour through limiting availability, access and increasing resilience (Byron, T., 2008). The first two can potentially magnify the problem as they stimulate the natural tendencies in children to break boundaries and emerge superheroes, as such we will focus on increasing resilience.

Social network services such as Facebook provide new data for social science research into, for example, the role of individual characteristics in friendship formation and the diffusion of tastes in social networks. This will aid is designing solid awareness portfolios. Social network services may eventually serve as e-Research platforms for delivering social network analysis tools (Ackland, R., 2009). Data for assessment of the effectiveness awareness strategies designed and deployed can be evaluated through the same platform, bringing the notion of a complete ecosystem.

We may capitalise on the design principles being extended to SNS, such as Safebook, a decentralized and privacy- preserving online social network application. (Cutillo, L. A., et.al., 2009). The two design principles of decentralization and exploiting real-life trust (Cutillo, L.A., et.al., 2009) used in Safebook makes it possible to create various mechanisms for privacy and security that will ensure the main security requirements for personalised data are met.

In the context of online social networking, surveillance is something potentially empowering, subjectivity building and even playful – what I call participatory surveillance. (Albrechtslund, A., 2008). This is also supported by (Wolak, J., et. al. , 2008), where mention is made of prevention strategies that target youths directly and acknowledge normal adolescent interests in romance and sex. These should provide younger adolescents with awareness and avoidance skills while educating older youths about the pitfalls of sexual relationships with adults and their criminal nature.

By nature humans have a tendency of conforming to a culture in context, better still children easily succumb to peer waves. Culture plays an important role in shaping behaviours of children in society as they seek acceptance at all levels. The “dot com” child lives for technology and is very dependent on SNS for information. Parties, dates, games and other activities are organised, initiated and shared on these platforms. There is no doubt that this same platform can offer a tool for conscientising the children (“dot-com” generation) on the threats that luck on the internet seeking to devour them and how they can stay safe.

Success stories of using social networks in health, election campaigns have been witnessed (Shirly, 2011; Wakefield, M.A., et. al., 2010). We therefore propose an awareness strategy capitalising on the connectedness of children to social networks. Social networking as an awareness strategy will prove efficient as some of its applications in other domains , where its trust have been extended to some non-profit organisations as explained by (Waters, R. D., et.al, 2009), where emphasis is placed on careful planning and research to develop social networking relationships with the intended audience.

5. Designing an awareness strategy

We propose the use of reverse engineering in using social networking platforms as an awareness campaign. The fact that the same platforms are being used for attacks, we propose the use of the same platform to avail possible solutions by reaching out to those being victimised. The observation that those having much online presence are the ones with the motive of taking advantage of naïve users online, the same presence could be extended from the positive side through awareness campaigns.

The resistance that social platforms may receive as a vehicle to advance possible solutions to the challenge of online abuses as presented by (Barnes, S. B., 2006), where mention is given of the outpouring of personal information in public social networking sites to be a problem, we envisage an opportunity that could be capitalised using social networking platforms as an awareness campaign tool. The motivation to look at social networking as a campaign tool is on the bases of its wide use among the targeted audience. It will be proper to utilise the platform they access frequently than trying other forms that will not pass the message timely. As presented on some of the case study findings some of the youth relate more to some of these social platforms than they do to physical human intervention.

The focus on designing an awareness strategy should not be one sided but holistic in nature. If effective solutions for example towards protecting privacy on online social networking sites can be approached in three different ways — social solutions, technical solutions, and legal solutions (Sullivan, B., 2005). The participation of all key stakeholders should be mandatory for effective results. As emphasised by (Sullivan,B., 2005) that experts are in tandem with the idea that, the initial step in building protections for teenage bloggers starts with parents. The increasing usage gap between parents and their children is one that is prompting the user traits earlier mentioned in the second section of this paper. Some of the initiative and software at the disposal of parents for monitoring their children's behaviours (Downes, S., 2006) should be promoted in the awareness campaigns too. As rightly presented by (Barnes, S. B.,2006), where he unequivocally mention that it is a parental responsibility to protect teens, however the education of teens and their parents to some of the security aspects of social platforms is a concerted effort to be shared among schools, social networking organisations, and government agencies.

The awareness strategies should include the commercial social network companies as key stakeholders. (Auchard,E., 2006) hints on some of the initiatives already made by commercial social networking companies in reaction to the problem of teens online. This clears some of the concerns on the buy -in by key stakeholders. For a successful awareness, buy-in is one of the requirements. With current initiatives underway in Namibia, there is hope of such awareness strategies to be explored and materialised. There are also various other initiatives by social networking sites to explore on technological solutions to protect their users better, where evidence is presented of Facebook's recent overhaul on its privacy setting to give members tighter controls over who sees what (Duffy,M., 2006). On the other hand MySpace worked on software to try and identify children under the age of 14, despite the difficulty presented in age identification online as some users do not avail correct details always (Reuters, 2006a).

The opportunity presented by the awareness

Online awareness campaigns via social network platforms could present both positive and negative results depending on how the awareness strategy has been designed and rolled out. On the positive side, coverage of a wider audience could be realised at the shortest space of time. However, such awareness campaigns if not properly structured may create room for more complicated online abuses by perpetrators.

We envisage an informed user if successfully presented , and a reduction of cases where personal dataveillance is at minimal as one of the biggest worries promoting cyberstalking as highlighted by (Huffaker, D.A., & Calvert, S.L., 2005) is revealing a considerable amount of information.

6. Conclusion and Recommendations

The work presented here is still at the theoretical level and is subject to testing for its practical relevance. However, the potential to explore both the positives and negatives of social platforms could be advanced. There is not much evidence of social networks being the sole cause for most child online abuses, but the existence of some of the child online abuses as cyber bullying, sexting, child pornography and many other related online negative exposures to minors is a serious cause for concern.

Social networking has both its ills and strength it is prudent to look at both from a constructive point of view as witnessed by many successful advertisements that have seen the growth of large corporations and a productive platform for dissemination of vital information among users.

7. Future Work

There is an ongoing project at its infancy in light on Child Online Protection initiatives in Namibia this research group is conducting with the full collaboration of UNICEF were the main focus is towards looking at all forms of avenues that can be explored to ensure children's safety online. There are various stakeholders who are involved in the same project too, with the same mandate of ensuring children are safe online.

8. References

Ackland, R. (2009). "Social network services as data sources and platforms for e-researching social networks". Social Science Computer Review.

Acquisti, A., & Gross, R. (2006). "Imagined communities: Awareness, information sharing, and privacy on the Facebook." In P.Golle & G.Danezis (Eds.), Proceedings of 6th Workshop on Privacy Enhancing Technologies (pp. 36–58). Cambridge, UK: Robinson College.

Ahmed, O. H., Sullivan, S. J., Schneiders, A. G., & Mccrory, P. (2010). "iSupport: do social networking sites have a role to play in concussion awareness?" Disability and rehabilitation, 32(22), 1877-1883.

Albrechtslund, A. (2008). "Online social networking as participatory surveillance." First Monday, 13(3).

Auchard, E.(2006). "MySpace.com hires child safety czar from Microsoft," Reuters (10 April), at http://today.reuters.com/news/articlebusiness.aspx? type=media & story ID = nN101347 & from=business, accessed 22 July 2015.

Bahrampour, T. & Aratani,L. (2006). "Teens' bold blogs alarm area schools," Washington Post (17 January), at http://www.washingtonpost.com/wp-dyn/content/article/2006/01/16/AR2006011601489.html, accessed 18 July 2015.

Barnes, S. B. (2006). "A privacy paradox: Social networking in the United States." First Monday, 11(9).

Benniger, J.R. (1987). "The control revolution: Technological and economic origins of the information society." Cambridge, Mass.: Harvard University Press.

Boyd, D. (2006a). "Friends, Friendsters, and MySpace Top 8: Writing community into being on social network sites." First Monday, 11(12). Retrieved July 28, 2015 from http://www.firstmonday.org/issues/issue11_12/boyd/

Byron, T. (2008). "Safer children in a digital world: the report of the Byron Review: be safe, be aware, have fun."

Cutillo, L. A., Molva, R., & Strufe, T. (2009). "Safebook: A privacy-preserving online social network leveraging on real-life trust." Communications Magazine, IEEE, 47(12), 94-101.

Downes, S. (2006). “Teens who tell too much,” New York Times (15 January), at http://www.nytimes.com/, accessed 28 July 2015.

Duffy,M. (2006). “A dad’s encounter with the vortex of Facebook,” Time (19 March), at http://www.time.com/time/magazine/article/0,9171,1174704,00.html, accessed 23 July 2015.

Ellison, N. B. (2007). “Social network sites: Definition, history, and scholarship.” Journal of Computer-Mediated Communication, 13(1), 210-230.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). ‘The benefits of Facebook “friends:” Social capital and college students use of online social network sites”. Journal of Computer-Mediated Communication, 12, 1143–1168.

Felt, A., & Evans, D. (2008). “Privacy protection for social networking apis.” 2008 Web 2.0 Security and Privacy (W2SP’08).

George, A. (2006). “Living online: The end of privacy?” New Scientist, 2569. Retrieved July 28, 2015 from http://www.newscientist.com/channel/tech/mg19125691.700-living-online-the-end-of-privacy.html

Huffaker, D.A., & Calvert,S.A.(2005). “Gender, identity, and langugage use in teenage blogs,” Journal of Computer–Mediated Communication, volume 10, number 2, at http://jcmc.indiana.edu/vol10/issue2/huffaker.html, accessed 16 July 2015.

Jenkins, H., & Boyd, D.(2006). “Discussion: MySpace and Deleting Online Predators Act. “DOPA 24 May, at http://www.danah.org/papers/MySpaceDOPA.html, accessed 26 July 2015.

Kornblum, J. (2005). “Teens wear their hearts on their blog,” USA Today (30 October), at http://www.usatoday.com/tech/news/techinnovations/2005-10-30-teen-blogs_x.htm, accessed 11 July 2015.

Kornblum, J., & Marklein, M. B. (2006). “What you say online could haunt you.” USA Today. Retrieved July 28, 2015 from http://www.usatoday.com/tech/news/internetprivacy/2006-03-08-facebook-myspace_x.htm

Lindamood, J., Heatherly, R., Kantarcioglu, M., & Thuraisingham, B. (2009). “Inferring private information using social network data.” In Proceedings of the 18th international conference on World wide web (pp. 1145-1146). ACM.

O'Keeffe, G. S., & Clarke-Pearson, K. (2011). “The impact of social media on children, adolescents, and families.” Pediatrics, 127(4), 800-804.

Reuters, (2006a). “State wants MySpace to raise minimum age,” (3 May) at http://www.rapidnewswire.com/5036-myspace-0245.htm, accessed 23 July 2015.

Richter, A., & Koch, M. (2008). “Functions of social networking services.” In Proc. Intl. Conf. on the Design of Cooperative Systems (pp. 87-98).

Sengupta, A., & Chaudhuri, A. (2011). “Are social networking sites a source of online harassment for teens? Evidence from survey data.” Children and Youth Services Review, 33(2), 284-290.

Shirly, C. (2011). “The Political Power of Social Media.” Foreign Affairs.

Stutzman, F. (2006). “An evaluation of identity-sharing behavior in social network communities.” Journal of the International Digital Media and Arts Association, 3(1), 10–18.

Sullivan,B. (2005). “Kids, blogs and too much information: Children reveal more online than parents know,” MSNBC.com, at http://www.msnbc.msn.com/id/7668788/print/1/displaymode/1098/, accessed 21 July 2015.

Valenzuela, S., Park, N., & Kee, K. F. (2009). “Is There Social Capital in a Social Network Site?: Facebook Use and College Students' Life Satisfaction, Trust, and Participation1”. Journal of Computer-Mediated Communication, 14(4), 875-901.

Wakefield, M. A., Loken, B., & Hornik, R. C. (2010). “Use of mass media campaigns to change health behaviour.” The Lancert, 376(9748), 1261-1271.

Waters, R. D., Burnett, E., Lamm, A., & Lucas, J. (2009). “Engaging stakeholders through social networking: How nonprofit organizations are using Facebook.” Public Relations Review, 35(2), 102-106.

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). “Online" predators" and their victims: myths, realities, and implications for prevention and treatment.” American Psychologist, 63(2), 111.

Ybarra, M. L., & Mitchell, K. J. (2008). “How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs.” Pediatrics, 121(2), e350-e357.

The use of e-procurement in South African public procurement law: challenges and prospects

Alison Anthony
University of the Western Cape
aanthony@uwc.ac.za

Abstract

The debate on the use of electronic methods to create a more efficient public procurement system has featured prominently in the international public procurement arena. To date many countries have implemented e-procurement procedures and have promulgated legislation in order to legally regulate these methods. In South Africa, however, the state has been slow to respond to this global trend of legal regulation of e-procurement. Public procurement is regulated by section 217 of the Constitution which requires that when government contracts for goods and services, it should do so in accordance with a system which is fair, equitable, transparent, competitive and cost-effective. Legislation which directly regulates public procurement in South Africa makes no express provision for the promotion of e-procurement. The Electronic Communication Transactions Act, although not directly regulating public procurement, does not preclude the use of e-procurement for commercial purposes. It therefore appears that there is in principle no impediment to the implementation of e-procurement procedures in South Africa, provided that the principles in section 217 of the Constitution are complied with.

It has been noted that the use of e-procurement has immense potential to decrease costs, increase transparency and limit corruption in competitive bidding processes. However, along with its advantages, the use of e-procurement may have a number of drawbacks. This paper seeks to determine what e-procurement entails, whether the current South African public procurement legal framework can be developed to include one of its models or a variation thereof, how South Africa can benefit from e-procurement and the extent to which the principles in section 217 of the Constitution may be affected.

Keywords

E-procurement, legal framework, competitive bidding.

Proceedings of the African Cyber Citizenship Conference 2015
Port Elizabeth, 2-3 November 2015 (http://accconference.nmmu.ac.za)
ISBN: 978-1-920508-67-8

1. Introduction

In order for the government to function, it needs goods and services. It may acquire these goods and services by using its own resources, or by contracting with outside bodies. The latter method is generally referred to as public or government procurement.

Government procurement usually contributes a large deal to a country's economy and is therefore of great importance. In 2002, government procurement was estimated to amount to 21.77% of the gross domestic product (GDP) (Audet 2012). Section 217 of the Constitution sets the standard for government procurement in South Africa. Section 217(1) provides that organs of state in the national, provincial or local sphere of government or any other institutions identified in national legislation when contracting for goods or services must do so in accordance with a system which is fair, equitable, transparent, competitive and cost-effective. Organs of state are not prevented from implementing procurement policies which provide for categories of preference in the allocation of contracts and the protection or advancement of persons, or categories of persons, (previously) disadvantaged by unfair discrimination in terms of section 217(2). Section 217(3) in turn provides that national legislation must prescribe a framework in terms of which section 217(2) must be implemented.

Electronic procurement, better known as e-procurement, has been employed in various countries for a number of years. It has been implemented in different ways, each with its distinct advantages (Soudry 2004). Generally, competitive bidding is the primary procedure used for the acquisition of goods and services by the government due to its competitive nature which is believed to yield the best value for money. It would appear that the electronic version of competitive bidding is the electronic reverse auction procedure. The United Nations Commission for International Trade Law's

(UNCITRAL) Model Law on Public Procurement of Goods,

Construction and Services (hereafter referred to as the UNCITRAL Model Law) makes reference to e-procurement in the form of electronic reverse auctions. The Model Law defines electronic reverse auctions in Article 2 as "an online real-time purchasing technique utilized by the procuring entity to select the successful submission, which involves the presentation by suppliers or contractors of successfully lowered bids during a scheduled period of time and the automatic evaluation of bids". It therefore entails active involvement of bidders during the bidding and award process.

2. Legislative framework for public procurement in South Africa

The legislation applicable to procurement in general includes the Preferential Procurement Policy Framework Act 2 of 2000 (PPPFA) and its Regulations which regulate preferential procurement by providing a framework in terms of which preferential procurement policies must be implemented. At national and provincial government level, the Public Finance Management Act 1 of 1999 (PFMA) and its Regulations do not regulate public procurement directly, but rather public finance in general and therefore public sector procurement. At local government level, the Local Government: Municipal Finance Management Act 56 of 2003

(MFMA) with its Regulations and the Local Government: Municipal Systems Act 32 of 2000, manage public finance and thus public sector procurement. Various other acts influence public procurement in South Africa, including the Electronic Communications and Transactions Act.

3. Electronic reverse auctions

One of the traditional means of bidding, called the English Auction, takes place when bidders congregate in a determined location and call out their bids so that each bidder is aware of the offer made by others. A bidder may bid several times as reserve prices are continuously increased until only one bidder remains and no other bidders increase their bids. The remaining bidder is then declared the winner who may claim the item at the price he last bid. Electronic reverse auctions operate in the same manner, except that the value of the bids are revealed electronically and the prices of bids decrease instead of increase (Soudry 2004). A mathematical formula is used to examine bids and award points for various aspects of the bids.

The UNCITRAL Model Law requires that the procuring entity electronically publishes an invitation to tender. The invitation must reflect a detailed description of the subject matter of the procurement, the terms and conditions of the contract and the criteria and procedure for examination of the bids including the mathematical formula to be used. The invitation must further inform bidders whether any other component, other than price, such as quality or preference will be evaluated.

4. Advantages and disadvantages of electronic reverse auctions

Advantages

It has been noted that implementing e-procurement is potentially beneficial in ensuring a lower price for the goods procured and a more efficient public procurement process which results in reduced costs and time periods (de la Harpe 2012). It can further promote transparency in the requirement that bidders are actively involved in a “real-time” procurement process. They are therefore continuously informed of their competitors’ bids and what their prospects of success are. The latter may even contribute to reducing corruption within the process. The use of e-procurement may also reduce administration costs, procurement staff and improve communication through speedier access to information (Eadie, Perera, Heaney and Carlisle 2007).

Disadvantages

With e-procurement being a relatively new form of procuring goods and services, it has a number of barriers. Due to the fact that bids are evaluated based on mathematical formulae, e-procurement may be possible only when procuring contracts of a relatively small value and where it is possible to evaluate aspects of bids by means of mathematical formulae. There is the inherent danger that secondary aspects such as quality and socio-economic considerations may be given insufficient attention (de la Harpe 2012). Products may therefore be procured at a lower quality for the sake of a better price.

A further possible threat in an e-procurement process is that it may in fact increase collusion where there is only a small number of contractors who can provide the desired product or service. The possibility of an IT failure during the procurement process is a further reality which may lead to legal disputes regarding liability for a failed process or a tender incorrectly awarded. It has also been noted that a lack of technical expertise, knowledge and access to information technology may be limited in some companies, especially small, medium and micro enterprises (SMMEs). Furthermore, the lack of legal certainty underpinning e-procurement may be a further barrier to the successful implementation of eprocurement (Eadie, Perera, Heaney, Carlisle 2007).

5. Electronic reverse auctions in South Africa

The legislation regulating public procurement both directly and indirectly do not expressly preclude the use of e-procurement in South Africa. The Electronic Communications and Transactions Act 25 of 2002 specifically makes reference to e-government services in sections 27 and 28 of the Act in providing for acceptance and issuing of documents by a public body. It is also a goal of the Act to promote the use of e-government services and electronic transactions between private and public bodies. It would therefore appear that there is room for the legal regulation of e-procurement in South African public procurement legislation.

As previously indicated, section 217 of the Constitution requires that the government when contracting for goods and services should do so in accordance with a system which is fair, equitable, transparent, competitive and cost-effective. Fairness in this context refers to equal access to the process and procedurally fair evaluation of bids. In advertising contracts electronically on a website available or accessible to all potential bidders, the e-procurement process will ensure equal access to contract opportunities. The evaluation of bids by means of a mathematical formula excludes human interference, thereby ensuring that bidders are evaluated procedurally fairly.

Equality in the South African public procurement context refers to substantive equality. This means that contractors are evaluated against the backdrop of section 9 of our Constitution. In order to give effect to this section and the equality element in section 217 of the Constitution, contractors' socio-economic circumstances are considered when evaluating their bids. Contractors may therefore be treated differently in view of South Africa's past discriminatory practices (Bolton 2007).

Throughout the tender process, bidders will be aware of the competing bids and the contents thereof. However, the identity of bidders should not be revealed in order to maintain the integrity of the process and prevent collusion. All information necessary to participate in the process, the evaluation criteria and information regarding the outcome of the process and the reasons therefore must be made available to all bidders. The principle of transparency will therefore be complied with (Anthony 2013).

The UNCITRAL Model Law provides in Article 54(1)(j) that a minimum number of bidders should be indicated in the invitation to tender so as to ensure effective competition. This provision therefore ensures that the competition principle will be complied with as mandated by section of the South African Constitution.

E-procurement will go a long way in reducing administrative costs, and significantly decrease the quantity of paper involved in a procurement process. It is designed to be faster than a paper-based tender process, thereby aiming to achieve best value for money. Eprocurement will therefore promote cost-effectiveness in compliance with section 217 of the Constitution.

6. Conclusion

Regulating e-procurement by means of legislation will go a long way in not only ensuring legal certainty, but also ensure that transparency and competition are promoted. E-procurement will further ensure that a cost-effective process is followed and that best value for money is therefore achieved.

It is important that the legislation enacted to regulate e-procurement gives effect to section 217 of the Constitution. On a cursory analysis, the UNCITRAL Model Law regulations on e-procurement comply with an e-procurement system which is fair, transparent, competitive and cost-effective. South Africa will thus benefit from a system similar to that in the UNCITRAL Model Law. The element of equity being unique to South Africa can be given effect to by providing greater access to SMMEs. The relevant training in information technology, institutional support within corporate bodies and innovative methods to convert equity aspects in bids to mathematical formulae will ensure that the element is complied with.

The use of e-procurement holds many benefits for the South African economy. It will further assist in increasing South Africa's contribution to environmental considerations and sustainable development. Furthermore, an inevitable decrease in human intervention in the e-procurement process will curb corruption and ensure that bidders are treated fairly. Although barriers to successful implementation of e-procurement exist, South Africa can benefit from the advantages offered by an e-procurement system and increase the country's global competitive market.

7. References

Anthony, A (2013) The legal regulation of construction procurement in South Africa LLM Thesis Stellenbosch University

Audet, D (2002) Government Procurement: A synthesis report 2 OECD Journal on Budgeting 1 180

Bolton, P (2007) The Law of Government Procurement in South Africa

de la Harpe, S (2012) The Use of Electronic reverse auctions in Public Procurement in South Africa Speculum Juris 21-37

Eadie, R., Perera, S, Heaney, G., Carlisle, J (2007) Drivers and barriers to public sector e-procurement within Northern Ireland's construction industry ITcon 12 103-120

Soudry, O (2004) Promoting Economy: Electronic reverse auctions under the EC Directives on Public Procurement Journal of Public Procurement 4(3) 340-374.

MFMA Municipal Supply Chain Management Regulations GN R868 in GG 27636 of 30-05-2005

PFMA Public-Private Partnership Treasury Regulation 16 GN R1737 in GG 25773 of 28-11-2003

PFMA Supply Chain Management Treasury Regulation 16A GN

R225 in GG 27388 of 15-03-2005

GN R502 in GG 34350 of 08-06-2011

The Cybercrime Landscape: The Human Threat Vector Taxonomy

I.Govender[1] & B.W Watson[2]
[1]Department of Mathematical Sciences, Stellenbosch University
ieg@sun.ac.za
[2]Department of Information Science, Stellenbosch University
bwwatson@sun.ac.za

Abstract

The literature on information systems (IS) security and the media alike highlight the grave concern for IS security breaches that permeates organisations. The key question this article examines is: What are the current threats to IS security in the context of a security human threat vector taxonomy? The risk factor in the context of organisational IT security is a function of the likelihood of a threat exercising a particular potential vulnerability, and the severity of its impact on the organisation. In order to implement security measures to safeguard the organisation's information systems, it is imperative to identify and understand the cyber threats 'out there' together with the vulnerabilities in the organisational IT systems. This is of relevance, to subsequently identify and implement the appropriate security controls for risk mitigation. This article contributes to praxis by exploring the recent key IS security threat patterns in organisations against a threat vector taxonomy, focussing on the human threat actors; both internal and external. This threat taxonomy that delineates the cyber-crime landscape, in conjunction with the current security threats/breaches, could serve to inform management in reviewing their risk management programme. Moreover, safeguards/security controls are recommended for specific security breaches.

Keywords

Cyber threat, breaches, insider attack, malware

1. Introduction

The literature on information systems (IS) security and the media alike highlight the grave concern for IS security threats and breaches that permeates organisations. Various studies in industry and surveys indicate that IS security continues to be one of the top managerial concerns (Willison & Warkentin 2013; Brenner 2009; CSI 2011; Deloitte 2010; Ernst & Young 2009). An increase in budgets for IS security depicts a peculiar relationship with an upward trend in computer crimes (CSI 2011). The World Economic Forum has established cyber-attacks as a global risk (The Global Information Risk Report, 2013). Choo (2011) asserts that "It is evident that cyber threats are seen as one of the top issues in crime and national security today, and an increasingly challenging policy area for governments - Cyber space is the new front line". Security practitioners anticipate a rife of more sophisticated security attacks in the not too distant future (Kisekka, 2015). Security threats to an organisation come in all shapes and sizes requiring a comprehensive approach of both, technical and behavioural controls (The human factor 2015: A Proofpoint research report, 2015).

Organisations are realising that cybersecurity has become a persistent, all-encompassing business risk. The risk factor in the context of organisational IS security is a function of the likelihood of a threat exercising a particular potential vulnerability, and the severity of its impact on the organization. In order to implement security measures to safeguard the organisation's information systems, it is imperative to identify and understand the cyber threats 'out there' together with the vulnerabilities in the organisational IS. This article progresses as follows; the next section elaborates on the threat vector taxonomy which then leads to the current major security threats/breaches as identified by international studies, focussing on the human factor, inside and outside of organisations. Concluding remarks are then stated.

2. IS Security Threat Vector Taxonomy

In an attempt to address the cyber-crime landscape, this article adopts Willison's and Warkentin's (2013) IS Security Threat Vector Taxonomy that delineates threats into two overarching categories i.e. external and internal threats (Figure 1). Warkentin and Johnston (2008) argued that it is incumbent for IS security managers to identify and mitigate a wide range of threats, which may originate from sources that are within the organisation itself (internal) or from external entities, and they may include human perpetrators or nonhuman phenomena (Loch et al. 1992). This article responds to this call by examining the recent key IT security threats/breaches in organisations as reflected in studies conducted by information security practitioners. Framing the recent significant threats/breaches occurrences against a Security Threat Vector Taxonomy, aligned with recommended security measures, could inform IS security managers in addressing their IT security programme. It could guide their risk management agenda, providing insight in the context of current threats and vulnerabilities. The focus of this study is on the human threat actors (both external and internal) and not the nonhuman factors.

Willison and Warkentin (2013) extended the Loch et al. (1992) threat taxonomy to include greater granularity, especially for the "insider threat" (Figure 1). Insiders are current employees who have access privileges and intimate knowledge of internal organisational processes that facilitates exploiting weaknesses. The current employee threat actors fall along a three level continuum as indicated by Willison and Warkentin (2013) in Figure 1 i.e. passive and non-volitional noncompliance, Volitional (but non malicious) noncompliance and the intentional malicious computer abuse employee, which is elaborated on later. This article further extends

Willison & Warkentin's (2013) threat taxonomy by incorporating 'other insiders' as another aspect of the internal human factor which addresses threats by former employees and the 'Quasi insider' which is elaborated on later.

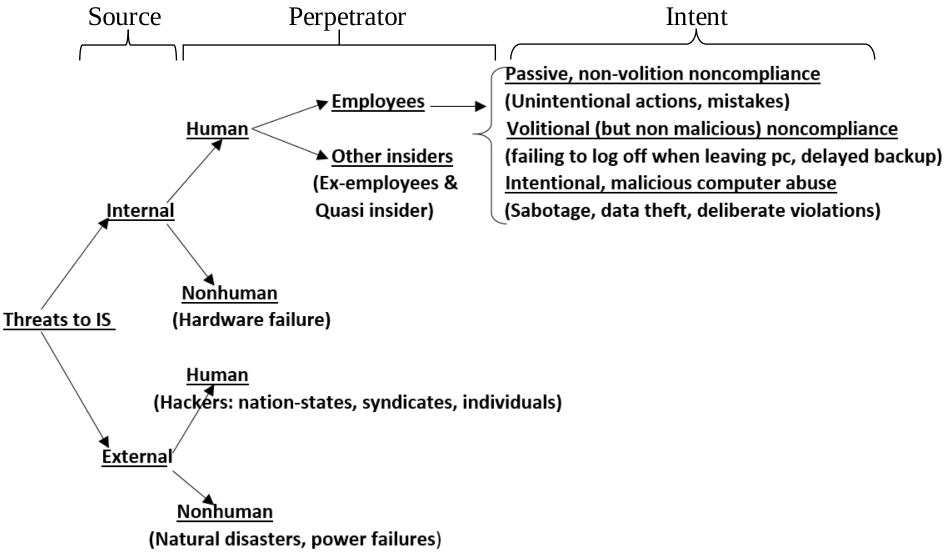
Source
Perpetrator
Intent
Threats to IS
Internal
Human
Employees
Other insiders
(Ex-employees &
Quasi insider)
Nonhuman
(Hardware failure)
External
Human
(Hackers: nation-states, syndicates, individuals)
Nonhuman
(Natural disasters, power failures)
Passive, non-volition noncompliance
(Unintentional actions, mistakes)
Volitional (but non malicious) noncompliance
(failing to log off when leaving pc, delayed backup)
Intentional, malicious computer abuse
(Sabotage, data theft, deliberate violations)

Figure 1: IS Security Threat Vector Taxonomy (adapted from Willison and Warkentin, 2013)

3. Research Approach

Recent large scale studies of IS security threats and breaches are examined against the threat taxonomy (Figure 1) in an attempt to inform IS security practitioners in addressing their organisational risk management agenda. A narrative review of the literature on security breaches from a practitioner perspective is used to summarise key findings from three major primary studies (Campbell, 2006). This article draws from these studies which were conducted by internationally established entities in the domain of IT security. Amongst the studies that were examined, a key study was the "Data Breach Investigations Report of 2015" (DBIR, 2015). The DBIR (2015) was compiled by Verizon, an international communications and technology company, together with the contribution of about seventy organisations, inclusive of forensics firms, Computer Security Information Response Teams (CSIRTs), government agencies etc. They examined 80,000 security incidents and more than 2,000 data compromises from 61 countries. Some regard it as the Data Breach Bible, due to its comprehensive examination of thousands of confirmed data breaches and security incidents from around the globe (Santillan, 2015). Another study that was reviewed was the "IBM X-Force Threat Intelligence Quarterly 2Q, 2015". The IBM X-Force research and development team f ocuses on security threats, highlighting the insider threats and examines ways to mitigate risks. Over the years, IBM X-Force has reported on a sampling of security incidents to understand trends and key events. The third key study that was reviewed is the "Global State of Information Security Survey 2015"; a worldwide study on information security coordinated by Pricewater House Coopers (PwC); an international consulting company. The results discussed in the PwC survey are based on responses of more than 9,700 company executives and directors of IT and security practices from more than 154 countries. This article examines these security threat/breach studies, amongst other security related studies, against the threat taxonomy (Figure 1) but only focussing on the human perpetrators from both the external and internal sources of IS threats.

4. External Human Threat: (Hackers, Espionage)

There are diverse motives for the external attack into the information systems of organisations. A study conducted by McAfee found cyber-attacks and network infiltrations that appear to be linked to nation-states and political goals (McAfee, 2009). The report states that although there has not been a full blown cyber war between major powers, the efforts of nation-states to build increasingly sophisticated cyber-attack capabilities suggests that a "CyberColdWar" may not be too remote. The report cited Distributed Denial of Service (DDoS) attacks targeting websites belonging to the U.S. government and intelligence agencies, South Korean government agencies, and Estonia government agencies. In 2014, the political conflicts between Russia and Ukraine resulted in widespread cyber-attacks between the two nations; defacing government websites on both sides of the conflict, as well as malware transmission.

The Global State of Information Security Survey (2015) reflects a concerning increase in nation-state attacks; seeking intellectual property (IP), blueprints, Mergers & Acquisition data, and Research & Development resources. Furthermore, the magnitude of attacks by organized crime syndicates also appears to be at an all-time high, with sophisticated levels of organisation and infrastructure of these syndicates. The survey found an 86% increase in respondents who say they have been compromised by nation-states. Given the ability of nation-state adversaries to carry out attacks without detection, the survey indicates that the volume of compromises is very likely under-reported. DDoS attacks and the use of sophisticated espionage spyware were found to be commonplace.

In the context of nation-state attacks, another striking finding of the Global State of Information Security Survey (2015) was the 64% increase in security compromises attributed to competitors where there was a strong possibility of nation-state backing. This was peculiar to Asia Pacific and more especially China. Respondents of the survey from China blamed competitors as the source of security incidents. For the first time, the US Department of Justice charged five Chinese military hackers for conducting cyber economic espionage against American companies in the nuclear power, metals, and solar energy sectors. Symantec, an antivirus corporation, unveiled attacks against major European governments. Due to the chosen targets and sophisticated malware employed, Symantec believes a state-sponsored group is responsible for the attacks. The survey study found that Critical Infrastructure of nations have also been targeted with the motive being theft of IP and trade secrets as a means to advance political and economic advantages. Sophisticated state-backed cyber adversaries used complex malware to infect the industrial control systems of hundreds of energy companies across the United States and Europe (The Global State of Information Security Survey, 2015). Nation-state security breaches were more frequent among sectors such as oil and gas, aerospace and defence, technology, and telecommunications entities. The 2015 Data Breaches Investigation Report identifies the manufacturing, public and professional sectors as the targets of choice for cyber espionage.

Phishing, as a social engineering approach for cyber-crimes, is commonplace to initiate cyber-attacks. Phishing is generally defined as online scams using unsolicited messages claiming to originate from authentic entities, such as banking and finance services (Choo, 2011). They deceive victims into disclosing their financial and/or Personal Identity Information (PII) to commit or facilitate other crimes (e.g. fraud, identity theft and theft of sensitive information). Phishing has come a long way since the early "phishing" campaigns that initiated an e-mail that appeared to be coming from a bank convincing users to change their passwords or provide sensitive information. Users were led to a fake web page and user's willingness to fix a non-existent problem led to account takeovers and fraudulent transactions. The 2015 Data Breach Investigators Report found Incidents within the pattern of Cyber-Espionage incorporates social attacks, especially using phishing carrying malware as the first step to infiltrate the organisation. Although the vector of malware installation is mostly through phishing, it was executed between either email attachments or links. For this type of incident, The 2015 Data Breach Investigators Report recommends: **"**start amassing e-mail transaction logs (in general), records of attachments, and records of links in e-mails. Log all DNS web-proxy requests and invest in solutions that will help you ingest and analyse this data both on the fly and forensically. Even if you don't manage to detect or deter these adversaries, you will at least have a much easier time figuring out what they did after the fact" (DBIR, 2015)**.** This report found that malware installed through web drive-by is also gaining momentum. The report asserts that if a state-sponsored adversary wants your data, they have a good chance of successfully infiltrating your organisation, unless another state-sponsored entity helps you defend it. Choo (2011) argue that irrespective whether a government or corporate comes under cyber-attack, it may not be immediately apparent whether the threat actor is a skilful teenager, an organised cyber-crime group, or a nation state. They advance that identifying the threat actor facilitates the appropriate response to each of the threats, determining the rules of engagement.

The Data Breach Investigations Report of 2015 asserts that organized crime was the key threat actor for Web App Attacks, with financial gain as the primary motive for the attacks. They use a Strategic 'Web Comprise approach' to first target web servers as a first step to set up an attack on a different target. The attack involves setting up an exploit (malware) in the selected website. Once targeted victims visit the compromised site, the exploit takes advantage of software vulnerabilities to drop malware. The dropped malware may be in the form of a remote access Trojan (RAT), which allows attackers to access sensitive data and take control of the vulnerable system. Cross-site scripting and SQL injection (SQLi) are also still prevalent in web app attacks (DBIR, 2015). This report asserts that Point-of-Sale (POS) Intrusions take pole position regarding the type of threat patterns. The combination of Internet-facing POS devices and default passwords made compromise trivial for attackers. POS attacks have evolved over the years, from simple storage scraping to active RAM skimming across all breach types. The industry sector most affected were accommodation, entertainment and retail sectors. Sophisticated breaches in larger organisations entailed a multi-step attack with some secondary system being breached before attacking the POS system. In the year 2014, several incidences emerged where vendors providing POS services were the source of the compromise, such that vendors had keyloggers installed through successful phishing campaigns or network penetrations. All breached POS vendors ended up with their remote access credentials compromised, inviting attackers into customer environments where the card harvesting began. The report asserts that monitoring tools for the POS environment is imperative to counteract these breaches (DBIR, 2015)

Malware is part of the event chain in most incidences of security breaches (DBIR, 2015). Malware was found to invade information systems, usurp existing functionality and showcase their destructive patterns as per their design. Choo (2011) categories malware into two broad categories i.e. generic malware that targets the general population and customised malware targeting specific institutions. Spam with malicious attachments provides one way to get malware into company networks and onto users' computers. Bot malware is a type of generic malware that is hosted on web servers by exploiting vulnerabilities of the specific server. Any user who visits these websites and whose operating system and internet browser is not updated with the latest patches, is likely to be infected with the bot malware, a process referred to as "drive-by attack". Machines infected with the bot malware can be directed to launch cyber attacks such as DDoS attacks, sending out spam and more malware, initiating phishing and click fraud, and hosting illegal child pornography (Choo, 2007). This category of malware is predominantly opportunistic in nature but there can also be financial motives (DBIR, 2015). Choo (2011) defines the phishing-based keylogger as an example of a customised malware that targets specific organisations. This malware misleads its victims into opening harmful attachments or visiting malicious websites, facilitating the installation of further malware such as the Zeus malware. The malware program is designed to harvest account numbers, login credentials and personal information which is relayed to a compromised server in waiting. Specialized classification patterns such as Cyber-Espionage pattern that requires maintaining persistence and Point-of-Sale Intrusions that involves capturing and exfiltrating data are the workings of customised malware. The (DBIR, 2015) states that criminals have become wise to the signature-and hash-matching techniques used by antivirus products to detect malware. Consequently, cyber criminals that design these malware use many techniques that introduce simple modifications into the code so that the hash is unique, yet it exhibits the same desired destructive behaviour. Therefore there are often millions of ‘different’ samples of the ‘same’ malicious program (DBIR, 2015).

The ‘IBM X-Force Threat Intelligence Quarterly, 2Q 2015’ found that another invasion of the network by another type of malware called ransomware that increased in 2014, poses a significant risk. Ransomware attacks varied, with one type extorting businesses to pay a fee to avoid a DDoS attack or public leak of data. Business websites were notified that they would be targeted by a DDoS attack unless they paid a ransom ranging from a few hundred dollars to several thousand dollars. Another type of attack is the crypto-ransom scheme, where attackers encrypt and lock out users from their own data, computers or mobile devices. They then demand a payment, usually in Bitcoin, in return for the unlock key (IBM X Force, 2Q 2015).

5. Internal Human Threat: (Insider Attack)

Johnstone et. al (2015) assert that organisations continue with the challenge of enforcing policies designed to protect assets from intentional or accidental information security violations by an organisation’s insiders (D’Arcy et al. 2009; Puhakainen and Siponen 2010). The 2014 US State of Cybercrime Survey found almost 32% of respondents revealing that the insider is more costly and damaging than incidents perpetrated by outsiders. Nevertheless, many companies are found wanting regarding an insider-threat program in place, and are consequently ill prepared to prevent, detect, and respond to internal threats. The IBM X-Force Threat Intelligence Quarterly 2Q, (2015) study findings reveal cases of former employees that create a “back door” before leaving the organisation. This “back door” can be activated once the ex-employee leaves the organisation or upon arrival at a new place of employment, providing outside access to hidden accounts or sensitive data. The study recommends a recurring process to review access logs and network activity to be on the ‘look out’ for these back doors or any other peculiar behaviour; inclusive of investing in automated monitoring services.

The first type of insider attack (The passive non-volitional noncompliance with ISP) in Figure 1, relates to unintentional mistakes, misunderstandings, and poor judgment which are bound to occur in the workplace. Acts such as accidental entry of incorrect data and actions of employees who are simply careless, sloppy, unmotivated, or poorly trained (Willison and Warkentin 2013) fall into this category on the continuum (Figure 1). A simple incident such as employees who forget to consistently comply with a clean desk policy, place corporate information at risk; even though the risk is accidental (Mutchler and Warkentin, 2015). The initial threat from accidents or oversights by careless or unmotivated employees, can be the precursor to more extreme incidents (Willison and Warkentin 2013). This kind of practice sets up the next phase to be exploited by the quasi insider which is discussed later.

In the context of the second and third types of insider attacks (Figure 1), convenience and financial gain were found to be key motivators (DBIR, 2015). The second type of insider threat on the continuum (Figure 1) are volitional (but non malicious) noncompliance by employees. This includes individuals who delay making data backups, fail to shred sensitive documents, fail to encrypt data before transmitting it, or fail to select strong passwords (Willison and Warkentin 2013). They knowingly violate security policies, but not with the intent of malicious harm. This type of insider is usually accentuated by the motive of convenience, where an unapproved workaround to speed things up or make it easier for the end user (DBIR, 2015). Although there’s no deliberate intention to harm the organisation, it can often lead to increasing the vulnerability of the organisation (DBIR, 2015). The third level on the continuum is the intentional, malicious computer abuse (Figure 1) by insiders. Intentional malicious abuse involves data manipulation or destruction, data theft, fraud, blackmail, or embezzlement. Insiders may also steal credit card numbers, may sell intellectual property to competitors, or may disclose sensitive, classified, or protected information to the public or to enemies of the state (Willison and Warkentin 2013).

The IBM X-Force Threat Intelligence Quarterly 2Q, (2015) report states even employees with the best of intentions, can inadvertently aid in an attack by clicking on a malicious link sent in a phishing email. To counteract this, the organisation needs to recognize the danger of malware distributed by spam and take steps to block it. Security Education, Training, and Awareness (SETA) is a common behavioural control to ensure every user is on constant alert and aware that even the most innocent action can open the door for an attack. To prevent this from happening, the organisation’s security team needs to recognize the danger of malware distributed by spam and implement the essential technical safeguards. In the context of behavioural safeguards, instructional programs are the typical controls applied to protect against unwarranted employee behaviors, including Information security policy compliance behaviors (Mutchler and Warkentin, 2015). The instructional program of preference by organisations to facilitate employees comply with the ISP is SETA (Mutchler and Warkentin, 2015).

Mutchler and Warkentin (2015) argue that especially the Awareness component of SETA often focuses on repetition of the information as a reminder for employees of the persisting security issues. They state that these Awareness programs have been often ineffective. They attribute this to the gap between understanding the instruction provided and performing the secure behaviors (Wombat Security Technologies). Mutchler and Warkentin (2015) advocate 'experience' as a pivotal factor to close the gap between the instruction and behaviour. They take heed of the recommendation by social engineering expert Stanganelli, (2013) who recommends adding direct experience to an instruction program because it can greatly improve the outcomes of instruction. Stanganelli, (2013) asserts that phishing awareness instruction that is combined with the direct experience of an internally controlled phishing occurrence is more effective and has been shown to reduce future successful phishing attacks by more than 75%. Consequently, penetration testers are using controlled attacks so that network staff have encounters with direct experiences of a hack which consolidates security instruction awareness programmes (Northcutt et al. 2006).

6. Quasi Insider

Besides vulnerable entries to a company's website or web servers, entities need to also focus on controlling other points of entry that might be open to franchisers, contractors or partners. This is inclusive of contract workers, electricians, construction workers, phone or other type of repair personnel who have access to the physical location or have access to networks; enabling tampering of systems and access to organisational resources. The Quasi insider refers to these third parties or parties that are associated with the organisation and have various modes of access to the organisation and its assets. A vulnerability often overlooked is paper copiers and fax machines which equipped with some type of memory or hard drive and are often connected to an internal network. Repair technicians with the relevant technical 'know how', can access these storage devices; furthermore, the storage device can also be accessed through the network. The Global State of Information Security survey highlight the lack of policies and due diligence regarding third parties, considering that third-party vendors are a significant source of cyber risk. This survey recommends that organisations anchor their third-party due diligence on three key practices: "Perform appropriate protections of vendors to ensure that they have the ability to safeguard the information, have robust contractual protection, and conduct ongoing monitoring to ensure the third party is protecting the data". It is in their own interest for corporates to take responsibility for their organisational data, more especially the personal information of customers, clients and employees, considering that data privacy regulations have become more stringent in this regard.

7. Conclusion

The purpose of this paper was to extend the 'security threat vector taxonomy' with the 'other insider' and examine the cybercrime landscape but limited to the human factor. This taxonomy framework depicts the 'threat source', 'perpetrators' and their motives. To this end, the current studies conducted by the major players in IS security were surveyed. This paper proceeds to delineate the key security threats/breaches uncovered in those studies onto the 'security threat vector taxonomy'. Moreover, mitigating measures for specific security threats/breaches are proposed. This could inform IS security practitioners, offering more insight of the mapping of the cybercrime terrain. This could contribute to their risk management and IS security programme by reviewing their safeguard measures and security controls.

8. References

2015 Information Security Breaches Survey. HM Government, https://www.gov.uk/government/publications/information-security-breaches-survey-2015 2015 [Date last accessed: 01.07.15].

Brenner, B. 2009. Why Security Matters Again, The Global State of Information Security, Joint Annual Report, PricewaterhouseCoopers (with CSO Magazine).

Campbell Collaboration (2006). Systematic Reviews in social sciences. A presentation on February 7, 2006.

Choo, K.R. 2011. The cyber threat landscape: Challenges and future research directions. Computers & Security. (30:2011) pp. 719-731.

CSI. 2011. "2010/2011 CSI Computer Crime and Security Survey," Computer Security Institute.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

DBIR, 2015. 2015 Data Breach Investigations Report, Verizon, http://www.verizonenterprise.com/DBIR/2015/; 2015 [Date last accessed: 01.07.15].

Ernst & Young. 2009. "Outpacing Change: Ernst & Young's 12th Annual Global Information Security Survey."

IBM X-Force Threat Intelligence Quarterly, 1Q 2015. Somers, NY: IBM Corporation

IBM X-Force Threat Intelligence Quarterly, 2Q 2015. Somers, NY: IBM Corporation

Johnstone, A.C., Warkentin, M. and Siponen, M. 2015. An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric. MIS Quarterly. (39:1) pp. 113-134.

Kisekka, V. Investigating Information Security Effectiveness after an Extreme Event, 2015, 10th Annual Symposium on Information Assurance (ASIA '15).

Loch, K.D., H.H. Carr, and M.E. Warkentin. "Threats to information systems: today's reality, yesterday's understanding." *Mis Quarterly* (1992): 173-186.

McAfee. Virtual criminology report 2009: virtually here: the age of cyber warfare. Santa Clara, CA: McAfee 2009, Inc; 2009

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757-778.

Santillan, M. Tripwire http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/takeaways-from-the-2015-verizon-data-breach-investigations-report/ 2015 [Date last accessed: 01.07.15].

The Global Information Risk Report. available at www.weforum.org/reports, Retrieved January 5, 2013.

The Global State of Information Security Survey, PWC, 2015 http://www.pwc.com/gsiss2015; [Date last accessed: 01.07.15].

The human factor 2015: A Proofpoint research report, 2015. [Online], Available: https://www.proofpoint.com/, [May 9, 2015].

Wang, J., Gupta, M. and Rao, H.R. 2015. Insider Threats in a Final Institution: Analysis of Attack-Proneness of Information Systems Applications. MIS Quarterly (39:1) pp. 91-112

Warkentin, M., and Johnston, A. C. 2008. "IT Governance and Organizational Development for Security Management," in Information Security Policies and Practices, D. Straub, S. Goodman and R. L. Baskerville (eds.), Armonk, NY: M. E. Sharpe, pp. 46-68.

Warkentin, M. and Siponen, M. 2015. Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications.

Willison, R. and Warkentin, M. 2013. Beyond Deterrence: An Expanded View Of Employee Computer Abuse. MIS Quarterly. (37:1) pp. 1-20

"I Am Because We Are": Developing and Nurturing an African Digital Security Culture

Karen Renaud[1], Stephen Flowerday[2], Lotfi ben Othmane[3], Melanie Volkamer[4,5]

[1]University of Glasgow, [2]University of Fort Hare, [3]Fraunhofer Institute for Secure Information Technology, [4]Technische Universität Darmstadt, [5]Karlstad University
karen.renaud@glasgow.ac.uk; sflowerday@ufh.ac.za; lotfiben.othmane@cased.de; melanie.volkamer@cased.de

Abstract

Technical solutions fail if people experience difficulties using them. Sometimes these difficulties force people to work around the security solutions in order to achieve legitimate goals. Improving usability undoubtedly helps, but this has not improved the situation as much as anticipated. In this paper we consider a variety of other reasons for non-uptake.

We argue that this situation can only be addressed by considering the person as a member of the wider community and not as a solitary agent. This aligns with the traditional African wisdom of Ubuntu: "I am because we are". We propose improving the African Digital Security Culture (ADSC): collective knowledge, common practices, and intuitive common security and privacy behaviour, in a particular society. We suggest a set of approaches for developing and sustaining ADSC in a society, for as members of a society we learn most effectively from each other, not from books, the media or by carrying out searches using search engines.

Keywords

Society; Information Security; Ubuntu

1. Introduction

The African philosophy of Ubuntu is considered to reflect the belief in a universal bond of sharing that connects all humanity. Nafukho (2006) explains that 'in traditional African society adult learning was viewed as holistic learning for life and work and formed the foundation of many African societies' (p. 408). He explains that this has lapsed somewhat, meaning that adult learning is not supported as much as it used to be, under the Ubuntu paradigm. In this paper we will argue that a resurgence of the Ubuntu mindset presents us with an opportunity to improve African resilience to online threats.

Sub-Saharan Africa has experienced a growth in mobile telephony that dwarfs the developed world. Aker & Mbiti (2010) explain that whereas only a quarter of the population has electricity, 60% of the population has mobile coverage. These figures are slightly higher in South Africa where 85% of the population has access to electricity and 95% has mobile phone coverage (Stats SA, 2013). With the increasing diffusion of smartphones and mobile Internet use (Goldstuck, 2012) comes an increasing vulnerability to attacks from cyber criminals worldwide. Dlamini et al. (2009) review the threats facing smartphone users, and argue that the human element is the real security challenge. Whereas a lot of effort has gone into helping companies secure their assets, personal security has not received as much attention, leaving the man and woman in the street vulnerable. According to Kritzinger & Von Solms (2010), 95% of Internet attacks involve targeting humans, not company IT systems directly. People need to be able to protect their data against unauthorized access, destruction, disclosure, and modification.

This is a position paper, presenting a literature review and concepts in order to propose a new way of making people less vulnerable, trying to improve uptake of security precautions and security software. We argue for considering society as a whole, and the role of influencers within a society, to develop individual resilience to security threats. We believe that we ought to borrow from the existing Ubuntu mindset to improve societal information security to nurture an African Digital Security Culture.

2. Poor Uptake of Security Mechanisms

Poor usability has been blamed for the meagre uptake of security products (Adams & Sasse, 1999). Yet there are other barriers to adoption too, such as those mentioned by Renaud et al. (2014), Harbach et al. (2013), Harbach et al., (2014) and Weirich & Sasse (2001). In the Sub-Saharan context there are additional location-specific obstacles (Prinsloo & Brier, 1996; Sayed & De Jager, 2014). Figure 1 depicts a nonexhaustive list of the barriers to adoption identified by researchers.

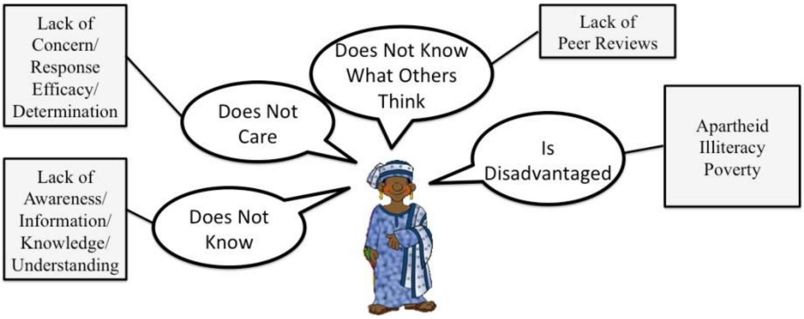
Lack of Concern/ Response Efficacy/ Determination
Does Not Know What Others Think
Lack of Peer Reviews
Does Not Care
Is Disadvantaged
Apartheid Illiteracy Poverty
Lack of Awareness/ Information/ Knowledge/ Understanding
Does Not Know

Figure 1: Barriers to Adoption of Security Precautions

To mitigate these barriers we need first to understand how to reach all South Africans, and then how to nurture a society where the idea of an African Digital Security Culture can be facilitated and encouraged. As mentioned before, we believe that we can nurture this culture more effectively where the Ubuntu mindset exists, since there is already a culture of adult education and community members helping each other. If we can piggy-back onto this existing mindset we might be able to help people to become more resilient.

3. Reaching Everyone; Improving Resilience

People need to know that they have an information need, be aware that there is something that they do not know, and be motivated to seek out information about a particular topic (information seeking). The former is awareness: something or someone making a person aware of something they knew nothing about before. Awareness has the potential to create a sense of an information need.

Having become aware of an information need, they might engage in information seeking. Case (2012) explains that information-seeking behaviour varies widely across people, situations and objects of interest so that it is difficult to predict how a particular person will go about seeking information.

It seems intuitive that people, having realised a need, will deliberately seek information from formal sources. Intuition is wrong in this case. In the first place it seems that information is gathered in passing, without the person even seeking it out (Babin et al., 2010). The literature suggests that much of what constitutes ‘everyday knowledge’ comes from our interactions with other people within our society (Bruner, 1990), not as a consequence of deliberate information seeking.

If people do deliberately seek out information it seems that they prefer to obtain information from friends and family (Case, 2012; Babin et al., 2010). There is a widespread myth that media has a significant impact on the public's thoughts, feelings and actions (Stansberry, 2012). Comstock (2013) reviews a number of studies providing strong evidence that public media has a negligible impact on the hearts and minds of the public.

The next place we might intuitively think people satisfy their need for information would be by using a search engine such as Google. Much research has focused on how search engines are used, but two studies have contrasted the use of search engines and other information channels. Gray et al. (2005) studied health-seeking information behaviour during adolescence. They discovered that participants considered the Internet their primary source, but they also acknowledge that it is unlikely to supplant trusted peers and adults. Morris et al. (2010) compared the use of a search engine with querying social networks and found that the social network delivered results more quickly than a search engine.

So, there are at least two phases: awareness followed by information gathering, the latter of which can be deliberate or vicarious. There is also another phase: sharing what you know. Kuhlthau (1991) found evidence that new knowledge and understanding leads to people sharing their information with others. The role of society seems to be crucial: people learn from others and, in turn, teach others.

This is a brief review but even so it seems clear that humans are hardwired to share information and to benefit from such sharing. In essence, we learn most effectively from each other, not from books, the media, or by carrying out searches using search engines.

Case (2012) argues that too little research has focused on sharing of information between peers, and the fact that humans often avoid and ignore relevant information. Yet a literature review of peer-related security support does indeed show that many eminent researchers have started looking at this aspect of security. Rader et al. (2012) carried out a study to investigate how non-experts learn about security, and argue for the crucial role of the stories people tell each other in educating people about security. Ashenden & Lawrence (2013) also argue for a social marketing approach to achieve behavioural change, and Lipford & Zurko (2012) argue strongly for a social approach to security. Finally, Camp (2011) argues that usage of security software might have a tipping point, where a herd effect leads to adoption by a group of people.

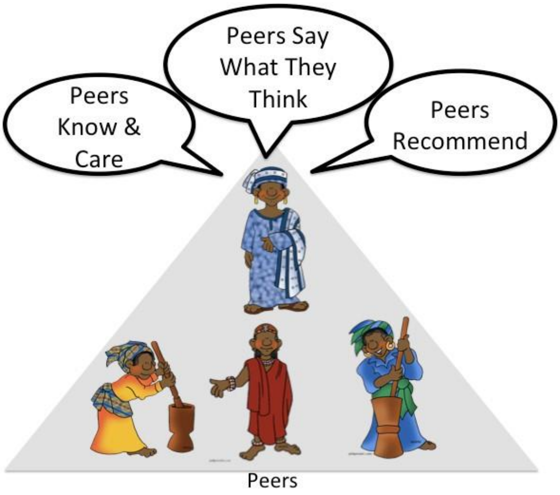

Figure 2: Societal Support

4. Nurturing an African Digital Security Culture

The key idea is that we should focus our efforts on building a security culture rather than focusing all efforts on reaching individuals. Very little effort has gone into helping the laymen and women with their digital security issues, either individually or by establishing an Ubuntu-like security assistance culture.

To address this obvious deficiency, an African Digital Security Culture (ADSC) for general society is proposed in order to ameliorate the risk impacts of security attacks that cannot be avoided purely by technical solutions, even if they are usable. This is because usability, on its own, does not guarantee adoption. By “society” we mean “The aggregate of people living together in a more or less ordered community” (Oxford English Dictionary). Establishing a healthy ADSC might well have the potential to address the various justifications that impair the uptake of usable security mechanisms by members of society.

There is, unfortunately, no simple way to reach everyone with awareness drives, especially those in rural areas who perhaps are not proficient in English. However, there are some things that can be done. We need to ensure that the community members support each other so that people are not grappling with security issues on their own. On the contrary, knowledgeable and experienced people could support others, gradually improving the societal digital security competence. This approach has been used successfully to support weight loss (Weight Watchers) and alcoholism (Alcoholics Anonymous).

This paper's contribution is to propose an approach, leaving the validation thereof to be pursued as future work. It is proposed that we focus our attempts on developing an ADSC in three phases, the first phase being calculated to initiate an interest in members of the society (start a revolution, excite an information need). Once people realise that there is something they do not know enough about, the second phase ensures that the information need thus created can be satisfied. We need to make it easy for a community's members to find the information they seek (to satisfy the information need we have created). During the second phase we ensure that peers can recommend a secure course of action. A third phase serves to monitor the efficacy of the approach and to feed back into a new iteration of phases one and two. We will now explain the proposed approach depicted in Figure 3.

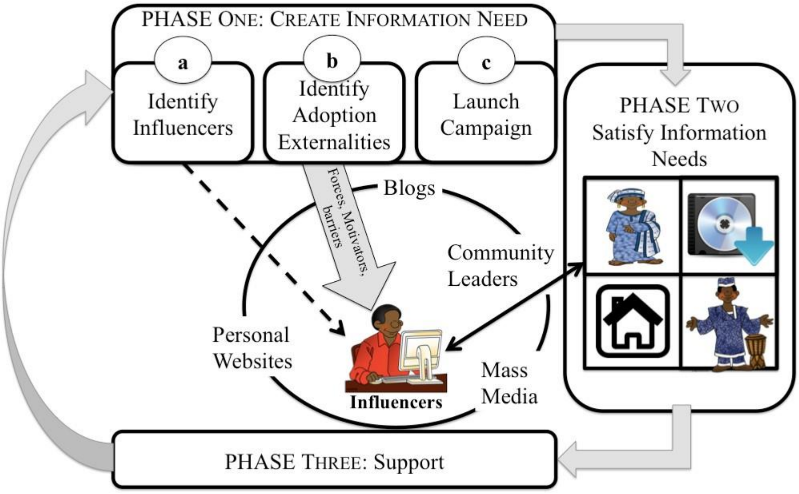
PHASE ONE: CREATE INFORMATION NEED
a
Identify Influencers
b
Identify Adoption Externalities
c
Launch Campaign
Forces, Motivators, barriers
Blogs
Community Leaders
Personal Websites
Mass Media
Influencers
PHASE TWO Satisfy Information Needs
PHASE THREE: Support

Figure 3: A Proposal for Building ADSC

Creating an Information Need (Phase One of the ADSC)

Our brief literature review made it clear that we ought not to be targeting individuals as a first step because they will not necessarily be convinced by outsiders coming in and offering advice.

The literature confirms that people learn most effectively from others in their own community. The usual approach is to provide information in the public media, make various Web resources available, or ensure that libraries stock informative pamphlets. While these sources of information may well come into play once an information need is experienced, it is necessary first for the information need to be registered, for curiosity to be piqued, within laypeople in a society. People in a given society inhabit different networks within which they choose to spend their time. It is here that we find key people who exert an influence over the other members of the societal network. These people are called influencers (Kiss & Bichler, 2008). The top criteria for an influencer's role in a community is their participation level, the frequency of activity and their prominence in the community (Gillin, 2008; Zhang, 2013). Donner et al. (2011) already experimented with the idea of training influencers in the community to use mobile Internet in South Africa.

After this, government-sponsored intermediaries should be made available to support the network because the way people are learning (isolated from expert knowledge) means that their knowledge is often fragmented and piecemeal. This, then, is what phase two addresses, by ensuring that experts and other information sources can play a role once influencers have initiated the process (Stansberry, 2012).

Phase one includes the following steps:

Identify the influencers in a particular community: Know the network, identify the influencers. Content of interaction is vital. The level of detail for the information is critical, so that influencers may give the right information to the people they influence.

Understand the forces, motivators and barriers to adoption: This will help to formulate adoption strategies or how future usage can align with current values and needs (Donner et al., 2011; Chakravorti, 2004).

Launch Campaign: We want to convince influencers of the benefits of the software solutions. This might need to happen face- to- face or via seminars. The aim is to ensure that they are as well informed as possible.

This exploits the theory of adoption externalities (Dybvig & Spatt, 1983). The idea is that you have to get enough influencers to start using a product so that it can diffuse through the community (Camp, 2011). This is particularly important for security products. Moreover, the training of influencers should be motivational and personcentred approach; something we learn from the drive to help people to stop smoking (Yuan et al., 2012).

Meeting the Information Need (Phase Two of the ADSC)

We need to satisfy the information needs excited in Phase one. Here we follow the advice of Donovan (2011) who considers the use of social marketing in promoting public health, a remotely related area to digital security. He proposes 4 P's: price, place, promotion and product, as follows:

People: Reaching people who currently do not have the knowledge and expertise to protect themselves. We do this initially via influencers.

Product: People are often flummoxed by the sheer range of products on offer. In a drive such as this one there should be a strong recommendation for one particular product. Moreover, such a product should offer simplicity and control to the adopters.

Place: Where should people go to seek information? Face- to- face word-of-mouth is the most effective route, so arranging community activities where this can take place would be a very effective launching pad to ensure that the campaign gets off to a strong start.

Politics: Target individuals who, even though they are not influencers, have the power to help people with the information need to satisfy their needs. Here people working in the community, such as librarians and teachers, can play a vital role in reaching people with vital information.

Support (Phase Three of the ADSC)

One cannot launch a campaign and then hope that it will continue without support. This is an essential component that will determine the success or failure of this security-related societal drive.

Phase three, the support phase, is grounded in the African philosophy of Ubuntu. Ubuntu, as explained by Eze (2005); Lutz (2009); Mabovula (2011) and Shutte (2009), embodies the “principle of caring for each other’s well-being and as a spirit of mutual support”. There is a collective community responsibility and Ubuntu is defined by some as “Your pain is my pain; My wealth is your wealth; Your salvation is my salvation”. Simply put: “I am because we are”. This phrase communicates a basic respect, compassion and support for others. The phrase “an injury to one is an injury to all” reinforces this community sentiment.

For developing and nurturing an African Digital Security Culture, the strengths of society and cultural philosophy, as a whole, need to be involved, supporting this initiative.

5. Conclusions

The use of pervasive computing systems, social networks, and public information systems exposes individuals to security risks. This paper discusses a number of reasons for the low uptake of usable security solutions collected from the literature.

The approach taken is that we deliberately act to complement usable technical solutions with ADSC: common understanding and attitude, collective knowledge, common practices, and intuitive common behaviour within societies. It also suggests an approach for developing and nurturing an African Digital Security Culture (ADSC) incorporating the Ubuntu philosophy. This work is a first step in motivating a need for focusing on an ADSC. Future work will include refining the approach for developing ADSC and the development of a coherent plan for deploying the approach.

Acknowledgements

This work was supported, in part, by the BMBF within EC SPRIDE, the Hessian LOEWE excellence initiative within CASED, a Fraunhofer Attract grant.

6. References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40-46.

Aker, J. C., & Mbiti, I. M. (2010). Mobile phones and economic development in Africa. Center for Global Development Working Paper, (211).

Babin, R., Grant, K., & Sawal, L. (2010). Identifying influencers in high school student ICT career choice. Information Systems Education Journal, 8(26), 1-18.

Bruner, J. (1990). Culture and human development: A new look. Human development, 33(6), 344-355.

Camp, L. J. (2011). Reconceptualizing the role of security user. Daedalus, 140(4), 93-107.

Case, D. O. (2012). Looking for information: A survey of research on information seeking, needs and behavior. Emerald Group Publishing.

Chakravorti, B. (2004). The role of adoption networks in the success of innovations: a strategic perspective. Technology in Society, 26(2), 469-482.

Comstock, G. (Ed.). (2013). Public communication and behavior (Vol. 2). Academic Press.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. Computers & Security, 28(3), 189-198.

Donner, J., Gitau, S., & Marsden, G. (2011). Exploring mobile-only Internet use: Results of a training study in urban South Africa. International Journal of Communication, 5, 24.

Donovan, R. J. (2011). The role for marketing in public health change programs. Australian Review of Public Affairs, 10(1), 23-40.

Dybvig, P. H. & Spatt, C. S. (1983). Adoption externalities as public goods. Journal of Public Economics, 20(2), 231–247.

Eze, M. O. (2005). Ubuntu: a communitarian response to liberal individualism? PhD dissertation, University of Pretoria, South Africa.

Gillin, P. (2008). New media, new influencers and implications for the public relations profession. Journal of New Communications Research, 2(2), 1-10.

Goldstuck, A. (2012). Internet matters: The quiet engine of the South African economy. World Wide Worx. Pinegowrie, South Africa. Available at: http://internetmatters. co. za/report/ZA_Internet_Matters. pdf (accessed 30 September 2012.

Gray, N. J., Klein, J. D., Noyce, P. R., Sesselberg, T. S., & Cantrill, J. A. (2005). Health information-seeking behaviour in adolescence: the place of the internet. Social science & medicine, 60(7), 1467-1478.

Harbach, M., Fahl, S., Rieger, M., & Smith, M. (2013, January). On the acceptance of privacy-preserving authentication technology: The curious case of national identity cards. In Privacy Enhancing Technologies (pp. 245-264). Springer Berlin Heidelberg.

Harbach, M., & Fahl, S. (2014). Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness. In Computer Security Foundations Symposium (CSF), 2014 IEEE 27th (pp. 97-110). IEEE.

Kiss, C., & Bichler, M. (2008). Identification of influencers—measuring influence in customer networks. Decision Support Systems, 46(1), 233-253.

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security, 29(8), 840-847.

Kuhlthau, C. C. (1991). Inside the search process: Information seeking from the user's perspective. JASIS, 42(5), 361-371.

Lipford, H. R., & Zurko, M. E. (2012, September). Someone to watch over me. In Proceedings of the 2012 workshop on New security paradigms (pp. 67-76). ACM.

Lutz, D. W. (2009). African Ubuntu philosophy and global management. Journal of Business Ethics, 84, 313-328.

Mabovula, N. N. (2011). The erosion of African communal values: a reappraisal of the African Ubutu philosophy. Journal of Humanities and Social Sciences, 3(1),

Morris, M. R., Teevan, J., & Panovich, K. (2010). A Comparison of Information Seeking Using Search Engines and Social Networks. ICWSM, 10, 23-26.

Nafukho, F. M. (2006). Ubuntu worldview: A traditional African view of adult learning in the workplace. Advances in Developing Human Resources, 8(3), 408-415.

Prinsloo, M., & Breier, M. (Eds.). (1996). The social uses of literacy: Theory and practice in contemporary South Africa (Vol. 4). John Benjamins Publishing.

Rader, E., Wash, R., & Brooks, B. (2012). Stories as informal lessons about security. In Proceedings of the Eighth Symposium on Usable Privacy and Security (p. 6). ACM.

Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn’t Jane protect her privacy? In Privacy Enhancing Technologies (pp. 244-262). Springer International Publishing.

Sayed, Y., & De Jager, K. (2014). Towards an investigation of information literacy in South African students. South African Journal of Libraries and Information Science, 65(1).

Shutte, A. (2009). Ubuntu as the African ethical vision. In M. F. Murove (ed.). African Ethics: An anthology of comparative and applied ethics. University of Kwazulu-Natal, press 85-99.

Stats SA (2013). General Household Survey – P0318. Pretoria: Statistics South Africa.

Stansberry, K. (2012). One-step, two-step, or multi-step flow: the role of influencers in information processing and dissemination in online, interest-based publics. Ph.D. dissertation, Journalism and Communication, University of Oregon, 2012.

Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: a first step towards effective password security in the real world. In Proceedings of the 2001 workshop on New security paradigms (pp. 137-143). ACM.

Yuan, N. P., Castaňeda, H, Nichter, M., Nichter, M, Wind, S, Carruth, L & Muramoto, M (2012). Lay health influencers how they tailor brief tobacco cessation interventions. Health Education & Behavior, 39(5), 544–554.

Zhang, Y., Li, X & Wang, T.-W. (2013). Identifying influencers in online social networks: The role of tie strength. International Journal of Intelligent Information Technologies (IJIIT), 9(1), 1–20.

Cyber Vulnerability Assessment: Case Study of Malawi and Tanzania

Stones Dalitso Chindipha1 and Barry Irwin2
Security and Networks Research Group, Department of Computer Science
Rhodes University, Grahamstown
South Africa
1g15c7469@campus.ru.ac.za
2b.irwin@ru.ac.za

Abstract

Much as the Internet is beneficial to our daily activities, with each passing day it also brings along with it information security concerns for the users be they at company or national level. Each year the number of Internet users keeps growing, particularly in Africa, and this means only one thing, more cyber-attacks. Governments have become a focal point of this data leakage problem making this a matter of national security. Looking at the current state of affairs, cyber-based incidents are more likely to increase in Africa, mainly due to the increased prevalence and affordability of broadband connectivity which is coupled with lack of online security awareness. A drop in the cost of broadband connection means more people will be able to afford Internet connectivity. With open Source Intelligence (OSINT), this paper aims to perform a vulnerability analysis for states in Eastern Africa building from prior research by Swart et al. which showed that there are vulnerabilities in the information systems, using the case of South Africa as an example. States in East Africa are to be considered as candidates, with the final decision being determined by access to suitable resources, and availability of information. A comparative analysis to assess the factors that affect the degree of security susceptibilities in various states will also be made and information security measures used by various governments to ascertain the extent of their contribution to this vulnerability will be assessed. This pilot study will be extended to other Southern and Eastern African states like Botswana, Kenya, Uganda and Namibia in future work.

Keywords

OSINT; Internet; security; cyber-warfare; infrastructure; vulnerability

1. Introduction

The 20th century saw a lot of innovations in as far as technological advancements are concerned. Among such innovations is the use of the Internet. This has come at a cost of information security risks ranging from a user level to national level and beyond (Calder, 2013). These risks to information include breach of access, spamming and spyware which all aim at deliberately compromising networks and computer systems. All these are forms of cyber- attacks. A good example is the case of Iran where the Stuxnet worm exposed vulnerabilities in Iranian nuclear enrichment facilities increasing its nuclear potential (O'Mahony, 2015). The inferred Russian involvement in cyber incidents in Estonia and Georgia is another example of cyber warfare. The case of Georgia qualifies to an act of cyber warfare primarily because of the damage that it caused; it disrupted military operations in the South Ossetia for an entire weekend (Espine, 2008; Herzog, 2011). The case of Estonia resulted in the disruption automatic teller machines transactions and telephone access to emergency services for both private and government sectors (Herzog, 2011).

2. Related work

If nations are to reduce the levels of cyber-attacks then we need to focus on both the organization level and, more importantly, the national level where policies and strategies are formulated (Swart et al, 2014). High security standards and principles at national level can only be improved and achieved through the cooperation of sectors, both private and government (Swart, 2015). With little to no effort being expended towards enforcement of these policies and strategies, nothing quantifiable has been done in achieving desirable results at national level as it has been the case at organization level. No continent has been left immune. Africa is particularly vulnerable to such security threats given the fact that it lacks security skill set and rapid roll-out of infrastructure. This has been shown in the case of South Africa (Swart et al., 2014), which is among the best resourced countries technologically within the African context.

Due to lack of resources to perform thorough research on national level (Swart et al, 2014) and failure to implement suitable security measures in order to curb vulnerabilities in the systems, much focus has been given at organization level rather than national level (Swart et al, 2013). This has not, however, solved the national security threats as various institutions which fall under the same nation could be using various means to ensure safety of their own institutional infrastructure while leaving the overall national level cyber threats unattended. On the other hand, if attention is given at national level it would ensure that most of these security threats are dealt with at entry level into a nation since the government exercises certain controls over Internet usage (Swart et al., 2014).

To prove how serious cyber-crimes have increased, the order of global annual expenditures has estimated its cost to be between $575 billion and 1 trillion dollars (CSIR, 2014). Cyber-crime is arguably the most prevalent crime in modern society to an extent that it can no longer be overlooked but must be dealt with urgently (Anderson et al., 2013). To address cyber security concerns, there is need for countries to produce cyber security policies that ought to be implemented at national level. At least thirty five countries internationally have implemented such policies (Hathaway, 2013).

One measurement that has been extensively used before in vulnerability assessment is Common Vulnerability and Exposure (CVE) metric (Swart et al., 2014). CVE provides a structured means through which information security vulnerabilities can be exchanged and makes data sharing across separate vulnerability capabilities easier due to its common naming (MITRE, 2015). This technique would help us in scoring and assessing the seriousness of the vulnerabilities available on the network, more importantly by looking into severity of vulnerabilities.

Information about the type of vulnerability, time stamp and severity score is provided by the CVE entries (Bozorgi et al, 2010). The severity and risk of the identified vulnerabilities is quantified using Common Vulnerability Scoring System (CVSS) which is an open framework (Mell et al., 2007). Base metrics, a component of the three metrics of CVSS, captures fundamental vulnerability feature such as access vendor, access complexity, authenticity, and the impacts on confidentiality, integrity and availability (Mell et al., 2007). CVSS is also preferred as it provides accurate and consistent vulnerability impact scores (NVD, 2015).

3. Methodology and Data Analysis

The study primarily focused on Internet Service Providers (ISP), devices commonly accessed on the Internet such as routers and servers using IP space attributable to Malawi and Tanzania. These data categories were defined within the open source intelligence tool Sentient Hyper Optimized Data Access Network (SHODAN) dataset itself, we just used them as they are i.e. they are known fields in SHODAN. All the data used in this study was obtained in June, 2015. The analysis of this data was used in conjunction with geolocation services in order to evaluate the degree to which potential vulnerabilities exist in the publicly accessible infrastructure of the nation states in question.

The use of Open Source Intelligence (OSINT) was preferred in this study because of several factors. Among them is its wide-ranging capability to allowing different inputs, hence providing room for evolution as technology standards evolve (Kapow Software, 2013). Furthermore, it is openly and legally accessible to the public and shareable making all legal implications in its acquisition of no concern (Schaurer and Störger, 2003). It is also relatively less expensive than collecting information via classified means (Pallaris, 2008). More importantly, it is reliable as not only do most agencies of the government use it in making decisions and policies, but it also provides awareness in understanding global security agenda (Pallaris, 2008).

Data processing was performed using a combination of common UNIX text processing tools such as AWK, and a series of custom Python scripts, which also performed the analysis and plotting of data. The majority of the input data was JSON formatted data files, as obtained from SHODAN. A selection of open intelligence sources such as SHODAN will be used to evaluate the degree to which potential vulnerabilities exist in the publicly accessible infrastructure of the states in question. Shodan primary objective is to collect data from the available ports unlike crawling a Website to access content (Harikrishnan, 2015). Given Internet connectivity to a device, Shodan can access all devices that are connected to the Internet such as IP-connected cameras, printers, traffic lights, medical devices, computers, power plants among others (Hill, 2013).

Outcomes

One of the factors we looked at is the Internet Service Provider. It is the organization that provides the IP space for the device in use (Shodan, 2015). Thus through this way we get to have a range of all IP addresses and all devices that a specific ISP assigned such device without leaving out any. In using the ISP we taking it as the ‘parent’ of the organization as far as IP ownership is concerned (Shodan, 2015). For an attacker to gain access to an organization's network he/she must have found a weakness through their system. One way to do that is to target devices that are connected to an organization’s network and have web interfaces. A web interface on a device creates a vulnerability to the device because it becomes easier to remotely manage the device. As long as it has a web interface or any open port Shodan can find it (Occupytheweb, 2014). It is for this reason that device type has been included in this study. The types of devices include web-cam, switch, router, firewall just to mention a few. One of hacker's best friends is an open port i.e. a port that enables an attacker to listen to a specific target (HOC, 2015). Through port scanning an attacker finds a way to determine what applications are exposed on a given target. This allows them to acquire information on possible vectors for attack (Johansson, 2005). It is for this reason that this study included port as a variable of interest.

From the data acquired, a pattern emerged from the two datasets. To begin with, we will look at the ISPs.

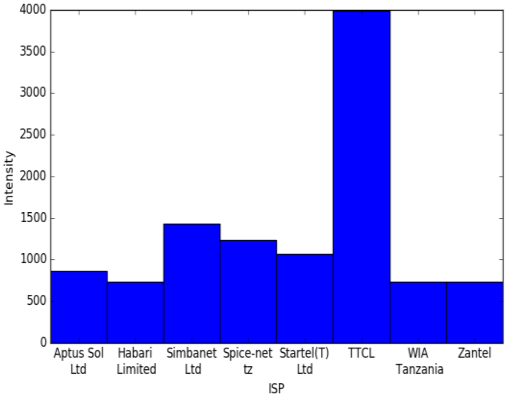

Figure 1: ISPs in Tanzania

Figure 1 shows a graph of the top 8 ISPs in Tanzania. There are 42 ISPs that were observed in the Tanzania's SHODAN dataset. However, these account for 65.53 % of the total instances of open ports within the Tanzanian dataset. Tanzania Telecommunications Company Limited (TTCL) is the oldest and largest ISP in Tanzania (Novatti, 2015). It also shows the highest prevalence of its clients on SHODAN by a huge margin as it can be seen from the graph. This is more than twice as much as its closest run which is Simbanet (T) Ltd. The other remaining ISPs from the graph above seem to show slight differences in their prevalence rate.

A similar analysis was also done for Malawi and Figure 2 shows the statistics there of. Unlike Tanzania, Malawi's SHODAN dataset could determine only seven ISPs as such all of them fit in a single graph.

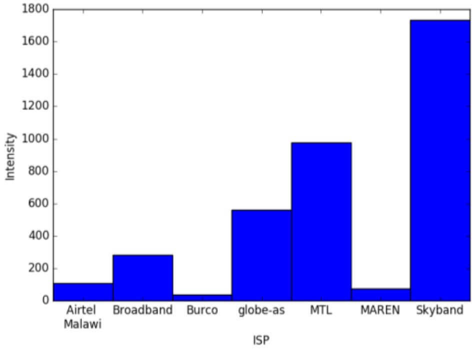

Figure 2: ISPs in Malawi

Figure 2 shows the ISPs from Malawi with Sky-band showing the highest rate of instances that were recorded by SHODAN. It is also the largest Internet service provider which is followed by MTL and globe in that order. SHODAN recorded a total of 3,836 instances for ISPs in Malawi while in Tanzania there were 15,513 instances. Table 1 shows the all the ISPs that were associated with IP addresses recorded in Malawi.

ISP	Instances	%
Airtel	108	2.82
Access	30	0.78
Burco	39	1.02
Broadband	284	7.40
Globe-as	562	14.65
Malswitch	11	0.29
MAREN	77	2.01

MTL	976	25.44
Sky-band	1732	45.15
TNM	4	0.1
NIC.mw	13	0.39
Total	3836	100

Table 1: ISPs in Malawi

Table 2 shows the top 10 ISPs in Tanzania that contribute over 70% of the total instances and the sum of the remaining 32 ISPs:

ISP	Instances	%
Aptus Solutions Ltd	863	5.56
Cats-Net Limited	372	2.40
Habari Node Ltd	732	4.72
Simbanet (T) Limited	1,432	9.23
Spice Net Tanzania Ltd	1, 230	7.93
Startel (T) Ltd	1,070	6.90
TTCL	3,376	21.76

University of Dar-Es-Salam	530	3.42
WIA Tanzania	729	4.70
Zanzibar Telecom(Zantel)	733	7.93
Other ISPs	4,446	28.66
Total	15,513	100

Table 2: ISPs in Tanzania

Another factor that was looked at was the device type used. Tanzania picked a wide variety of devices that are more in number and type than those picked in Malawi. Table 3 shows these devices for both Tanzania and Malawi respectively. The study also looked at the ports that were more prevalent in both Malawi and Tanzania. One interesting feature is that for Malawi the port which was more prevalent than the rest is 443 while in Tanzania it is port 80. Figure 3 show graphs that were made from these statistics for Tanzania and Malawi respectively. The total number of instances recorded for Malawi was 3,855 while for Tanzania it was 15,513

	Tanzania		Malawi	
Device Name	Devices	%	Devices	%
Firewall	62	9.62	10	1.25
Media Device	2	0.31	1	1.25
PBX	35	5.43	-	-
Printer	111	17.24	23	28.75
Printer	6	0.93	-	-

Server				
Router	9	1.40	1	1.25
Switch	414	64.29	45	56.25
WAP	5	0.78	-	-
Total	644	100.00	80	100.00

Table 3: Device types use

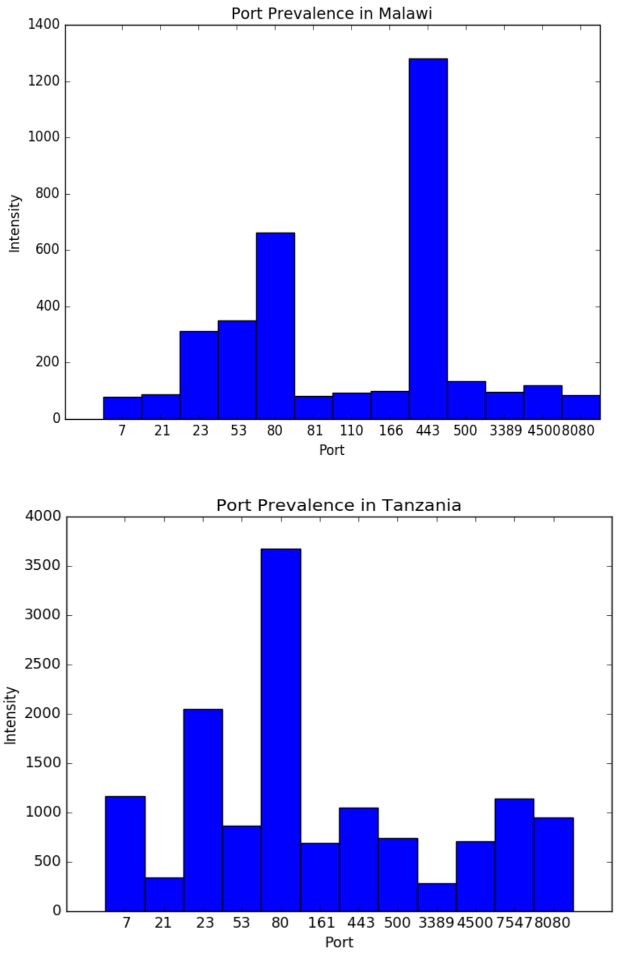

Figure 3: TCP and UDP Port prevalence

SHODAN picked a lot of ports with multiples instance from both Tanzania and Malawi datasets. For this study we only selected those that show a lot more instances than others. These have been recorded in Table 4. The table shows port numbers and the transport protocols used. These are some of the ports that were found open by SHODAN in both datasets. Once ports like 80/tcp (HTTP), 21/tcp (FTP), 22/tcp (SSH), 23/tcp (TELNET), 161/udp (SNMP) and 5060/udp (SIP) are left open to the general Internet for access, it enables SHODAN's capability to pull service banners from such devices and servers from the web (Occupytheweb). Some ports appear on both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) like 443 for example (Touch et al, 2015). In addition to this, the tables also show the port application for each transport protocol they use (Stretch, 2015; Touch et al, 2015).

4. Observations

Working with the results that we have it shows that the differences in ISP prevalence mean that clients within TTCL IP address space are more potentially more prone to attacks than the rest of the ISPs in Tanzania. In Malawi, it is Sky-band clients, followed by MTL clients who are more prone to attacks than the rest of the ISPs. These are countries that have over 12 million people, but the representation of the data is not proportional to entire population. This is one of the shortfalls for OSINT where we cannot do anything about, without further inputs and aggregation of additional sources.

The availability of few device types in both countries does not give a clear picture if the rest of the other devices were not recorded or that these are the only ones that popped up. Failure to know that a device is ‘emitting’ the signal and open to the Internet at large would make it harder to curb the problem as ports work specific to certain devices.

			Tanzania	Malawi
Port Number	Transport Protocol	IANA Names	Devices	Devices
7	TCP	Echo	233	94
21	TCP	FTP	338	87
23	TCP	Telnet	2051	311
25	UDP	SMTP	272	57
53	UDP	DNS	869	349
80	TCP	HTTP	3675	663

110	TCP	POP3	233	94
111	TCP	SUN RPC/NFS	128	27
123	TCP	NTP	248	20
137	TCP	NETBIOS	267	59
143	UDP	IMAP4	196	57
161	TCP	SNMP	690	-
166	UDP/TCP	Sirius System	-	99
443	TCP/UDP	HTTP over SSL	1058	1279
500	TCP/UDP	ISAKMP	742	133
993	TCP	IMAP over SSL	76	13
995	TCP	POP3 over SSL	69	11
1723	TCP	MS PPTP	190	55
1900	TCP/UDP	SSDP	134	8
3389	TCP	MS-RDP	287	97
4500	TCP/UDP	IPSec NAT-Travel/Other	705	119
7547	TCP/UDP	DSL Forum CWMP	1140	-
8443	TCP/UDP	PCSync HTTPS	69	-

8080	TCP	HTTP Alternate	954	85
9001	TCP/UDP	Other	229	-
9002	TCP/UDP	Other	67	-

Table 4: TCP/UDP Port prevalence

There are also some ports that should never be open to the larger world outside of an organisations internal network. For example port 110/tcp for a local RPC proxy, commonly found as a potential port forward on router devices. This was found to be open in both Malawian and Tanzanian datasets. The same goes for port 7/tcp/udp utilised by the legacy echo service, which has a vulnerability to be exploited to create a DoS (Denial of Service) threat as attackers use it to relay flooding data. Port 3389/tcp for Microsoft terminal services and remote desktop, should also be protected, as then potentially provides remote login and console access to systems, potentially deep inside an organisations network. All these ought to be closed for security purposes. Alternatively, in the case of port 3389/tcp since it is used for remote connection an organization can reconfigure and use another port (Microsoft, 2015) to serve the same purpose unlike it since it is now well known to act as a window to threats from outside the organization especially hackers.

Another area to look at is port 443/tcp which is used for secure hypertext transfer protocol while port 80/tcp is for hypertext transfer protocol meaning it is more secure for browser communication to occur on 443/tcp than 80/tcp. Based on this knowledge, it would be safe to say that since in Malawi port 443/tcp is more prevalent as compared to port 80 in Tanzania then Malawi is safer than Tanzania in the context of browser communication.

Out of the 26 ports that are recorded in Table 4, 53.85% of them use Transmission Control Protocol (TCP) , 11.53% use User Datagram Protocol (UDP) and 34.62% use both TCP and UDP thus moving TCP to 88.47% prevalence rate. It is also worth noting that with the exception of port 53/udp (DNS) most ports that are heavily used and have high prevalence rate use TCP.

The “Router” device type was that identified most frequently by SHODAN in data from both countries. Tanzania showed more device types that can be potentially exploited via the Internet. Both countries have left certain ports that are supposed to be closed to the outside world hence providing a window for the threats to penetrate their systems. Even bigger ISPs have not been left out by SHODAN meaning that their clients are at an equal risk just as the smaller ISPs. The problem of insecure misconfigured networks is thus seen to be prevalent across the IP address space assessed.

In view of these outcomes it becomes more clear why certain devices should never been connected to the internet. Good examples are cameras and media devices. Much as it becomes easy to monitor it also puts the device at risk of being accessed. Some devices like printers and routers need to be properly secured and default passwords removed as an attacker can easily find his way around them and gain control of them. Proper measures need to be taken to ensure that ports 443/tcp, 80/tcp, 53/udp are properly secured for fear of being used as a means of pivoting access or gaining further information about a target network. Since certain ports cannot be closed due to the services that they run then it is proper and wise to ensure that all applications that use these ports are properly patched and kept up to date. Some ports like 3389/tcp need to be protected as the services using them cannot easily be configured to use alternate ports. Since services such as this should only use locally/internally suitable firewall rules and/or VPN access requirements would ensure that servers are accessed remotely in a secure manner.

5. Conclusion

Major Internet service providers need to take an active in ensuring the safety and security of its clients as high prevalence of their cases could easily trigger keen interest to an attacker who has a proper motivation. Secondly, there is need to close some ports that are used for remote access or change them. If these two cannot work then patching and keep our systems up to date is recommended for hackers can easily get in through them. All devices with web interfaces need to be secured with proper strong passwords and remove all default passwords as SHODAN can easily detect them. Of the devices available switches seem to be very prone to attacks hence need to ensure that they are properly secured too.

5.1 Impact of findings

The study sets a benchmark for future work since now work of similar nature has not been done in Malawi and Tanzania respectively. In addition to this it also helps our understanding of the current state of affairs in relation to cyber vulnerabilities.

5.2 Future Work

This pilot study will be extended to other Southern and Eastern African states like Botswana, Kenya, Uganda and Namibia. The main objective will be to observe pattern and behaviour of these variables and to assess the level of access these device types are exposed to on the Internet since SHODAN showed that it is possible to access some of these devices, especially those that still utilise system/vendor default passwords or have no passwords at all. The study will also analyse the level of access to open source intelligence repositories and their role in contributing to a national level security assessment. The paper will also look into a comparative analysis aimed at assessing the factors that affect the degree of security susceptibilities in various states. Another comparative study will be done to see if there are changes to these factors once new data is collected and whether progress is made before recommendations are made.

Acknowledgements

The authors wish to acknowledge the funding received from the Beit Trust for this research and COE sponsors for funding registration fees.

6. References

Alan Calder. IT governance green paper: Information security & ISO 27001, 2013.

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. “The Economics of Information Security and Privacy: Measuring the cost of Cybercrime”, 2013.

Chris Pallaris. Open Source Intelligence: “A strategic enabler of National Security”. Vol.3, Series: CSS Analysis in security policy, Issue: 32. Publisher: Center for security studies, ETH Zurich, April 2008.

Center for Strategic and International Studies. Net losses: “Estimating the global cost of cybercrime”. (Date Accessed: 28/SEPTEMBER/2015). URL: http://www.mcfee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Florian Schaurer and Jan Störger. “Guide to the Study of Intelligence: The Evolution of Open Source Intelligence (OSINT)". 2003.

Hackers Online Club (Date Accessed: 30/JULY/2015): “Network Hacking”. URL: http://www.hackersonlineclub.com/network-hacking

Harikrishnan . R. Shodan search engine for penetration tests: How-to. (Date Accessed: 07/August/2015). [Online]. URL: http://searchsecurity.techtarget.in/tip/Shodan-search-engine-for-penetration-tests-How-to

Hathaway, M. “Cyber readiness index 1.0”. (Date accessed: 28/September/2015). URL: http://belfercenter.hks.havard.edu/publication/23607/cyber_readiness_index_10.html

Herzog, Stephen. “Revisiting the Estonian cyber-attacks: Digital threats and multinational responses.” Journal of Strategic Security 4, no. 2(2011):49-60.

I.P. Swart, M.M. Grobler and B. Irwin: “Visualization of a Data Leak: How Can Visualization Assist to Determine the Scope of an Attack?”, IEEE (2013).

I. Swart, B. Irwin, and M. Grobler: “Towards a platform to visualise the state of South Africa’s Information Security”. In: ISSA 2014: 13th International Information Security for South Africa Conference: Workshop on ICT Uses in Warfare and the Safeguarding of peace, Sandton, South Africa, 13-15 August 2014.

I.P. Swart: “Pro-active visualization of cyber security on a National Level: A South African case study”, PhD, Rhodes University. (2015)

Jennifer O'Mahony, (Date Accessed: 28/May/2015). “Stuxnet-worm-increased-Irans-nuclear-potential”. URL: http://www.telegraph.co.uk/technology/news/10058546/Stuxnet-worm-increased-Irans-nuclear-potential.html.

Jeremy Stretch. (Date Accessed: 28/JULY/ 2015) “Common ports: TCP/UDP Port Numbers”. URL: http://packetlife.net/media/library/23/common_ports.pdf

Jesper Johansson. (Date Accessed: 30/JULY/2015). “How A Criminal Might Infiltrate Your Network”. URL: https://technet.microsoft.com/en-us/magazine/2005.01.anatomyofahack.aspx

Joe Touch; Eliot Lear, Allison Mankin, Markku Kojo, Kumiko Ono, Martin Stiemerling, Lars Eggert, Alexey Melnikov, Wes Eddy, and Alexander Zimmermann, (Date Accessed: 29/JULY/2015). “Service Name and Transport Protocol Port Number Registry”. URL:http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=111

Kapow Software. “Building your osint capability: collect any content, in any language, from any website, without attribution", May 2013.

K. Hill. (2013, May) “The crazy things a savvy Shodan searcher can find exposed on the internet. Forbes”. Date Accessed: 07/August/2015. [Online]. Available: http://www.forbes.com/sites/kashmirhill/2013/09/05/the-crazy-things-a-savvy-shodan-searcher-can-find-exposed-on-the-internet/

Lawrence Abrams, (Date Accessed: 29/JULY/2015): “TCP and UDP Ports Explained” URL:http://www.bleepingcomputer.com/tutorials/tcp-and-udp-ports-explained/

Mehran Bozorgi, Lawrence K. Saul, Stefan Savage, and Geoffrey M. Voelker. “Beyond heuristics: Learning to classify vulnerabilities and predict exploits”. In Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '10, pages 105-114, New York, NY, USA, 2010. ACM. ISBN 978-1-4503-0055-1. doi: 10.1145/1835804.1835821.

MITRE. “CVE - Common Vulnerabilities and Exposures. Technical report”, MITRE, 15 February 2015. URL http://cve.mitre.org/about/documents.html/.

Microsoft. (Date Accessed: 07/OCTOBER/2015). “How to change the listening port for Remote Desktop”. URL: https://support.microsoft.com/en-us/kb/306759

National Vulnerability Database. (Date Accessed: 30/JUNE/2015). "Common Vulnerability Scoring System Support V2". URL http://nvd.nist.gov/cvss.cfm

Occupytheweb, (Date Accessed: 17/SEPTEMBER/2015) "Hack Like a Pro: How to find vulnerable targets using Shodan-The World most dangerous search engine." URL: http://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-targets-using-shodan

Shodan. (Date Accessed: 01/JUNE/2015) "Banner Specification". URL: https://developer.shodan.io/api/banner-specification

Tom Espine: "Georgia accuses Russia of coordinated cyber-attack", 2008. URL: http://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/.

Mobile Phone Costs: Exploring the relationship between Information Overload and Attention

In’aam Soeker[1] and Jacques Ophoff[2]
Department of Information Systems
University of Cape Town, South Africa
e-mail: [1]inaamsoeker@gmail.com, [2]jacques.ophoff@uct.ac.za

Abstract

The mobile phone has changed the way individual’s access and consume information. It has transformed the way individuals connect and maintain their physical and virtual relationships and has facilitated online presence. This study explores how the mobile phone affects users’ attention. It follows a qualitative methodology making use of focus groups for data collection. It shows how users associate a benefit and cost to the information they gain from their mobile phone. Themes that emerged include valued application characteristics, online presence, distraction and dependence, and interaction norms. The findings show that the information received and allocation of attention is context dependent and that complex psychological and sociological effects are present. The increased attention users pay to their mobile phone is leading to new social norms of mobile phone use.

Keywords

Mobile phone, information overload, attention, interaction norms, communication context, behavioural experiences, millennials

1. Introduction

Digital technology is advancing and transforming the way individuals live their lives. Smartphones, one of the most prominent technologies today, changes the way information is accessed and consumed by individuals (Matthews et al., 2009). During the information age, knowledge meant power and your success was a determinant of how much knowledge you held. However, the ever-increasing flows of excessively redundant information we encounter every day consumes our already limited capacity of attention (Davenport & Beck, 2001). This can be seen as a ‘cost’ of using such devices and services (Davenport & Beck, 2001; McCullough, 2013).

Attention is scarce because it a finite human resource (Berman & McClellan, 2002; Huberman, 2009; Terranova, 2012). With the ever-increasing overload of information exposure users will soon start to feel attention fatigue (Roth, 2007). The aim of this study is to provide a deeper understanding of the influence mobile phones have on users’ attention, focussing on millennials due to their comfort and use of technology.

The rest of the paper is structured as follows. First a review of relevant background literature is given. Thereafter the research methodology is discussed. This is a followed by the data analysis and discussion. The conclusion provides a summary and points to further research opportunities.

2. Background

Mobile phone capabilities keep progressing beyond expectations, leading to an unabated adoption rate. Several studies have shown that, due to their functionality, accessibility to mobile phones are essential to young individuals (Porter et al., 2012; McCullough, 2013). Srivastava (2005) found that many individuals are spending most of their time on their smartphones, using it to surf the web or social media applications. The more time young individuals spend, the more attention they pay to their phones (Malinen & Ojala, 2011). Previous research in mobile communications has also focused on attention and information overload (Ling & Campbell, 2011), instrumental information access (Bertel, 2013), and communication and information needs (Mihailidis, 2014). Though examining the youth, the above studies have broadly focused on the use of mobile phones and thus attention and information overload costs have not been fully explored.

2.1 Attention

In comparison to millennials and later, previous generations did not suffer from the attention deficit occurring in our society today (Davenport & Beck, 2001; Berman & McClellan, 2002; McCullough, 2013). This deficit is mainly due to the information overload currently experienced. Simon (1971, pp. 40-41) noted that “in an information-rich world, the wealth of information means a death of something else: a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients.”

Attention is defined as a cognitive process in which we selectively absorb information (Davenport & Beck, 2001). Our attention needs to be allocated selectively given the vast amount of information we are exposed to every day. Huberman (2009) found that attention can be selectively allocated to information that is most relevant to the task at hand, but that our attention is constantly competed for through social media networks, blogs, chats, and emails appearing on our mobile phone screens.

2.2 Information Overload

Today individuals are over-consuming the abundance of information available to them, which leads to what is commonly known as information obesity (McCullough, 2013). The smartphone is a source for accessing information, transferred through mediums of communication, also known as applications, such as: text and instant messaging, email, gaming, social media, and most importantly the web (Srivastava, 2005; Huberman, 2009; Ling & Campbell, 2011). However, feature phones have messaging and web access capabilities which also make them sources for information access. We use the term mobile phone as including both these device classes.

Information can be distributed to individuals using a pull or push mechanism. Pull information is demanded and pursued by the user, for example searching Wikipedia. Push information is sent without the user’s control, for example spam (Jackson & Farzaneh, 2012).

Terranova (2012) found that the seamless overload of information from text-messages, emails, or social networks via mobile phones acts as digital distraction to its users. Van Kleek (2011) supported this claim by adding that the impact of these digital distractions are having a negative effect in individuals’ lives to the point where it could potentially become hazardous. Individuals are susceptible to noticing any form of interruption, irrespective of how important the requirement of their full attention to a particular situation may be (Van Kleek, 2011; LaRose et al., 2014). For example, while driving an individual receives a notification of an incoming message; this distracts them and becomes hazardous to the individual (Van Kleek, 2011). In addition, Malinen and Ojala (2011) found that in certain instances, for example while studying, young individuals would consciously switch their mobile phones off, as they were aware that their attention would be diverted to their mobile phones when they received a message. Thus individuals are aware of the distraction of mobile phones, albeit that they cannot control it in certain instances (Van Kleek, 2011; Malinen & Ojala, 2011).

2.3 Mobile Phones

According to Ling and Campbell (2011) the mobile phone enables the cultivation of interpersonal ties which provides a social network platform for individuals to achieve and accomplish connections, thus acting as an enabler of the personal sphere. Mobile phones allow individuals to extend their computing prospects and to achieve their information-based needs (Matthews et al., 2009). However, switching between mobile applications lead to our attention also being switched and the brain having to reorient itself, which negatively affects our already limited attention capabilities (Terranova, 2012; McCullough, 2013).

Recent reports indicate that people now spend more time on their mobile phones than watching television, estimated at almost 3 hours every day (Brustein, 2014). In a survey of American users, the Pew Research Center (2015) found that young users spend the majority of their time on social media and 15% of users aged 18-29 years are heavily dependent on a smartphone for online access.

Individuals have been found to be attached to their mobile phones, not only physically but also emotionally (Srivastava, 2005). The physical attachment can be displayed by mobile phones being kept constantly on their person; emotional attachment is displayed when individuals feel unsettled when another individual browses through their mobile phone (Srivastava, 2005). Individuals have become too reliant on their smartphones as they try to do anything and everything on it (McCullough, 2013). In addition, giving too much attention to a mobile phone can be interpreted as impoliteness and incivility by co-present others (Ling & Campbell, 2011; Malinen & Ojala, 2011).

3. Methodology

There are a limited number of studies exploring the abovementioned issues (perhaps due to their interdisciplinary nature). Thus the current study aims to explore issues around mobile phone usage, information overload, and attention in millennials. Issues around which this exploration is structured include: users' relationship with their mobile phone, behavioural experiences, and perceived costs (internal and external) to the individual.

A qualitative study using focus groups was employed due to the subjective nature of the phenomenon of interest. A focus group is a form of group interview, involving a small number of participants (in a common location) in a focused discussion of the phenomenon, under the supervision of a facilitator (Bryman, 2012). Focus groups are well-suited for exploratory research as they allow the participants to fully interact and convey their views of the situation by enabling them to speak freely about the topic. For this study three focus groups, each consisting of 6-10 participants, were used (total of 23 participants). Purposive sampling was used to select participants; this ensured an equal representation of income, employment status, gender, and culture (Bryman, 2012, p. 418). Participants ranged from 19-25 years old and were all residents of Cape Town, South Africa. Gender, age, and employment status data of focus group participants are detailed in Table 1.

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Focus Group 1	F, 20, S	F, 20, S	F 20, S	F, 20, S	M, 22, S	M, 23, E	M, 22, S	-	-	-
Focus Group 2	F, 21, S	F, 22, S	M, 22, S	F, 19, S	F, 21, E	M, 22, E	-	-	-	-
Focus Group 3	M, 20, S	M, 22, S	F, 21, E	F, 23, E	F, 23, S	F, 24, E	F, 24, E	M, 25, E	M, 22, E	M, 25, E

Table 1: Focus group participant demographics (Male/Female, Age, Student/Employed)

Ethical clearance was obtained before commencing with data collection. Best practices were followed to minimise facilitator bias and facilitate group discussion (Bryman, 2012; Silverman, 2013; Flick, 2014). A semi-structured interview schedule was used to focus discussion. Questions were tested for clarity and unambiguousness using a pilot study with a small group of people. Based on feedback question wording was improved and irrelevant questions were removed.

Focus group sessions were conducted over a period of approximately four weeks. Sessions were recorded using audio and then transcribed for analysis. Thematic analysis was used to analyse the data. Thematic analysis is a method by which major themes are identified, analysed, and codified from the data collected (Braun & Clarke, 2006).

4. Data Analysis and Findings

Participants in the focus groups had mutual feelings and perceptions about their use of mobile phones, information of interest, and how they allocate their attention. All participants appeared to be very experienced with their mobile phones, often giving long and elaborate answers. Some participants, appearing shyer and introverted, contributed with shorter and less complex answers. The majority of participants seemed to have extreme relationships with their mobile phones in terms of use and allocation of attention; a small minority seemed to be less absorbed by all of it.

Existing literature (e.g. Sohn et al., 2010) and focus group data exhibited the following usage pattern: 1) a mobile phone consists of many applications, 2) each application encompasses and provides certain information, 3) that information is then the determining factor of the how users allocate their attention, and 4) this leads to interaction norms depending on the communication context. The following subsections discuss these aspects and themes identified during data analysis.

4.1 Valued Application Characteristics

Applications that participants perceived to be the most attention-grabbing were found to be those that they selectively installed on their mobile phone. This is due to most applications being able to push notifications to the user. The following application characteristics are perceived as valuable, resulting in the installation of the application.

Information

Participants from all focus groups agreed that information about people, latest news, politics, and sports (mainly suggested by males) are the main factors for installing a specific application. This could be due to the fact that users prefer information that is live, current, and real. Information that they perceive to be relevant to their lives are the type of information they find interesting. Users start using and paying attention to applications regularly if they find the information to be attention-grabbing. Participants confirmed a change in application use from push notifications to regularly pulling information, as found in previous literature (Jackson & Farzaneh, 2012).

Entertainment/Interest/Fun

Participants perceived applications that grab their attention to be interesting and fun in terms of the information they provide. Entertainment applications, on the other hand, was perceived to occupy, entertain, and distract for a lengthy period of time, e.g. playing games, watching YouTube videos, or listening to music. Remaining occupied prevents feelings of anxiousness, with users feeling the need to pay attention to their mobile phone as their 'escape'. Free time is not spent on personal (offline) relaxation, but used to stay connected with the people or information through their mobile phone. One participant mentioned that when he is on a date and his date had to leave to use the restroom, he would take that opportunity to pay attention and check his mobile phone. Another participant mentioned that he uses it as a way to occupy himself while waiting for someone. Thus, the mobile phone is used to kill free time more specifically in times when he is bored or experiencing lack of stimulation. Using their phone to avoid boredom was also reported by 77% of users in the Pew Research Center (2015) study, second only to coordinating with others.

(Value-added) Purpose

Participants ranked applications according to the perceived value: phone calls, SMS's, WhatsApp, BBM, and lastly social media notifications. Attention-grabbing applications were those perceived to serve a purpose in the participants' lives and users spent most of their time on those applications. Some applications provide value in terms of (university) work for example: *"I'm always using my mobile phone to check any announcements my lecturers might have made on Vula. My mobile phone has actually made accessing my university information easier really; now I can just log onto Vula and access a lecture if I'm struggling."*

(Online) Presence

Participants were attracted to applications that allow them to establish an online presence in the virtual world. For example, Twitter allows users to gain followers, the more followers you have the more popular you are in the virtual world, which could often spill over to the physical world. As one participant stated: *"People have* *online presences on social media. Some people get affirmation and motivation through their online presence. When people find themselves in a face-to-face conversation/interaction, often they would still find themselves checking their phones because of their constant need to get this affirmation by social media. They sometimes feel that the satisfaction of this affirmation by the virtual world is greater than the satisfaction they receive during their face-to-face interaction (physical presence)."* The type of online presence is important and determines how much attention an application gets. Especially social media provides a sense of identity, status, and popularity. Social media application has become a way for people to feel important to others, raise their social status, and increase their popularity (Srivastava, 2005; Ling & Campbell, 2011).

4.2 Behavioural Experiences

Several behaviours, both positive and negative, were reflected in the focus group discussions. It is interesting to note that these are influenced by social and personal context, as well as technical aspects.

Dependence

Participants reported spending anywhere from 2-17 hours a day using their mobile phone (average of 10 hours for ten participants who reported a specific amount of time). A lot of this time consists of switching between their mobile phone and other activities. As reported in prior research, regularly phone use can create a dependency causing users to feel lost without it (McCullough, 2013). The majority of focus group participants felt dependent on their mobile phones and relied heavily on it in order to accomplish their daily activities. One participant described the feeling of being without a mobile phone as "empty" and "naked".

Users often feel dependent on the on the mobility offered by their mobile phone, having a need to be constantly available. A number of participants mentioned that they would often feel lost without their mobile phone, if they were to leave it at home, and would more likely than not go to fetch it if possible. Users seem to feel more comfortable when they are able to stay in contact with others, have the option to listen to music, or play games on their mobile phone. This confirms that users perceive their mobile phone to be an extension of themselves (McCullough, 2013). One participant noted: *"I only really feel comfortable when I am paying attention to my mobile phone."* When users feel that their comfort depends on their mobile phone, it becomes a clear indication that it has moved beyond just being an accessory to them – it is something they constantly rely on.

Happiness and relaxation

One participant conveyed how her daily routine consists of coming home from university, plugging her mobile phone in to charge, as she has depleted her battery from paying large amounts of attention to it during the day, and then paying attention to social media applications again to relax. One interesting factor contributing to feelings of relaxation is mobile phone signal strength. Focus group discussions reflect that the stronger and more reliable the signal strength, the happier and more relaxed the user feels. Signal strength determines the amount of information a user can get access to in a shorter period of time, as opposed to a slower connection.

A participant related how, the more stable and stronger the connection, the more relaxed and at ease the participant felt. Mobile phones acquire signal strength through a cellular service provider or through Wi-Fi access points. The following participant comment illustrates this point: "*In one of the rooms in my house the Wi-Fi connection is really strong and stable which is where I go to relax and spend quality time my mobile phone."* The participant responses indicate that they not only depend on the information they receive, but also on how fast they can access it.

Addiction

Focus group participants all agreed that they have become addicted to the applications on their mobile phone. One participant illustrated this point by saying: *"Sometimes the information I get while using an application isn't relevant but I would continue using it for hours due to my addiction to the application. I like being on the application rather than not being on it."* Users are constantly checking their mobile phones for notifications which enable them to see if there is something interesting happening right now. This suggests that users have a need to constantly consume new information to feed their addiction. Users have become addicted to the mobility offered by their mobile phone (Srivastava, 2005), the ability to constantly be connected, and the online presence it offers.

The majority of participants mentioned that they always take their mobile phone with them wherever they go, be it to go get something in the fridge or while they use the bathroom. Nobody could give a clear indication as to why they are constantly giving their mobile phone this much attention besides that it has become a reflex. One participant noted that she would find herself at a point where she had paid attention to all the information her social media applications could offer her and yet would still check and pay attention to her mobile phone every five minutes or refresh the page in expectation of new information arriving: *"I often remain on Twitter or Instagram, even after I have read all the information, and I would just keep on refreshing the page hoping someone would post new information."*

Curiosity

Once a notification is received on a user's mobile phone they tend to feel curious as to what the content of that notification may be. Thus once they hear the sound, vibration, or see the notification light they automatically turn their attention towards their mobile phone to pay attention to this unknown information. One participant explained: *"In certain circumstances, for instance when you're chatting to someone and you receive a notification, you know who sent the message.... So you kind of know the content of what the message might say... So you wouldn't still pay attention or check the message to reply. However, if you weren't interacting with your mobile phone and you received a notification you would generally be curious as to who is trying to get your attention, thus you would instantly pay attention to the message."*

When information is unknown to users they tend to be more interested in it – curiosity causes a constant pull of users' attention (Pihlström & Brush, 2008). The users do not usually know whether the unknown information will outweigh the information they get from their physical environment, but due to their curiosity perceive paying attention to the unknown information to supersede their physical setting.

4.3 Perceptions of Attention Allocation

Participants described full attention as that moment you become lost in what's happening. They often felt this in times when their full attention was given to the task at hand. This section discusses how, and to what extent, users allocate their attention to their mobile phone.

Distraction

All the participants perceived mobile phones as a distraction within itself. When a notification comes through on their mobile phone it instantly distracts them from what they are currently doing and they would immediately direct their attention to it. This leads to them being less able to focus on other activities for extended periods of time. Many of the participants felt that having their mobile phone on their person already instigates a reflex of checking their mobile phone frequently. This results in habits of dealing with things rapidly in a multitasking manner, as opposed to a contemplative and creative way of thinking (Van Kleek, 2011; Malinen & Ojala, 2011).

Subconscious attention and phantom vibrations

Subconscious attention is the attention users allocate to their mobile phone due to expecting some kind of information, as stated by a participant: *"When I'm busy having a conversation with someone over WhatsApp, my mobile phone will always have my attention as I am expecting a message from that person. So I would sit and anticipate a message to come through. Often I would find myself pre-occupying myself with other physical activities until I receive a message to reply."* Some users stated that they would subconsciously pay attention to their mobile phone with the hope that they receive a notification with some information. It seems that such users have started to depend on the overload of information from their mobile phone.

Due to the attachment users have to their mobile phones, they often feel phantom vibrations (Drouin, Kaiser, & Miller, 2012). One participant mentioned: *"When I am expecting a message from someone, I sometimes feel a vibration from my mobile phone and automatically assume it's a message. When I check it there is no message and it did not really vibrate."* When a user considers their mobile phone to be an extension of them, such as an arm or leg, it could be similar to phantom leg syndrome. Dependency on a mobile phone causes hallucinatory symptoms like the imagined vibration (Drouin, Kaiser, & Miller, 2012).

4.4 Interaction Norms

A mobile phone allows users to interact without the need to be in the same physical location. Different social rules are constructed for different types of interactions.

Face-to-face interactions

Face-to-face interactions refer of physical interactions with people. The majority of participants agreed that in face-to-face interactions they would not generally pay attention to their mobile phones. This is dependent on the value of the interactions, for instance if the co-present other is discussing something important they would give their full attention to the co-present. While the interaction proceeds the only acceptable time to pay attention to a mobile phone would be when a call is received, as participants agreed that a phone call is associated with urgency and importance. The above is related by a participant as follows: *"Whether I pay attention to my mobile phone while in a face-to-face interaction depends on the level of importance of the current conversation. I will not, generally, use my mobile phone but if I find the conversation to be pointless or add no value, then I would definitely pay attention to any notification that I receive from my mobile phone."* One participant stated that he/she would always pay attention to the mobile phone, even during an important face-to-face interaction. This participant perceives the (potential) information just as important as the conversation at hand – a perception that could be related to addiction.

Group interactions

All participants perceived that if they found themselves in a group (of at least three people) it is more acceptable to use a mobile phone. One participant explained: *"I feel more comfortable when I pay attention to a notification I receive on my mobile phone while I'm in a group of people. Due to the fact that the attention is not solely on me so I evade the feeling of being rude as opposed to a face-to-face interaction."* This suggests that users often weigh the dynamics of the group before they pay attention to their mobile phone. It seems that users attach a different social rule to a group than to a face-to-face interaction.

4.5 Communication Context

Users have established situations where it is acceptable, and sometimes necessary, to pay attention to a mobile phone as well as when it is completely unacceptable. The use of certain communication channels imply relative urgency. All of the participants agreed that upon receiving a phone call it is acceptable and encouraged to pay attention to a mobile phone. The participants perceived a phone call as an urgent form of communication as opposed to a text or instant message. They reasoned that people do not opt to make a phone call, which is more expensive and perceived to be of more effort as opposed to sending a message, which is easier, cheaper, and convenient. By sending a message the need to speak to someone is eliminated and users have the option to respond to the message in their own time.

Users often find it unacceptable to pay attention to their mobile phones in situations where it can be considered rude, uncivil, and inappropriate co-present behaviour (Ling & Campbell, 2011; Malinen & Ojala, 2011). Participants confirmed this and suggested the following instances: meetings, religious gatherings, family events, dates, important face-to-face interactions, and while eating or sleeping.

4.6 Summary of Findings

Based on our interpretive findings, Figure 1 captures the emergent themes into a conceptual model depicting the interactions taking place. Information flows from mobile applications which are selectively installed by users according to need and perceived value. Information from these applications demand user attention, which could lead to information overload. Attention paid to information could be mediated by interaction norms and the communication context. The user’s behavioural experience may also have a moderating effect on the amount of attention paid. Behavioural experience may also be influenced by technical aspects (e.g. the mobile phone or application) and by context.

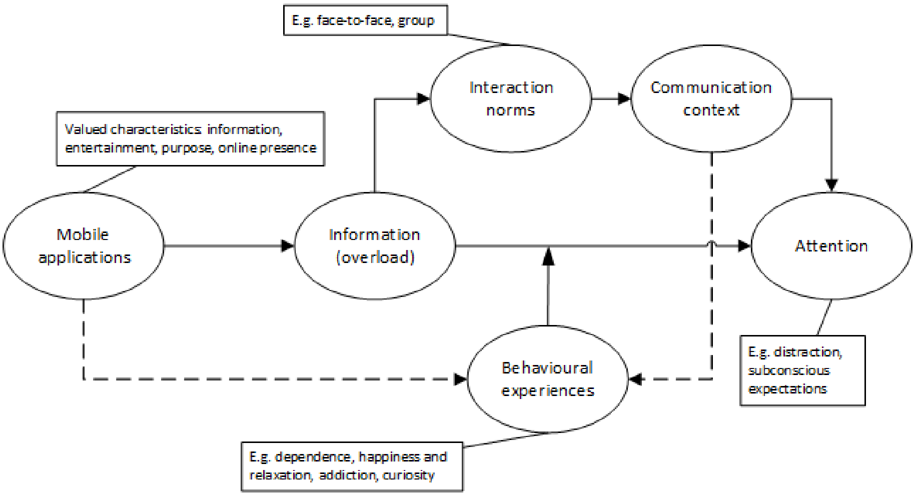
E.g. face-to-face, group
Interaction norms
Communication context
Valued characteristics: information, entertainment, purpose, online presence
Mobile applications
Information (overload)
Attention
Behavioural experiences
E.g. distraction, subconscious expectations
E.g. dependence, happiness and relaxation, addiction, curiosity

Figure 1: Conceptual model based on emergent themes

5. Conclusion

The objective of this study was to explore the influence of mobile phones on users' attention, focusing on millennials. A qualitative approach using focus groups was employed. The findings show that young users' associate complicated cost-benefit trade-offs with the use of mobile phones. A need exists to create and maintain virtual relationships, often at the cost of physical connections. This could be due to the ease, accessibility, and convenience offered by mobile phones.

Limitations of this study include a relatively small sample from a single geographic location. This limits generalisation of the findings. General limitations linked to focus groups, such as group effects (Bryman, 2012, pp. 517-518), may also have an impact on the findings.

The exploratory analysis points to several interesting cross-disciplinary research areas, especially psychological and sociological issues arising from mobile phone use. Cultural effects as well as generational (e.g. digital natives) characteristics may also affect the relationship we have with our mobile phone. We should revisit the notion that attention is valuable and scarce, the allocation of which should be managed like any other finite resource (Davenport & Beck, 2001). Future work should examine technical and behavioural aspects of managing information overload and attention. Theories from the social sciences, such as cognitive dissonance, could be used to probe cognitive and emotional discomfort. There is also scope for experimental studies evaluating technical mechanisms to limit information overload. With the proliferation of new technologies and increasing connectivity this can prove highly beneficial as we continue to become immersed in a digital world.

6. References

Berman, S. & McClellan, B.E. (2002). Ten strategies for survival in the attention economy. *Strategy & Leadership,* 30(3), 28-33.

Bertel, T. F. (2013). "It's like I trust it so much that I don't really check where it is I'm going before I leave": Informational uses of smartphones among Danish youth. *Mobile Media & Communication,* 1(3), 299–313.

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.

Brustein, J. (2014, November 19). We Now Spend More Time Staring at Phones Than TVs. Retrieved September 18, 2015, from http://www.bloomberg.com/bw/articles/2014-11-19/we-now-spend-more-time-staring-at-phones-than-tvs

Bryman, A. (2012). *Social Research Methods (4th edition).* Oxford ; New York: Oxford University Press.

Davenport, T.H. & Beck, J.C. (2001). *The Attention Economy*. Boston, Massachusetts: Harvard Business School Press.

Drouin, M., Kaiser, D. H., & Miller, D. A. (2012). Phantom vibrations among undergraduates: Prevalence and associated psychological characteristics. *Computers in Human Behavior*, 28(4), 1490–1496.

Flick, U. (2014). *An Introduction to Qualitative Research (5th edition).* Los Angeles: SAGE Publications Ltd.

Huberman, B.A. (2009). Social attention in the Age of the Web. Working together or apart: Promoting the next generation of digital scholarship, 62-129.

Jackson, T.W. & Farzaneh, P. (2012). Theory-based model of factors affecting information overload. *International Journal of Information Management*, 32, 523-532.

LaRose, R., Connolly, R., Lee, H., Li, K. & Hales, K.D. (2014). Connection Overload? A Cross Sectional Study of the Consequences of Social Media Connection. Information Systems Management, 31, 59-73.

Ling, R. & Campbell, S.W. (2011). *Mobile Communication: bringing us together and tearing us apart.* New Brunswick, New Jersey: Transaction Publishers.

Malinen, S. & Ojala, J. (2011). Maintaining the Instant Connection – Social Media Practices of Smartphone Users. In *From Research to Practice in the Design of Cooperative Systems: Results and Open Challenges*. London: Springer London, 197-211.

Matthews, T., Pierce, J. & Tang, J. (2009). No smart phone is an island: the impact of places, situations, and other devices on smart phone use. Research Report RJ10452, IBM, 10452.

McCullough, M. (2013). *Ambient Commons: Attention in the Age of Embodied Information*. London: The MIT Press.

Mihailidis, P. (2014). A tethered generation: Exploring the role of mobile phones in the daily life of young people. *Mobile Media & Communication*, 2(1), 58–72.

Pihlström, M., & Brush, G. J. (2008). Comparing the perceived value of information and entertainment mobile services. *Psychology and Marketing*, 25(8), 732–755.

Porter, G., Hampshire, K., Abane, A., Munthali, A., Robson, E., Mashiri, M. & Tanle, A. (2012). Youth, mobility and mobile phones in Africa: Findings from a three-country study. *Information Technology for Development*, 18(2), 145-162.

Roth, C. (2007). Techniques to Address Attention Fatigue and Info-Stress in the Too-Much-Information Age. Collaboration and Content Strategies.

Silverman, D. (2013). *Doing Qualitative Research: A Practical Handbook (4th edition)*. London ; Thousand Oaks, California ; New Delhi ; Singapore: SAGE Publications Ltd.

Simon, H.A. (1971). Designing Organizations for an Information-Rich World. In *Martin Greenberger, Computers, Communication, and the Public Interest*. Baltimore, MD: The John’s Hopkins Press.

Sohn, T., Seltur, V., Mori, K., Kaye, J., Horri, H., Battestini, A., Ballagas, R., Paretti, C., & Spasojevic, M. (2010). Addressing Mobile Information Overload in the Universal Inbox through Lenses. *Proceedings of MobileHCI '10*, ACM, 361–364.

Pew Research Center (2015, April 1). “The Smartphone Difference”. Retrieved from http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

Srivastava, L. (2005). Mobile phones and the evolution of social behaviour. *Behaviour & Information Technology*, 24(2), 111-129.

Terranova, T. (2012). Attention, Economy and the Brain. Culture Machine, 13, 1-19.

Van Kleek, M. (2011) Effort, memory, attention and time: paths to more effective personal information management. PhD Thesis, MIT, 2011.

Increasing the level of security awareness among web applications developers

Moses Moyo[1], Hanifa Abdullah[2] & Marriane Loock[3]
[1] School of Computing UNISA, Pretoria, South Africa
1 msosesm50@gmail.com
[2]abdulh@unisa.ac.za
[3]loockm@unisa.ac.za

Abstract

Web applications have popularised information interaction and transformed how organisations manage their information. The ease and cost effectiveness with which web applications are developed and deployed make them a better substitute for desktop applications in various organisations. Unlike desktop applications, web applications seem to demand less formal programming skills and knowledge hence an influx of developers is emerging to pursue web development for financial reasons. However, web application development presents many complex security issues that developers without sufficient level of security awareness may overlook. Nowadays, web applications have become one of the biggest sources of data breaches in many enterprises regardless of sophisticated web security systems used. This paper reviews existing literature on web applications security focusing much on those security vulnerabilities that developers may overlook. The paper also discusses security implications to information systems where such applications could be used. The paper suggests practical ways that could possibly be adopted in order to increase the level of security awareness among web application developers.

Key terms

Web applications, security awareness, web application security

1. Introduction

The demand for web applications is on the rise because they can be used to process sensitive data and perform powerful actions with real-world consequences (Taylor, 2012). These capabilities make web applications potential tools in growing technologies such as cloud computing and business intelligence hence they play a pivotal role in electronic commerce. Regardless of these benefits, web application can have the potential of information security breaches that originate from the developers' lack of information security awareness. Peculiar and significant security vulnerabilities in web applications tend to present organisations with many problems to deal with (Petukhov & Kozlov, 2008). Each new web application developed, has the potential to contain security vulnerabilities due to code errors therein (Stuttard & Marcus , 2011). Vulnerabilities in web applications are difficult to deal with from a risk management perspective because it is hard to determine their presence and whether they are exploitable or not (Guglielmino, 2013). Web applications always present complex sets of security issues for developers, therefore, the most secure and hack-resilient web applications are those that have been built from the ground up with security in mind (Meier, et al., 2003). Many web applications are now being developed in-house by developers with divergent skills and knowledge, including developers who may barely understand security problems that arise in the code they produce and the vulnerabilities they create in the applications (Stuttard & Marcus , 2011). Web applications security presents developers with unprecedented challenges that require practical solutions. Security challenges in web application development have escalated because many developers lack expertise in web applications security. In this context, the diversity of web applications being developed has become a cause for concern because each different application is most likely to contain peculiar vulnerabilities that the developers and organisations will be ignorant of.

The contribution made by various web developers is vital; however, this could be enhanced by increasing their level of security awareness in web application development. The major objective of this paper is to identify and discuss crucial web application vulnerabilities due to programming errors that developers may overlook. The paper also discusses possible practical approaches that could be utilised to increase the level of security awareness among web application developers.

The paper is organised into six sections with interrelated subtopics on web application security and awareness approaches. Section 1 is the introduction, Section 2 gives back ground of study, Section 3 is on related works, approaches to raise security awareness and challenges in the security approaches and web application. Section 4of this paper deals with possible approaches to security awareness whilst Section 5 elaborates on challenges and security awareness programmes and ultimately Section 6 is the conclusion.

2. Background

2.1 Importance of security awareness in web application development

Security awareness refers to owners, providers, users and other parties that should be able to gain knowledge about information security, be aware of the importance of information and be consistent with maintaining security (Hentea, 2005). According to (Kruger & Kearney, 2006), security awareness deals with the use of security awareness programmes to create and maintain security-positive behaviour as a critical element in an effective information security environment. The purpose of security awareness is to focus attention on security, creating sensitivity to the threats and vulnerabilities of computer systems and recognition of the need to protect data, information and systems (Awoleye, et al., 2014). Being security aware means that one understands that there is the potential for some people to deliberately or accidentally make use of applications to steal, damage, or misuse the data that is stored within an organisation's information system. With reference to web application security issues, there has been less development in security awareness compared to some long established areas such as networks and operating systems (Stuttard & Marcus , 2011). Networks and operating systems security is taught as subject to students pursuing IT or computer science courses while web application security does not receive the same attention. In fact, software security is hardly taught in many computer science programmes; therefore, some professional engineers and developers often lack the necessary skills to build secure software (Taylor, 2012), yet alone developers. This brings about a widespread confusion and misconceptions on many major web application security concepts among some IT personnel who have a reasonable grasp of how to secure networks and hardening of hosts (Meemeskul & Dowland, 2013; Stuttard & Marcus , 2011).

The use of web application platforms and development tools makes it easy for developers to produce powerful web applications within a limited space of time (Stuttard & Marcus , 2011). In such circumstances, creating applications does not require any technical understanding of how the applications work or the potential vulnerabilities they may contain. This lack of security awareness tends to lead developers to produce functional but insecure codes. The implication is that the majority of web applications in use today are likely to have been produced by developers who lack the technical knowledge and experience to identify security vulnerabilities. Many vulnerabilities in web applications occur because web developers concentrate much on securing the connection between the hypertext transfer protocol (HTTP) server and the web client instead of their source codes (Meemeskul & Dowland, 2013). With so many cyber security attacks taking place over web applications, developers should strive to produce secured applications to avoid/prevent potential losses to business data (Suyo, 2015). To achieve this, the level of security awareness among various developers should be increased by making them aware of potentially critical vulnerabilities, their impact on organisations and how they can be prevented.

2.2 Security concerns in web applications

The need to increase security awareness among developers arises from security concerns in web applications that have been overlooked for some time (Suyo, 2015). Research indicates that most business organisations and users have migrated most of their transactions to the Web (Kerner, 2012). This has prompted cyber criminals to follow suit and simultaneously rendering information security in web applications almost unachievable (Context Information Security, 2013). Some web applications being used are those developed or customised without addressing security concerns and could contain unknown security vulnerabilities that cyber criminals can easily utilise. The openness of the Web environment and the vulnerabilities in web applications created with less security considerations make easier for cyber criminals to create security threats that target web applications. Vulnerabilities in web applications provide cyber criminals with many options for breaching security in many organisations that use these applications (Cenzic, 2014). Some of the vulnerabilities have been well documented for years and developers do not address them during coding (Vijayan, 2009). One major reason for this situation could be that the majority of the web developers lack understanding of the security threats to web applications and effective ways of addressing the concern (Stuttard & Marcus , 2011). With the web application-based threats on the rise, there is a need to transform the way modern information technology security should be implemented and managed (Kerner, 2012). This implies that organisations that utilise web applications have to change the way they manage their information systems if they were to address the new security challenges they are facing.

Brumfield (2015)’s Verizon 2014 Data Breach Investigations Report indicates that web application vulnerabilities accounted for 35% of all data breaches in 2014. Figure 1 below depicts the distribution of data breaches in 2014.

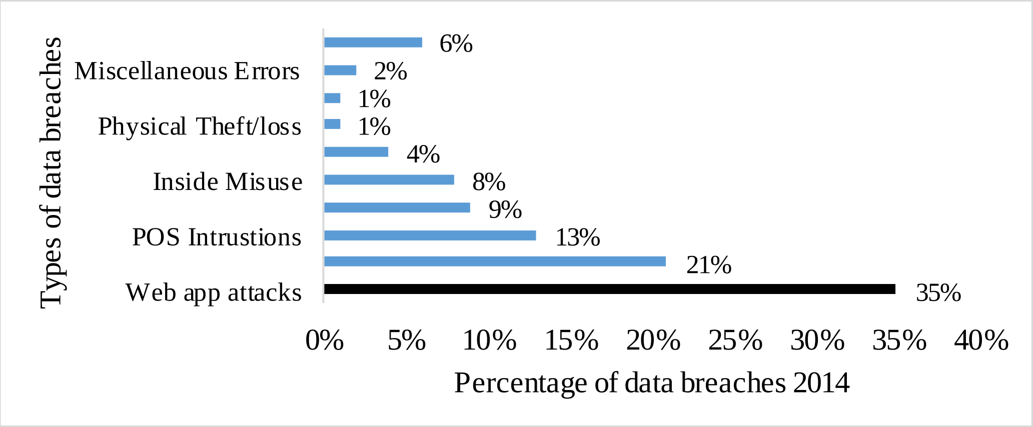

Figure 1: Verizon 2014 Data Breach Investigation Report (Brumfield, 2014)

The data on web application security indicate a cause for concern for organisations that had migrated to web applications as most of their developers always struggle with completion of projects on time in order to get compensated rather than security certification (Qualys, 2014). Literature shows that most security vulnerabilities in web applications appear to emanate from continued emphasis on time-to-market the software at the expense of secure coding practices (Vijayan, 2009). This also reveals the central point in application development in general that developers are judged according to the performance of their code rather on its security (Cenzic, 2014). This observation reinforces the notion that developers will always view software development from a different standpoint to that of security professionals unless something is done to increase their security awareness.

According to (Context Information Security, 2013)'s 3rd Annual Web Application Vulnerability Report, on average, the number of security issues affecting each web application increased from approximately 12.5 in 2010 to 13.5 in 2011, before a small decline to 12.1 in 2012. A sharp increase in new vulnerabilities was expected in 2013 to 2015 as the use of insecure web applications increased (Context Information Security, 2013). A survey on web application security conducted by (Freed, 2013), found that 99% of the web applications tested had at least one vulnerability, 82% of the web applications had at least one high/critical vulnerability, 90% of hacking incidents were not publicly reported and 30% of the hacked organisations knew of the vulnerability that led to the breach beforehand. Cenzic Application Vulnerability Trends Report (2014) also indicates that 96% of all web applications tested in 2013 have one or more serious security vulnerabilities. This would imply that the majority of the web applications-based information systems of these organisations could have been compromised at some point and also security was not an important factor in web development.

Bird and Kim (2012)'s survey on application security programs and practices, found that only 23.6% of the organisation included security in all stages of application development life cycle, 30% of the organisations indicated that security was important but developers determined where to involve the security team, 25.5% indicated that security reviews took place after the development process when the security team was trying to fix bugs in the code before full production; 18.6% of the organisations did not perform security reviews at all, Figure 2. In more than 70% of organisations application security was either taken as an afterthought process or was completely disregarded. The implication is that programmers were concerned with developing working applications disregarding the consequences of the vulnerabilities existing in their code.

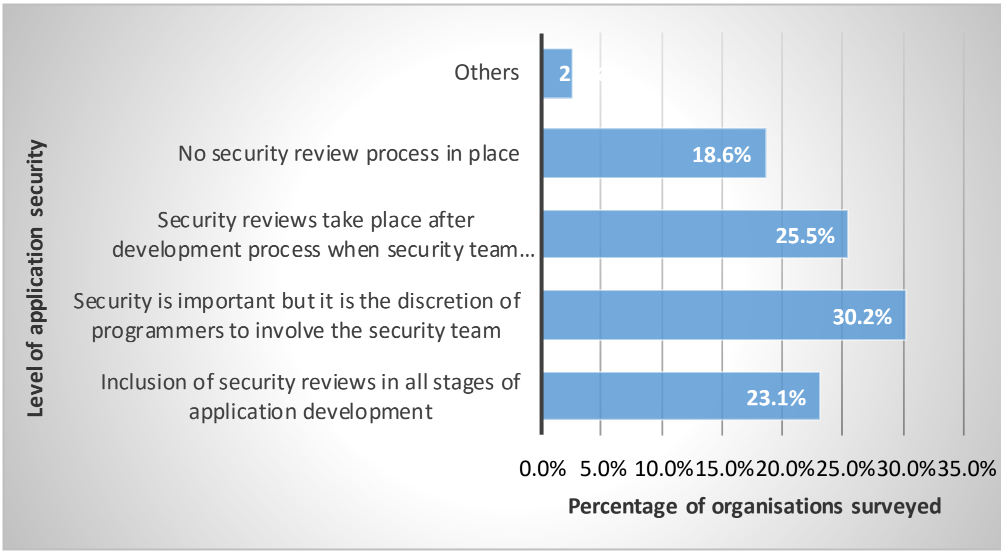

Figure 2: level of application security for internally developed application (Brumfield, 2014)

These results are cause for concern since web applications deliver their core functionality by connecting to internal computer systems that store highly sensitive data needed to perform business operations for organisations (Stuttard & Marcus , 2011). Such critical data is subsequently exposed to security threats when computers hosting insecure web applications are connected to the Internet for remote access. Attackers utilise the existing programming flows in web applications to steal valuable data, plant malicious code, penetrate deeper into the organisation network to reach internal resources and modify or destroy sensitive data (Guglielmino, 2013; Vijayan, 2009). Security breaches in web applications seem to be difficult to block even if an organisation implements the most sophisticated defence systems (Guglielmino, 2013). The best option is to include inbuilt security features within the application during application development stages.

The first challenge in web application security is web developers' inadequate knowledge of security problems associated with the applications they develop and the environment in which the applications will be used (Kerner, 2012). A number of web applications developers with partial or no understanding of web applications security problems are actively involved in developing unsecured web applications. The second challenge pertains to the use of different frameworks in web applications development for these present unique security vulnerabilities that developers tend to overlook (Context Information Security, 2013; Stuttard & Marcus , 2011). In this state of insecurity, web applications are frequently used to directly access and control valuable data in databases (Freed, 2013). This implies that a large number of web applications which are being used for business transactions today are most likely to be poorly coded and contain security vulnerabilities.

3 Related works

3.1 Types of web application security vulnerabilities

In order to develop awareness into web application security, it is imperative for developers to be acquainted with common security vulnerabilities and the dangers they pose to organisations' information systems (Cenzic, 2014; Vijayan, 2009). Application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application (DuPaul, 2015). A web application is vulnerable when it has the propensity for infiltration which may be a result of flaws within the code that makes up the application (Moen, et al., 2007). Cyber criminals exploit vulnerabilities in an application to compromise the confidentiality, integrity and availability of resources that a web application possesses (Kalman, 2015). Today, there are readily available tools and methods that cyber criminals utilise to discover web application vulnerabilities in order to compromise the applications (DuPaul, 2015). It would be highly impossible for developers to be acquainted with the devious methods used by cyber criminals. Too much investment in security gadgets by some organisations also reinforces the tendency of overlooking web application security among developers. For example, 90% of security investments are directed to network security, while 75% of the attacks that occur take place at the application layer in which over 90% of the security vulnerabilities exist (Pescatore & Orans, 2011). Overemphasis on network security and lack of awareness of application security make many organisations overlook web application security risks entirely (The Times of India, 2015). This implies that financial resources are misdirected to the network layer instead of the application layer where most of the vulnerabilities exist.

A number of reports on web application vulnerabilities seem to concur on common web application security vulnerabilities but differ on the rating of their prevalence (Brumfield, 2014). For example, Cenzic (2014) identify and rank web application vulnerabilities as shown of the Figure 1 below.

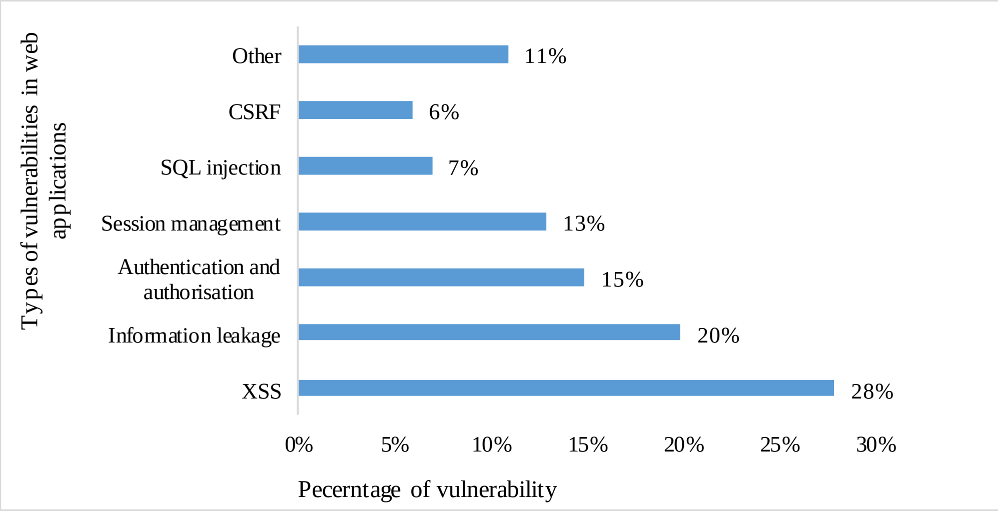

Figure 3: Distribution of types of web allocation vulnerability

(Cenzic, 2014)

These results show that up to 28% of the web vulnerabilities are exploitable through cross site scripting threats, 20% result into information leakage, 15% are due to authentication and authorisation errors, 13% occur due to session management errors, SQL inject accounts for 7%, cross site request forgery also accounts for 6%.

The Open Web Application Security Project (OWASP) (2014) also identifies and defines its top 10 web application vulnerabilities that web application developers should be aware of and encouraged to prevent in their applications. This paper briefly explores the top five web vulnerabilities as identified by (OWASP, 2014).

Structured query language (SQL) injection is a security vulnerability in which an attacker is able to submit a database SQL command that a web application executes, exposing the back-end database (Partington & Xebia, 2005). SQL injection contributes over 20% of all web application vulnerabilities (DuPaul, 2015; OWASP, 2014; Sadalkar, Mohandas & Pais, 2011). A SQL injection attack technique usually tricks the database to execute unintentional commands or change data (DuPaul, 2015; Sadalkar, et al., 2011). An attacker uses SQL injection to manipulate (create, read, update, alter or delete) data stored in an organisation's back-end database by exploiting a security vulnerability in the application layer (Kalman, 2015). To address this problem, web developers should be aware of SQL injection vulnerability, prioritise how to locate and prevent/minimise it in web applications they develop. This can be achieved by writing code that validates or encodes user-supplied data.

A Broken authentication and session management attack usually takes place whenever there is session hijacking or false authentication on a web application (Charu & Deepika, 2014). This vulnerability is due to web application functions for authentication and session management that are incorrectly implemented and hence, allow cyber-attackers to compromise passwords, keys, session tokens or to exploit other implementation flaws to assume other users' identities (Gupta, 2011). Developers frequently produce flawed custom authentication and session management schemes in web applications and these are normally difficult to locate due to unique implementations (Sundar, 2014). Cyber-attackers use leaks or flaws in the authentication or session management functions to perpetuate their malicious intentions on vulnerable web applications. Although developing error-free authentication and session management schemes is an essential component of web application security, it is one of the areas in which web application developers face serious challenges that require immediate redress (Charu & Deepika, 2014). This implies that poorly developed web applications have flaws which result in incorrect implementation of authentication and session management. Such applications do not enforce unbreakable and unrepeatable authentication and authorisation mechanisms. It becomes simple for cyber-attackers to guess passwords and personify themselves as authorised web application users further compromising the confidentiality, integrity and availability of critical information of an organisation.

Cross-Site Scripting (XSS), vulnerabilities always target scripts that a developer embeds in a web application page being executed on the client-side, the web browser instead of the server-side (DuPaul, 2015; Open Web Application Security Project OWASP, 2014). Internet security weaknesses of client-side scripting languages such as HyperText Markup Language (HTML) and JavaScript act as security holes for XSS threats (Kalman, 2015). An XSS vulnerable web application accepts users' data and dynamically inserts it in web pages without first properly validating it. The attacker is able to take control of the user's browser or account and execute malicious code that displays arbitrary content on the browser (Kalman, 2015). By utilising the XSS vulnerability a cyber-attacker is able to by-pass security controls in the web application and executes malicious codes in the context of the session of the victim. It has been observed that web application developers tend to ignore filters that block any malicious activities due to user input data (Shankdhar, 2013). This could be a result of ignorance on the part of the developers on the need for securing the applications.

Insecure Direct Object Reference is a vulnerability in a web application which provides direct access to objects based on input that the user supplies. Insecure Direct Object References is a widespread web application security vulnerability that allows requests to be made to specific objects through pages or services without the proper verification of requester's right to the content (Wang, 2014). This flaw takes place when a programmer exposes a reference to an internal implementation object, such as a file, directory, or database key (OWASP, 2014). Without an access control check or other protection, attackers can manipulate these references to access unauthorised data (OWASP, 2014). This programming flaw provides an easy way for cyber-attackers to bypass authorisation in order to access critical information resources stored on web servers. In this case direct object reference vulnerabilities take place when there are insufficient authorisation checks carried out against object identifiers used in requests.

Security misconfigurations are poorly configured security controls in web applications, as the name implies. The OWASP (2013) identifies a security misconfiguration as a critical web application security vulnerability and places it in the top five common security vulnerabilities. These security misconfigurations can exist at any level of a web application such as the platform, web server, application server, database, framework, and also custom code (GitHub Security, 2015). Application security misconfiguration attacks and exploit configuration weaknesses or flaws that exist in a web application (Cornell, 2013). By exploiting security misconfigurations, cyber-criminals are able to circumvent system authentication methods and gain unauthorised access to sensitive information, compromise files, or even perform unintended actions. Relying on default security settings tends to lead to security misconfigurations. Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform.

Having explored the security problems in web applications, the following subsection discusses the importance of security awareness in web application development.

3.2 The need for security awareness among web application developers

Research indicates that most security breaches in web applications occur in the application layer due to insecure code that developers produce (Context Information Security, 2013). Vulnerabilities in web applications considered urgent are normally not fixed because developers are always too busy to work on web applications security issues; web developers believe that fixing vulnerability in a web application takes a lot of their programming time; and web developers regard web application security as not being a corporate priority (Ponemon Institute, 2013). It could be deduced from this report and other arguments raised before that there is a need to focus more on web application security awareness among web developers than application users.

Many web application developers tend to be inexperienced graduates from tertiary institutions who lack security skills and knowledge in this dynamic field. Such developers are usually more concerned with the functionality of their applications than security aspects. Most organisations who hire these developers are also ignorant in web security matters. In most organisations, there are hardly any security specialists to conduct security tests on web applications before they are deployed. This implies that the majority of such web applications are unsecure and they make information systems in organisations unsecure and be at risk to cyber-attacks.

Most of the current vulnerabilities in web applications are well documented yet web application developers still produce applications prone to attack through similar vulnerabilities. This serves as an indicator for the need to raise the level of security awareness among developers. A number of strategies for increasing the level of security awareness among web application developers are suggested in this paper. Subsection 4 below deals with approaches that could be used to raise awareness among web developers.

4 Possible approaches to raise security awareness for web application developers

Many web application security initiatives on offer seem to be inaccessible by web developers and as a result these developers remain marginalised (McElroy & Weakland, 2013). Existing security initiatives also focus more on security personnel and use of existing technology to address web application security than developer's skills and knowledge in dealing with security issues at code level (Cenzic, 2014). For this reason, OWASP (2014) and (Merkow & Raghavan, 2010) advocate for security awareness approaches that address process, technology and developers' problems in an organisation. Bird and Kim (2012) (Bird & Kim, 2012) surveyed application security approaches used by various organisations to foster security awareness among software developers. Figure 3 shows results of the survey.

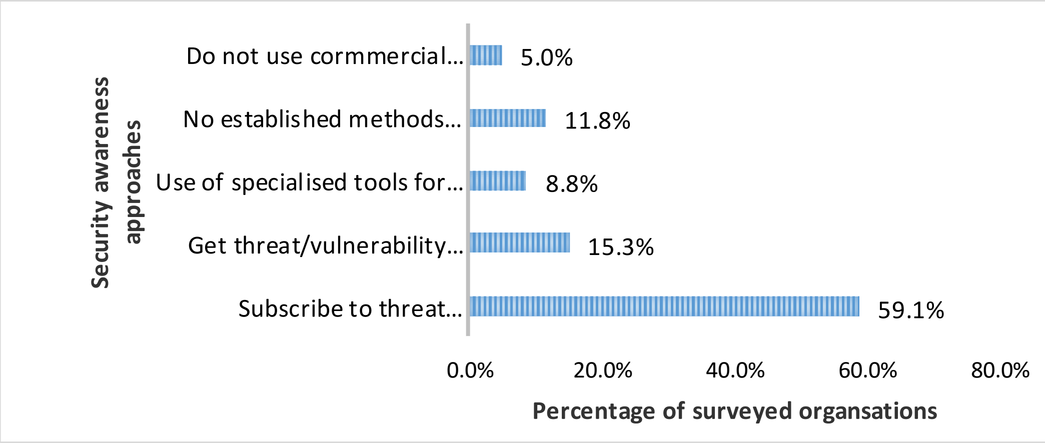

Figure 4: Application security vulnerability awareness approaches

(Bird & Kim, 2012)

The above security awareness approaches were based on external sources, 75% of organisations (59.1% and 15.3%), 8.8% utilised specialised tools to get vulnerability information, 11.5% did not have any established security awareness approach to track vulnerabilities and yet 5% used own developed software. It is not clear how developers for these organisations were involved in web application securities particularly in-house developed. Similarly, a number of authors who emphasise the need for web application developers to be proactive in addressing security issues in their web applications suggest peripheral activities that would not foster long term security awareness among web developers (Taylor, 2012; Cornell, 2013).

This paper discusses the possibility of using a blend of traditional and contemporary security awareness approaches to increase level of security awareness among web developers. The first option to secure web application is security awareness from web developers implying that the hands-on security awareness approach is the most appropriate choice to achieve this feat. Hands-approaches have the potential to provide developers with an opportunity to develop crucial skills in securing web application at code level. Suggested traditional methods include workshops, targeted risk identification and prevention activities, computer based training while contemporary methods would involve methods such as online video training and security discussion groups. Traditional methods are used to initiate programmers to secure coding while contemporary methods support them while at their work places.

Workshops on web security: These consist of activities designed to promote learning, discussions and feedback about web application security topics or brief for a small group and emphasising problem-solving in an identified deficient area (Spagnoletti, et al., 2013). Workshops provide a form of outreach and participation that enable deep-rooted industry initiatives for software security (Lackey, 2012). Properly planned workshops can always maintain continuous interaction among developers and security specialists who assist novice developers' access to proposed tools, processes and emerging best practices (McElroy & Weakland, 2013). In our context workshops focus on particular aspects of web application security in which developers learn from experts, such as, how to identify SQL injection vulnerability in the code and also fixing the bug. Of paramount importance, web application security workshops should ideally, devote significant time to hands-on safe coding activities such as:

- code review, flaw and vulnerability identification in design
- applying security-specific activities at each stage of design
- techniques in input validation
- various approaches to web security design
- application testing for vulnerability

Hands-on activities have the potential to make developers to realise the importance of using security specific processes when creating web applications and also the need to guard against security violations. In workshops, developers can also be trained on basic secure coding techniques to ensure that they do not introduce vulnerabilities during the authoring of the application. Workshops can also provide security specialists to demonstrate how to use vendor-security tools on security tools scan for security vulnerabilities in applications they develop. Suggested hands-on activities would include basic security in input validation and language specific instructions on security. By giving developers insight on security practices for the language and runtime environment for which they develop applications for leverage better coding practices that consequently reduce errors in the final web application.

Targeted risk identification and prevention activities: These are informal or formal activities designed to raise security awareness among developers by providing them with opportunities to examine their code with the intention of identifying security loopholes. In this, case developers are presented with various codes that have security vulnerabilities and allowed to identify the code flaws and also how they could be exploited. These activities are then repeated using the developer's own codes. In the long run, the developers become aware of the vulnerability in their code and also the threats likely to exploit those flaws. This will also provide the developers with opportunities to explore several appropriate ways of reducing and preventing the flaws in the code in order to reduce or eliminate the security risks. This would require developers to work under an experienced security expert in web application development.

Computer-based awareness training for secure coding: This involves delivering awareness material through a computer utilising various methods of delivery options such as text, audio, video, interactive quizzes and screenshots (Gardner & Thomas, 2014). The materials are easy to customise to meet the needs of group of developers who will be at different stages of security awareness. Computer-based training materials are easier to distribute using CD-ROM and later transferred to the computer hard drives for use by different web developers at their various places. This makes it easy to distribute awareness materials to different places where there is limited internet access.

Online video training on security vulnerabilities: Traditional personalised awareness programmes are usually expensive and time consuming while awareness manuals are unpopular because they are impersonal. Online awareness programme including videos provide a good alternative method to foster security awareness to developers. Online videos have a potential to deliver security awareness material which are interactive and interesting to different audience under different circumstances (Gardner & Thomas, 2014). The materials on videos can be customised to cover small segments of large topic in a short amount of time. Video awareness programmes are flexible in that they can be used to cover any learning materials deemed suitable for any group of learners. It would be far more effective for web developers to learn aspects of web security through visual methods if code snippets are presented and the explanations given. Another advantage of online video programmes is that developers will access the material at their desk at the any time that suits them. This can be reinforced by using posters and e-mails on topical issues.

By participating in security awareness programmes, developers could understand basic principles of secure software development, and learn to identify where web applications diverge from those principles (Meemeskul & Dowland, 2013; Pearson, 2015). In this way, security awareness efforts for web developers aim to bring about behaviour change while reinforcing good security practices among inexperienced developers (Wilson & Hash, 2003). Behaviour change is a result of on-going exposure to the right security awareness experiences that raise security interest among developers. The most important part of generating security awareness is ensuring that developers receive regular security awareness training (Pearson, 2015). An effective security awareness programme should seek to equip knowledge and to expose developers or those who maintain the web application source code to security standards and best practices (Russell, 2002). In our opinion, developers should be able to perform application testing in order to identify security flaws introduced in all stages of development (design, implementation and deployment) of a web application. Furthermore, developers should be able to identify those functions that are critical to security and perform test on those functions to verify whether they operate correctly.

However, there are challenges likely to arise from the approaches used to raise awareness among developers. The challenges are discussed in the following section.

5 Challenges in awareness programmes for web developers

An awareness programme starts with awareness, followed by training and then evolving into education. Security awareness programs are meant to focus web developers' attention on security issues or collection of security vulnerabilities. However, there are always challenges in getting awareness messages and content to the intended audience. With vast of approaches available to make the materials available to the developers, problems that need to be dealt with include the preparedness of the developers to learning more about web security. They have to overcome the tension between the need to build as many insecure web applications to meet the target and the need to build few but secure applications. Secondly, it would also be a challenge to reach these developers since most of them are not members of professional bodies and regulating their activities would also provide another challenge.

6 Conclusion and future research

Web applications will remain the weakest security point in many organisations where developers are failing to sufficiently address security vulnerabilities in their code. As the demand for web applications escalates, new players in the form of developers produce applications for financially disadvantaged business organisations. Most web developers are ignorant of web security vulnerabilities that exist in the code they produce and the effects such codes might have on the security of information systems of organisations using such applications. It is worthwhile to provide security awareness programmes to developers utilising many possible approaches regardless of the challenges that exist. Developing secure web applications can be achieved if web developers have a high level of security awareness and apply this during web development rather than later.

It is therefore, suggested that further empirical research studies to assess the level of security awareness among developers be conducted; the findings of these studies be used to formulate and develop appropriate security awareness frameworks for web developers.

7 References

Awoleye, O. M., Ojuloge, B. & Ilori, O. M. (2014). Web application vulnerability assessment and policy direction towards a secure smart government. Government Information Quarterly Volume 31, Supplement 1, 14 June 2014, p. 118–25.

Bird, J. & Kim, F. (2012). SANS survey on application security programs and practices. December 2012. A SANS Whitepaper. Available at: http://www.sans.org/reading-room/whitepapers/analyst/survey-application-security-programs-practices-35150 [Accessed 30 June 2015].

Brumfield, J. (2014). Verizon 2015 Data Breach Investigations Report. [Online] Available at: http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/ [Accessed 26 June 2015].

Cenzic, (2014). Application Vulnerability Trends Report: 2014. [Online] Available at: https://www.info-point-secrity.com/sites/default/files/cenzic-vulnerability-report-2014.pdf [Accessed 12 June 2015].

Charu, N. & Deepika, V. (2014). Cross Site Scripting Attack and Broken Authentication and Session Management Attacks. Progress In Science and Engineering Research Journal, 4(2), pp. 190-193.

Context Information Security, (2013). Web apps still a cause for concern according to Context Information Security. Web Application Vulnerability Statistics 2013. [Online] Available at: http://www.realwire.com/releases/Web-apps-still-a-ca [Accessed 21 March 2015].

Cornell, D. (2013). Tackling Web application security through secure software development. [Online] Available at: http://searchsecurity.techtarget.com/feature/Tackling-Web-application-security-through-secure-software-development [Accessed 14 March 2015].

DuPaul, N. (2015). Common Web Application Vulnerabilities. [Online] Available at: http://www.veracode.com/security/web-application-vulnerabilities [Accessed 21 March 2015].

Freed, A. (2013). Web Application Vulnerability Statistics Report Released. [Online] Available at: http://www.corero.com/blog/329-web-application-vulnerability-statistics-report-released.html#sthash.nm0Sgacy.dpuf [Accessed 15 June 2015].

Gardner, B. & Thomas, V. (2014). Building an Information Security Awareness Program: Defending Against Social Engineerig Technical Threats. Bristol City: British Library Cataloging.

GitHub Security, (2015). Security Misconfiguration. [Online] Available at: https://bounty.github.com/classifications/security-misconfiguration.html [Accessed 15 April 2015].

Guglielmino, E. (2013). Application Security in the Software Development Life cycle: Issues, Challenges and Solutions. [Online] Available at: http://www.quotium.com/content/uploads/2014/01/Seeker-Application_Security_in_the_SDLC.pdf [Accessed 10 April 2015].

Gupta, P. (2011). Broken Authentication and Session Management, SQL Injection. [Online] Available at: http://www.idrbt.ac.in/PDFs/PT%20Reports/2011/PuneetGupta_BrokenAuthentication_2011.pdf [Accessed 17 March 2015].

Hentea, M. (2005). A Perspective on achieving Security awareness. Issues in Informing Science and Information Technology, 24 September, pp. 15-38.

Kalman, G. (2015). 10 Most Common Web Security Vulnerabilities. [Online] Available at: http://www.toptal.com/security/10-most-common-web-security-vulnerabilities

Kerner, M. S. (2012). Why Are Web Applications a Security Risk? [Online] Available at: http://www.esecurityplanet.com/trends/why-are-web-applications-a-security-risk.html [Accessed 10 April 2015].

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers and Security, 25(2), pp. 289-296.

Lackey, Z. (2012). Effective approaches to web application security. [Online] Available at: https://www.owasp.org/images/b/b4/Effective_approaches_to_web_application_security.pdf [Accessed 17 June 2015].

McElroy, L. & Weakland, E. (2013). McElroy, L. & Weakland, E. 2013. Measuring the Effectiveness of Security Awareness Programmes., Educause. [Online] Available at: https://net.educause.edu/ir/library/pdf/ERB1310.pdfm [Accessed 20 March 2015].

Meemeskul, T. & Dowland, P. S. (2013). Investigating Options of Securing Web Application. [Online] Available at: Https://www.cscan.org/download/?Id=716. [Accessed 23 April 2015].

Meier, J. D. et al. (2003). Improving Web Application Security: Threats and Countermeasures, Microsoft Corporation. [Online] Available at: https://msdn.microsoft.com/en-us/library/ff648647.aspx [Accessed March 12 2015].

Merkow, S. M. & Raghavan, L. (2010). Secure and resilient software development. Boca Raton: CRC Press, Taylor & Francis Group.

Moen, V., Klingsheim, A. N., Simonsen, K. I. & Hole, K. J. (2007). Vulnerabilities in egovernments. International Journal of Electronic Security and Digital Forensics,, 1(1), p. 89–100.

OWASP, O. W. A. S. P. (2014) 2013 Top 10 2013-Top 10 Vulnerabilities. [Online] Available at: https://www.owasp.org/index.php/Top_10_2013-Top_10 [Accessed 21 March 2015].

Partington, V. & Xebia, K. E. (2005). Top Ten Web Application Vulnerabilities in J2EE. [Online] Available at: https://www.owasp.org/images/2/2e/OWASP_NL_Top_Ten_Web_Application_Vulnerabilities_in_J2EE.pdf [Accessed 23 April 2015].

Pearson, A. (2015). How to Train Secure Web Application Developers. [Online] Available at: http://www.securityinnovationeurope.com/blog/how-to-train-secure-web-application-developers [Accessed 28 June 2015].

Pescatore, J. & Orans, L. (2011). Enterprise Strategies for Mitigating Denial-of-Service Attacks [Online] Available at: https://www.gartner.com/doc/1759917/enterprise-strategies-mitigating-denialofservice-attacks [Accessed 23 March 2015].

Petukhov, A. & Kozlov, D. (2008). Detecting Security Vulnerabilities in Web Applications Using Dynamic Analysis with Penetration Testing. [Online] Available at: https://www.owasp.org/images/3/3e/OWASP-AppSecEU08-Petukhov.pdf [Accessed 23 September 2015].

Ponemon Institute, (2013). Ponemon State of Web Application Security Report. [Online] Available at: http://www.applicure.com/blog/ponemon-state-of-web-application-security [Accessed 15 February 2015].

Qualys, (2014). Six Essential Elements of Web Application Security: Cost Effective Strategies for Defending Your Business. [Online] Available at: https://www.qualys.com/docs/whitepapers/qualys-six-essential-elements-web-application-security.pdf [Accessed 25 June 2015].

Renfroe, N. A. & Smith, J. L. (2011). Threat/Vulnerability Assessments and Risk Analysis. [Online] Available at: http://www.wbdg.org/resources/riskanalysis.php#top [Accessed 25 June 2015].

Russell, C. (2002). Security Awareness- Implementing an Effective Strategy. [Online] Available at: http://www.sans.org/reading-room/whitepapers/awareness/security-awareness-implementing-effective-strategy-418 [Accessed 23 June 2015].

Sadalkar, K., Mohandas, R. & Pais, R. A. (2011). Model Based Hybrid Approach to Prevent SQL Injection Attack in PHP. Haldia, nfoSecHiComNet.

Shankdhar, P. (2013). How to Prevent Cross-Site Scripting Attacks. Application Security. [Online] Available at: http://resources.infosecinstitute.com/how-to-prevent-cross-site-scripting-attacks/ [Accessed 23 March 2015].

Spagnoletti, C., Bonnema, R., McNeil, N. & Spencer, M. (2013). Workshop Preparation and Presentation: A Valuable Form of Scholarship for the Academic Physician. [Online] Available at: https://www.aamc.org/download/358432/data/toolkitworkshoppresentations.pdf [Accessed 20 March 2015].

Stuttard, D. & Marcus , P. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition. John Wiley & Sons, Inc., Indianapolis. [Online] Available at: https://leaksource.files.wordpress.com/2014/08/the-web-application-hackers-handbook.pdf [Accessed 13 March 2015].

Sundar, V. (2014). Strong Authentication Meaningless - if Authenticated Session management is Weak. [Online] Available at: https://www.linkedin.com/pulse/20140817070548-4298133-strong-authentication-meaningless-if-authenticated-session-management-is-weak [Accessed 3 May 2015].

Suyo, E. (2015). How to Fix Common Web Application Vulnerabilities. [Online] Available at: https://blog.elearnsecurity.com/top-5-common-web-vulnerabilities-and-how-to-fix-them.html [Accessed 14 March 2015].

Taylor, J. (2012). Want to Reduce Application Security Risk? Build more Secure Software. [Online] Available at: http://blog.securityinnovation.com/blog/2012/05/want-to-reduce-application-security-risk-build-more-secure-software.html [Accessed 25 March 205]. [Accessed 14 March 2015].

The Times of India, (2015). IT managers must watchout for web apps-related security breaches: Report. [Online] Available at: http://timesofindia.indiatimes.com/tech/tech-news/IT-managers-must-watchout-for-web-apps-related-security-breaches-Report/articleshow/47747401.cms [Accessed 15 June 2015].

Vijayan, J. (2009). Web application security is growing problem for enterprises. [Online] Available at: http://www.infoworld.com/article/2630437/web-applications/web-application-security-is-growing-problem-for-enterprises.html [Accessed 16 February 2015].

Wang, H. (2014). Preventing Insecure Direct Object References in App Development. [Online] Available at: https://tuftsdev.github.io/DefenseOfTheDarkArts/students_works/final_project/fall2014/hwang.pdf [Accessed 8 February 2015].

Wilson, M. & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. [Online] Available at: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf [Accessed 4 March 2015].

A Solution to improve the cyber security of home users

Basie Von Solms & Jonathan Roussel
University of Johannesburg, Johannesburg, South Africa, 2000
basievs@uj.ac.za ,jonathan23@live.co.za

Abstract

The past few years have seen cyber criminals shifting their focus of attacks away from a few large bodies (such as large enterprises) to many smaller bodies. The reason is that large enterprises have numerous security measures in place and it therefore requires considerable time to subvert their systems. Smaller organisations have much less security in place and it therefore requires minimal time to subvert their systems. Cyber criminals are creating increasingly sophisticated attacks. Current attacks aimed at small bodies involve installing malicious software on users' machines, collecting data, logging key strokes, viewing users' computer screens and turning on users' microphones or cameras, to name but a few. Information collected can be used to launch an attack or even allow for identity theft, which in many cases is aimed at looting money from victims. Currently, the small bodies or victims of cyber attack are small companies and home users who make use of personal computers at home. This paper will investigate this aspect with the main objective of illustrating a solution to improve the cyber security of home users who make use of personal computers at home.

Keywords

Cyber Security, Home Users, Cyber Crime

1. Introduction

It has been documented that home users are increasingly becoming the targets of cyber attack [10], [22]. This paper investigates home users as targets of cyber attack and provides a solution to aid in their security.

Home users are on their own with the sole responsibility of protecting themselves from cyber attack, which leaves them to rely upon their own knowledge to protect themselves [10]. Home users, however, lack the knowledge and technical skills needed to secure their information and themselves [18], which means that it is unlikely that they will be secure [10].

It is widely accepted that home users are currently the targets of cyber attacks as it is very difficult for them to secure their computer systems comprehensively.

In this paper we investigate how the security of home users can be improved by moving most of the security responsibility away from them to another body.

Our main objective is to develop a prototype to help home users protect their systems by taking many security responsibilities away from them.

Sections 1 through 3 investigate home users as targets of cyber attack. Section 4 takes a look at who's responsible for the cyber security of home users. Section 5 examines the idea of shifting cyber security away from home users as a way in which to create a safer cyber environment for them. Section 6, 7and 8 take a look at Internet service providers, cloud computing and Chromebook respectively as solutions for taking cyber security responsibility away from home users. Section 9 investigates the main, partial functionality of the solution named SecureLink for aiding in the cyber security of home users by shifting many cyber securities away from them.

2. What makes home users targets of cyber attack?

There are several reasons leading to home users being targets of cyber attack [10], [18].

Home users are on their own with the sole responsibility of protecting themselves from cyber attack, which leaves them to rely upon their own knowledge to protect themselves [10]. Home users, however, lack the knowledge and technical skills needed to secure their information and themselves [18], which means that it is unlikely that they will be secure [10].

Several reasons account for home users being the target of attack, some of which are as follows [10]:

- Users lack security awareness.
- They use weak passwords.
- They allow software licences to lapse.
- They forget to download patches for their software.
- Users do not set correct settings.
- They do not keep tabs on new technology.

3. The attack landscape of home users

As in the past, unpatched systems and application vulnerabilities are the main reason that most systems are compromised [22].

It is well documented that cyber criminals are shifting their focus of attack to platforms which home users are making use of [13], [21], [22].

It can be seen from the literature listed above that:

The use of email as an attack vector has decreased with the rise in popularity of the mobile and social networking platform. These platforms offer a new dimension to attacking home users. Spam, malware and phishing attacks have been seen to take place and increase in number on these chosen platforms.

In contrast to traditional PC attacks, mobile attacks are not linked to mobile vulnerability but rather to mobile architecture. Android’s architecture allows for the use of rogue apps (cloud applications) which could easily contain malware. This is a far easier way than having to locate and make use of vulnerabilities as with traditional computers. It is expected that mobile vulnerabilities will be made use of to compromise devices in the future.

Mobile malware is on the rise with the main objective being to steal sensitive information from victims.

The distribution of malware and spam as well as phishing and spoofing attacks are increasingly taking place on the social networking platform. Spam takes the form of fake offerings such as survey scams and free gift cards where a user gives up personal information to retrieve such an offer. Phishing takes the form of fake websites which target a user’s interest in, for example, famous athletes or actors. These websites require a user’s social media login credentials to login.

The mobile and social networking platforms, offer more exposure to personal information and provide attackers with many new ways to steal personal information which cyber criminals can make use of to achieve any of the following [22]:

- Take over a user’s account

- Assume a victim’s identity

- Infect a victim's computer with malware

- Supplement spam and phishing attacks

It is clear that cyber criminals, even though focusing on new mediums, have not abandoned the email platform as a medium for attack nor has there been a decrease in malware destined for traditional PCs [13].

4. Who is responsible for protecting home users?

One could argue that the role players involved in providing users with computing facilities should have the responsibility to protect home users which include computer manufacturers, OS developers, application developers and Internet service providers (ISPs). These role players do provide security features with their products but users are still vulnerable to attack due to their bad habits of not using or maintaining these features [11] as discussed in section 2.

A viable solution would be to train users through an awareness programme on how to use and maintain their system with the security it provides and other related security issues. However, there is a flaw in this strategy in that there is no way of knowing whether the awareness information provided to users is in fact read and understood [10]. To overcome this, it would better to provide the user with security technologies in such a way that they work seamlessly and on the fly with little or no intervention by users. This means that users will need very little or no knowledge of how to manage these technologies [10].

5. Shifting cyber security responsibility away from the user

Home users are currently responsible for all their cyber security and are referred to as thick clients [10]. Our objective, as we stated in section 1, is to shift cyber security away from home users in order for them to have minimal security responsibility, referred to as thin clients [10].

6. Internet service providers (ISPs) as a viable solution to take cyber security responsibility away from home users.

There have been attempts to produce legislation for securing user computers but these have encountered the following problems [16]:

- Around the time the Internet was born, the design of OSs allowed for adding a security component when needed, leading to the issue that any computer bought even today would not have an up-to-date OS. A solution to this would be to redesign the OS with security as a main component. The problem with this, however, is that it would take several years to market.

- Computer software is another barrier to legislation. Forcing software companies to redesign their software with security as a main concern would take a very long time.

Due to the time it would take for application developers to redesign their products and for OS developers to market their products, both with security as a main component, the only other party left to take on the responsibility of mitigating threats is ISPs. Internet Service Providers (ISPs) act as an interface between clients and the internet and have the ability to monitor Internet traffic [9], making them suitable to act on this traffic [5], [19]. There are several ISPs currently taking on some cyber security responsibilities [1], [2], [8], [18] and several governments getting involved with ISPs taking on such responsibility [4], [5], [18]. Even though in a prime position to take on cyber security responsibilities, research shows that there are several Issues against ISPs taking on such responsibility which hinders the progression of ISPs in this domain [5], [16], [18].

7. Cloud computing as a viable solution to take cyber security responsibility away from home users.

- Due to the issues limiting ISPs from taking on cyber security responsibilities, another solution that meets the objective of shifting responsibility away from home users is cloud computing.

- From the following literature we found that [6], [12], [15], [17], [20], [22], [23]:

- Any services/applications are always the latest, most up-to-date version. The only way a system could be compromised is through zero-day vulnerabilities.

- It was stated in section 3 that unpatched vulnerabilities are the main reason that most systems are compromised. Unpatched application vulnerabilities are eliminated with cloud computing applications as they are updated on the fly by service providers.

- Cloud computing has overcome the problem of computer software being a barrier to legislation aimed at securing user computers as discussed in section 6, as applications are merely transformed into cloud applications. This is done by software vendors in a timely manner.

- Cloud applications are more secure than traditional applications because updating and security settings are made by software service providers.

- Cloud applications take the responsibilities of maintaining and updating applications (including cloud security applications) away from users, but users still have the respective responsibilities for their OS.

- In terms of applications, when looking at section 2, we see that following responsibilities are taken away from users via cloud computing:

    - Setting correct settings for applications

    - Not allowing a lapsed licence of an application to affect a client's machine

    - Protecting a user's sensitive data

    - Backing up a user's data

- For some devices, most of their applications are cloud based while for others, all applications are cloud based, which renders the device, referred to as a thin client, useless without an Internet connection.

In terms of our main objective pointed out in section 1, it is clear that the architecture of cloud computing has the ability to shift cyber security responsibility away from users and in doing so, provides for a more secure environment for home users. However a limitation of cloud applications is that an internet connection is needed at all times for users to effectively make use of them.

8. Chromebook as a viable solution to take cyber security responsibility away from home users.

It was pointed out in section 6 that a solution to the problem of current OSs, any computer bought even today would not have an up-to-date OS, would be to redesign the OS with security as a main component and that the problem with this is that it would take several years to market.

From examining the following literature we found that [7]:

Chromebook is a new type of computer with an operating system called Chrome OS and applications which are all cloud based. Being cloud based means that all applications are always up to date and have no functionality without an Internet connection. With Chromebook however, Google has made its products partially available when offline [24].

Chrome OS has been made with automatic updating and self checking capabilities. Each time a Chromebook is booted, it performs a self check and updates in less than 10 seconds. The self check is named the verify boot process where each time the system is booted, it determines if the OS has been tampered with or corrupt whereby the OS will be restored from a known local backup or from the cloud if tampering has been detected.

Chromebook also offers sandboxing [19] and jailing of applications.

In section 3, it was stated that unpatched system and application vulnerabilities are the main reason that most systems are compromised. With Chromebook, the Chrome OS and all applications update automatically without user intervention meaning that unpatched system and application vulnerabilities will not occur in Chromebook.

From an analysis of all the security features of Chromebook [7], the following responsibilities were found to have been taken away from home users:

- Many security aspects which a home user would have to be made aware of have been taken away from users

- Updating or maintaining the OS, as this occurs at every boot up as well as when an update becomes available. Updating and maintain applications is also taken away from users.

- Setting correct settings for the OS and applications

- Chromebooks have an OS that receives updates forever; no annual licence is needed so a licence cannot lapse. Applications can not cause vulnerabilities if their licences lap due to Chromebooks sandboxing mechanism.

- Protecting sensitive data through encryption
- Backing up data with Google Drive
- Reformatting the OS if any unauthorised changes have been made
- Plug-in management and automated updating
- Monitoring phishing sites and sites containing malware
- Eliminating dead applications
- Eliminating malware through email
- The need to keep tabs on new technology
- The need to source and maintain the correct security for themselves □ Identifying and avoiding the following social media attacks:
    - Likejacking
    - Fake plug-in scams

When assessing the responsibilities left to users by Chromebook, the following were found:

The need to create strong passwords

Overcoming phishing, which the Chromebook does to a certain extent

Identifying some social networking attacks which include spoofing, spam, phishing, fake offerings, manual sharing scams and copy and paste scams

Keeping safe on mobile devices

It was stated earlier in this section that the problem with redesigning the OS with security as a main component is that it will take several years to market. This has not been the case for Chromebook. In terms of market sales Chromebook was the top selling Notebook on Amazon.com, constituting 25% of Notebooks sold for less than US$300 [14]. Computer maker Acer had more sales of Notebooks using the Chrome platform (5 to 10% of Acer’s US shipments) after the release of Windows 8 by Microsoft, which failed to ignite the market [3].

9. SecureLink as a viable solution to take cyber security responsibility away from home users.

With the Chromebook being the most in line with our objective, we based our prototype on this model. To achieve our objective, we focused on those remaining cyber security responsibilities Chromebook left in the hands of home users. For these remaining responsibilities, we created a Virtual Extension of Chromebook to shift as many of those remaining security responsibilities away from home users. We refer to Chromebook and the Virtual Extension of Chromebook as SecureLink. We refer to the

SecureLink virtual extension component as SL-VE for short. This section illustrates the basic functionality of SL-VE only, only a part of the functionality of the actual prototype.

With social networking being the most popular activity on the Internet [22], and being a new platform for attacking victims as stated in section 3, solving social networking security issues became our first priority of those responsibilities left to users by Chromebook as stated in section 8.

As stated in section 3, the mobile and social networking platforms, offer more exposure to personal information which cyber criminals can make use of to achieve any of the following:

- Take over a user’s account
- Assume a victim’s identity
- Infect a victim’s computer with malware
- Supplement spam and phishing attacks

We found that, in the case of 1 and 3 above, instead of collecting personal information, it would be quicker to steal login credential through:

- A phishing website spoofing a known site.
- A phishing site that targets a user’s interest which requires social networking login credentials, as we stated in section 3.

Therefore our focus for SL–VE was to better protect login credentials. This meant:

- Stronger passwords
- The elimination of phishing sites spoofing social networking sites
- The elimination of phishing sites that target a user's interest which requires social networking login credentials

For this reason we created the Virtual Extension of Chromebook, SL-VE.

SL-VE was developed as a web based application as Chromebook does not allow for any applications to be installed on it. If a user wants to navigate to a desired website, the user must first copy the web address and paste it into SL-VE. This process places some responsibility on users but only because SL-VE cannot be installed on Chromebook.

For any legal website to which a user is required to log in, the user needs to have an account on that legal website. To gain access to their account, the user needs to input their username and password combination.

SL-VE links the legal website address with the username and password combination used for the legal website in question. In SL-VE, there are two stages to the process of username, password and website linking. These are enrolment and validation. In stage 1, the enrollment stage, the legal website address, and associated username and password combination of each website must be registered into SL-VE, which is then saved. In stage 2, the validation stage, the desired website address and associated username and password combination must be input into SL-VE.

If the username and password issued in stage 2 match the username and password for a legal website enrolled in stage 1 and the desired website is the same website which was issued in stage 2, the website is safe (assuming that the website enrolled in stage 1 is legitimate).

If the username and password in stage 2 match the username and password for a legal website enrolled in stage 1, but this desired website is not the legal website issued in stage 2, it indicates one of the following:

- The user made a mistake by inputting the incorrect website address
- A phishing site spoofing a known site
- A phishing site, which targets a user's interest in, for example famous actors or athletes.

Thus with these two stages, spoofing and phishing websites can be signalled.

For SL-VE to work, the following conditions must be met:

- The same username–password pair may not be used on more than one legal site

- Authentic legal website addresses/URL’s need to be registered with SL-VE (by an administrator of SL-VE) which users may use in the enrolment process.

In the enrollment stage, users are trained to create strong passwords through an interactive password building interface.

The following responsibilities, which the Chromebook left to users, have been taken away from users by SL-VE:

- Creating stronger passwords

- Spoofing sites elimination

- Phishing aiming to acquire login credentials

SL-VE aids in protecting more than just the user’s social networking site accounts. For any authentic site, SL-VE will be able to avoid spoofing of such a site, as well as avoid login credentials of such a site to be lost through phishing.

With SecureLink (Chromebook and SL-VE), the following responsibilities were found to be left in the hands of users:

- Being able to identify and avoid phishing

- Being able to identify and avoid some social networking attacks

- Staying safe on mobile devices

By looking at the responsibilities left in the hands of home users, it is clear that SecureLink takes many security responsibilities away from home users which was the objective as stated in section 1.

10. Conclusion

By using Chromebook and the Virtual Extension i.e. SecureLink, most security responsibilities are moved away from the user.

In terms of this research, the following limitation was encountered:

1. Limited information with regards to extensive securities of ISPs as well as Chromebook. This is more than likely due to them hiding security details so as to avoid breach as well as for competitiveness.

For future research, ways in which to take on those responsibilities left in the hands of home users should be investigated and catered for as far as possible.

11. References

[1] AOL (n.d.). Choose the right plan for you!. [ONLINE] Available at: http://get.aol.com/plans/index.php?regtype=client&offergrp=webreg. [Last Accessed 16 June 2013].

[2] Comcast Expert (2013). Using Email Client Programs with Comcast Email. [ONLINE] Available at: http://customer.comcast.com/help-and-support/internet/email-client-programs-with-xfinity-email/ . [Last Accessed 4 June 2013].

[3] Culpan Tim & Debra Mao (2013). Acer Sees Success in Chrome; Windows Fails to Drive Sales. [ONLINE] Available at: http://www.bloomberg.com/news/2013-01-27/acer-sees-success-in-Chrome-pcs-as-Windows-fails-to-drive-sales.html. [Last Accessed 16 August 2013].

[4] Cyber Clean Centre (n.d.). What is Cyber Clean Centre?. [ONLINE] Available at: https://www.ccc.go.jp/en_ccc/index.html . [Last Accessed 13 June 2013].

[5] Evers Joris (2005). ISPs versus the zombies. [ONLINE] Available at: http://news.cnet.com/ISPs-versus-the-zombies/21007349_3-5793719.html. [Last Accessed 12 June 2013].

[6] f-secure (n.d.). security-as-a-service . [ONLINE] Available at: http://www.f-secure.com/en/web/business_global/security-asa-service . [Last Accessed 14 July 2013].

[7]Google (2013). Meet Chromebooks. [ONLINE] Available at: https://www.google.com/chromebook/. [Accessed: 26 September 2014]

[8] Hu Jim (2004). Comcast takes hard line against spam . [ONLINE] Available at: http://news.cnet.com/Comcast-takes-hardline-against-spam/2100-1038_3-5230615.html . [Last Accessed 15 June 2013].

[9] Jen Tracy (2000). Police Get Window Of Access To E-mail. [ONLINE] Available at: http://www.themoscowtimes.com/sitemap/free/2000/1/article/police-get-window-of-access-to-email/268089.html. [Accessed: 29 november 2013].

[10] Kritzinger, E., & Von Solms, S. H., (2011) Security for home web users: from a thick web user to a thin web user.

[11] Ledford, J.L. (2006) The Personal Cybersecurity Bible, Boston: Thomson Course Technology PTR.

[12] McAfee (n.d.). Security-as-a-Service. [ONLINE] Available at: http://www.mcafee.com/us/products/security-as-aservice/index.aspx . [Last Accessed 15 July 2013].

[13] McAfee (2013). McAfee Threats Report: Second Quarter 2013. [ONLINE] Available at: http://www.mcafee.com/mx/resources/reports/rp-quarterly-threat-q2-2013.pdf. [Accessed: 29 June 2014].

[14] Mick Jason (2013). Quick Note: Samsung Chromebook is Top Selling Notebook on Amazon. [ONLINE] Available at: http://www.dailytech.com/Quick+Note+Samsung+Chromebook+is+Top+Selling+Notebook+on+Amazon/article32003.htm. [Last Accessed 19 August 2013].

[15] Nieh Jason ;Yang S. Jae ;Novik Naomi (2000). A Comparison of Thin-Client Computing Architectures. [ONLINE] Available at:http://academiccommons.columbia.edu/catalog/ac%3A110384. [Accessed: 3 october 2013].

[16] Purcell TY (2002). User Security and The Internet Service Provider. [ONLINE] Available at: http://www.giac.org/paper/gsec/1950/user-security-internet-service-provider/103393 . [Last Accessed 10 June 2013].

[17] Rouse Margaret (2010). Security-as-a-Service. [ONLINE] Available at: http://searchsecurity.techtarget.com/definition/Security-as-a-Service. [Last Accessed 10 July 2013].

[18] Rowe B, Reeves D, Wood D & Braun F, (2011). The Role of Internet Service Provider in Cyber Security . [ONLINE] available at: http://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf [Last Accessed e.g. 31 August 11].

[19] Ryan Paul (2010). Google demonstrated Chrome OS during a press briefing today in San Francisco . [ONLINE]

[20] Available at: http://arstechnica.com/gadgets/2010/12/google-demos-Chrome-os-launches-pilot-program/ . [Last Accessed 16 august 2013].

[21] Secunia (n.d.). Free PC security for your home. [ONLINE] Available at: http://secunia.com/. [Last Accessed 15 June 2013].

[22] Sophos. (2013). Sophos Security Threat Report 2013. [ONLINE] Available at: https://www.sophos.com/enus/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf. [Accessed: 2 May 2014].

[23] Symantec (2013). Symantec Internet Security Threat Report. [ONLINE] Available at: http://www.symantec.com/security_response/publications/threatreport.jsp. [Accessed: 19 August 2014].

[24] Williams Mark I (2010). A Quick Start Guide to Cloud Computing: Moving Your Business into the Cloud. Great Britain: Kogan Page.

[25] Womack Brian (2013). Google Chromebook Under $300 Defies PC Market With Growth. [ONLINE] Available at: http://www.bloomberg.com/news/2013-07-10/google-Chromebook-under-300-defies-pc-market-with-growth.html. [Last Accessed 18 august 2013

Difficulties Encountered in South Africa with Sentiment Analysis using Twitter

Laurie Butgereit
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
laurie.butgereit(at)nmmu.ac.za

Abstract

Twitter provides a wealth of data which can be used by researchers. There has been research where Twitter data has been used to attempt to detect earthquakes, predict the stock market, predict the outcome of elections, monitor sporting events, and determine general public sentiment. In many cases, the results of these research projects can be compared against unbiased external parties. In some cases, especially in cases which involve human sentiment and emotion, it is much harder to judge the results of such research. The author has previously reported on three Twitter based projects. Those previous papers emphasized the algorithms and techniques involved. This current paper, however, differs from those previous papers and describe the numerous difficulties encountered when dealing with research based on data from Twitter.

Keywords

Twitter, Sentiment Analysis, Evaluation

1. Introduction

Twitter provides a wealth of data which can be used as the basis for research. A superficial search at scholar.google.com with the keyword Twitter provides links to research papers which have used Twitter data to attempt to detect earthquakes (Sakaki, Okazaki, & Matsuo, 2010), predict the stock market (Bollen, Mao, & Zeng, 2011), predict elections (Tumasjan, Sprenger, Sandner, & Welpe, 2010), monitor sports events (Zhao, Zhong, Wickramasuriya, & Vasudevan, 2011), and determine general sentiment (Pak & Paroubek, 2010).

In many cases, it is easy to determine if the research based on Twitter content generated positive results or negative results. If Twitter data is used to attempt to detect earthquakes, the results can be compared against data from a geological survey department or seismic department. If Twitter data is used to attempt to predict elections, the results can be compared against the outcome of the elections.

ISBN: 978-1-920508-67-8

But when Twitter data is used as the basis for research to determine sentiment or emotional states of human beings, it is more difficult to judge the results when compared to reality in an unbiased manner. There are a number of reasons for this including the quality of the training data, human emotional differences, and the reliability of the evaluation process.

The author has previously reported on three projects based on data provided by Twitter. The first project attempted to crowdsourced the weather report over one city in South Africa by monitoring Twitter (Butgereit, 2014a). The second project attempted to map Highveld thunderstorms as they moved across Gauteng by monitoring Twitter (Butgereit, 2014b). The third project attempted to rank the level of anger expressed against Eskom due to load-shedding by using Twitter (Butgereit, 2015).

These three previous projects used DSR (Design Science Research) to guide the research. DSR is an iterative methodology consisting of three interwoven cycles: a relevance cycle, a design cycle, and a rigor cycle (Hevner, 2007). These three interwoven cycles ensure that a DSR project creates an innovative artifact which is relevant. The artifact must be well designed and rigorously evaluated (Hevner & March, 2003; March & Smith, 1995; Vaishnavi & Kuechler, 2007). The GDC (General Design Cycle) of DSR consists of five steps (Oates, 2006): Awareness, Suggestion, Development, Evaluation, and Conclusion. These five steps are iterated numerous times until the artifact is satisfactory.

The information provided in this paper was gleaned during the Development and Evaulation steps of the GDC of the three previous projects. This paper augments the previous papers and explains in detail the difficulties which were encountered in attempting to obtain and/or generate unbiased training data, to cater for different people's different perceptions of emotions, to cater for South Africa's multi-lingual society and to evaluate the results in a way that was free from author bias.

This paper will first provide a short summary of the three original projects and then itemise specific difficulties and possible solutions related to mapping Twitter information, training data, people's different perceptions, multi-lingual society, specific South African political landscape, geolocation, and unbiased evaluations. In some cases, solutions are described and in other other cases, the problems can form the basis of future research.

2. Project #1 - Crowdsourced Weather Reports of Pretoria

The term crowdsourcing was coined by Jeff Howe in his 2006 article in Wired Magazine (Howe, 2006). He defined a situation where people use their “spare cycles to create content, solve problems, even do corporate R&D”. Crowdsourcing taps into the collective intelligence of the public to complete a task that would normally be done by one person or a specific agent (Alsever, 2007).

Twitter is an example of a crowdsourcing website where people freely contribute information to the general public about what they are experiencing, thinking, or feeling. These contributions are in the form of short tweets (Java, Song, Finin, & Tseng, 2007; Kwak, Lee, Park, & Moon, 2010).

Twitter provides an open API (Application Programming Interface) to allow people to search for and extract specific tweets. This search and extraction can be done by a combination of keywords and geo-location (longitude and latitude).

The tweets extracted for Project #1 included official tweets from various weather organisations and news organisations. These tweets were kept at the ground truth of the situation. The term ground truth means different things to different people. However, Sikdar, Kang, and Adah specifically speak of ground truth with respect to Twitter credibility (Sikdar, Kang, O'Donovan, Hollerer, & Adal, 2013).

The research concluded that exceptional weather conditions where the weather changes abruptly such as thunderstorms could be easily determined by monitoring Twitter. But ongoing conditions such as ongoing cold weather or ongoing hot weather over a period of days were more difficult to determine. The full research can be found (Butgereit, 2014a).

3. Project #2 – Tracking Highveld Thunderstorms

The project previously described in Section 2 found that dramatically changing weather was much easier to determine using Twitter than ongoing unchanging weather. This led to a second research project of attempting to map or track Highveld thunderstorms as they travelled across Gauteng.

Very few natural disasters occur in the South African inland province of Gauteng. There are few earthquakes and no tsunamis. Heat induced thunderstorms, however, are a common occurrence in the summer months and are often dramatic with gusting wind, frequent lightning and thunder, and hail (Archer et al., 2010; Carte & Held, 1978; Kruger, Goliger, Retief, & Sekele, 2010). When weather conditions dramatically change, people flocked to Twitter to comment. In the case of Highveld thunderstorms, the tweets included vibrant descriptions of hail, lightning, property damage, flood waters, and warnings to other people.

In order to evaluate this project, lightning stroke maps from the South African Weather Service were obtained. An exercise of content analysis as described by Krippendorf (1980) was undertaken where two independent coders would compare maps generated by the South African Weather Service with maps generated by the Twitter analysis software. These two coders, working independently, ensured that the results were reproducible and free from author bias. The full research can be found at (Butgereit, 2014b).

4. Project #3 - Anger about Load Shedding

Eskom is the primary supplier of electricity in South Africa and generates approximately 95% of the South Africa's electricity (Eskom). In recent years, however, Eskom has not be able to consistently satisfy the public's demand for electricity. On November 1, 2014, Eskom reported that a coal silo collapsed at its newest power station. According to Eskom, the damage to the coal silo caused a drop in electricity production at that power station from 3,600 MW (Megawatts) to 600 MW (Zwane, 2014). The drop in electricity production at the power station forced Eskom to implement load-shedding as it struggled to find the required capacity. This load-shedding started immediately in November and continued into the Christmas holidays. As South Africa went back to work in January after the festive season, the threat of load-shedding continued. At the time of writing this paper (mid-July), the load-shedding is continuing.

People flocked to social media to complain about the load-shedding and Eskom in general. The author's previous research (Butgereit, 2015) reported on an algorithm which could be used to quantify the amount of anger expressed in a post on Twitter (called a tweet). That algorithm generated a number between the value of 0 (no anger) to 10 (extreme anger). The algorithm could then be used to compare the relative anger in two tweets and rank one tweet as containing more anger than another tweet.

Just over 70,000 tweets were extracted during the period Nov 23, 2014 to Dec 31, 2014. Of those 70,000 tweets, only eleven calculated to a value more than ten and their scores were manually reduced to ten.

The evaluation of this project, however, was problematic because there was no unbiased standard of anger which could be used for comparison.

5. Brief Comparison of Projects #1, #2 and #3

It is important to note that both Project #1 (crowdsourced weather reports) and Project #2 (mapping Highveld thunderstorms), there were independent unbiased standards against which the project results could be compared. In the case of Project #1, the tweets from official weather organisations and news organisations were considered to be the ground truth for the evaluation project. In the case of Project #2, lightning stroke maps from the South African Weather Service were used as the basis of evaluation.

Project #3 (measuring anger), however, was different. Project #3 attempted to quantify anger and, as such, there was no ground truth or unbiased measurement of anger against which the project could be evaluated. The remaining portion of this paper deals primiarly with the difficulties with sentiment analysis using Twitter data.

6. Training Data Difficulties

Typical research in sentiment analysis or opinion mining usually starts with creating or obtaining a training corpus. This training corpus is a collection of sample tweets (or messages or documents depending on the research) which have been already tagged or identified as representing certain emotions, sentiments, or opinions.

This section of the paper describes three difficulties encountered when attempting to locate and/or create training data for Twitter based sentiment analysis.

In the case of attempting to mine opinions or sentiment on Twitter, there are, in fact, a number of freely downloadable corpora of tagged tweets available such as (ThinkNook, 2012). The difficulty which was encountered, however, was that none of these corpora contained sample tweets about load-shedding or electricity supply. They were corpora on general tweets and would not be appropriate as training data for a project to specifically handle tweets about load-shedding. For example, the corpora (ThinkNook, 2012) had sample tweets such as:

> Happy Blue Year to you too, Gary All the success in 2009!

> Her music makes me sad. I always think of those commercials with all the abandoned pets.

These sample tweets would be of no benefit in a project specifically looking at anger about load-shedding.

The next possible solution is to create such a corpora. As mentioned previously, the research reported in (Butgereit, 2015) collected approximately 70,000 tweets over a six week period and it was possible to extract a random subset of 1,000 tweets which could be used as a basis for training data. The difficulty, however, was how to tag or label these tweets in a way which was free from author bias. In view of the fact that the research was about anger expressed via Twitter and in view of the fact that anger is a very human emotion, in order to create this training corpora, people (real human beings) needed to label or tag these tweets.

The previous research described the creation of a mechanical turk to easily allow members of the public to tag or label this training set. The term Mechanical Turk originally referred to a hoax automaton which was created by Wolfgang van Kempelen near the end of the eighteenth century which played chess with members of the public (Standage, 2002). In more recent years, the term refers to Amazon's crowdsourcing facility where the general public can post small jobs which need to be done and people can respond by doing these jobs for small amounts of money (Amazon). The common noun mechanical turk refers to any such facility.

The mechanical turk created for (Butgereit, 2015) was a web application specifically formatted for small cell phone screens. By developing the mechanical turk for mobile devices, it was hoped that university students could assist in tagging tweets during small amounts of free time while on campus between classes. The web application also made it easy for the coders or people labeling the training data to start and stop. In other words, it was possible for the coders to label ten to twenty tweets, and then stop, and continue later in the day.

The author acted as one of two coders labeling the tweets reported in (Butgereit, 2015). From personal experience, the exercise is not particularly pleasant. It is boring and tedious. In addition, in view of the fact that these particular tweets were about anger, it was difficult to remain unemotional and calm while tagging hundreds of tweets about anger. For that reason, the second coder needed to be offered certain amount of money in order to create a second set of labels for the training data.

The next difficulty which was encountered was the difference in opinions between the two coders as to the amount of anger expressed in the tweets. In the research reported in (Butgereit, 2015), the two coders only agreed on the labels for 58% of the tweets.

This difficulty of creating or obtaining unbiased training data is exacerbated by the fact that various corpora of training data available on the Internet (such as (ThinkNook, 2012)) do not provide information on how the labels were actually obtained. Were the labels merely the opinion of one researcher or do the labels have some sort of statistical strength?

This section of the paper itemised three difficulties which arise when attempting to create or obtain training data for Twitter based research. These three difficulties are 1) lack of good existing training corpora 2) logistics of crowdsourcing labels for new training data 3) statistical concerns about the labels which are put on existing training corpora which can be sourced on the Internet.

7. Perception Difficulties

People perceive things differently. People hold different opinions. People use sarcasm differently. People have different personal histories. Some people routinely use swear words while other people reserve swear words for only dramatic situations. For example, to a person who was unaware of the Eskom load-shedding crisis, the following tweets may be considered to be positive tweets:

> Eating salad by candlelight. Thanks for the romantic evening, Eskom.

> Lots of people having braais tonight. Must have all expected an eskom moment.

But to a South African who has suffered through load-shedding, the tweets can be considered to be sarcastic and should be labeled as negative. (For readers who are not from South Africa, the word braai was originally an Afrikaans word indicating cooking over an open fire but has migrated to English and indicates a happy social occasion of cooking over the fire with friends in a relaxed setting.)

People's political beliefs also influence their perception of tweets. Consider the following:

> Blame apartheid for Eskom's struggles - President Zuma

For a person who supports South African President Zuma and the ANC (African National Congress) political party, this is a positive tweet which validly explains the load-shedding crisis. For a person who does not support South African President Zuma, this is a sarcastic negative tweet.

This problem of perception differences happens at numerous points in research using Twitter. In the research reported in (Butgereit, 2015), this occurred both when two coders were attempting to create unbiased training data and it also occurred when four coders were creating tagged data against which the algorithm could be tested and evaluated.

8. Language Difficulties

South Africa is a multi-lingual society with eleven official languages (Mesthrie, 2002) and numerous unofficial languages. Many common words migrate among the languages. As mentioned in Section 7, the Afrikaans word braai is widely used by non-Afrikaans speakers in South Africa to indicate a social meal cooked over an open fire with friends. The Zulu word yebo can be heard in English conversation with the meaning of an enthusiastic yes!

Words of exasperation have also migrated from language to language. The word eish (pronounced eeesh) has migrated into English and denotes an amount of exasperation, desperation or lack of understanding. An interesting Twitter hashtag which appeared in many tweets was #Eishkom which was a play on sounds between the words Eskom and eish. For example:

> eish wont be having dat meal dat i have been craving for ,for the whole day thanks to eskom #blackout

> #eishkom NOOOooooo!!!! :(this ain't right

The Zulu word wena means you but often appears in English tweets for extra emphasis in the form of you guys. For example:

> @Eskom_MediaDesk viva! Eish. Dark Africa wena!

> yohhhh wena don't even say. There I was cooking my sunday lunch #Eskom does a #powercut stunt. My chicken was half way cooking

Swear words also migrate. In addition, people who are not home-language English speakers often revert to their home language when they wish to swear. For example:

> But no lights on? Thanks for fokkol #Eskom!

> Bluh bluh "eskom life, power circle" bluh bluh, fokof we busy getting load shedding...

Sounds from languages also migrate. The Twitter hashtag #eksdom appeared often. It plays on the Afrikaans sentence “Ek is dom” (I am stupid) which sounds similar to Eskom. For example:

> Home, walk in door, stand on cat. #eksdom #eishkom #loadshitting #eskom

And some tweets represent the multi-lingual nature of South Africa:

> Fok wena maan. @Eskom

The sample tweets in this section exemplify some of the difficulties when attempting to determine sentiment or emotion in tweets in South Africa's multi-lingual society. It is not possible to use labeled tweets from other English speaking countries and it is not possible to use a dictionary of words (such as was mentioned previously in Section 4 Rule 1 above) because the dictionary would not contain the nonEnglish words which have migrated into South African English.

9. South African Society

A number of tweets deal specifically with South African society, news or folklore. These tweets express anger by comparing Eskom to other South African institutions or news makers which also illicit anger in the public.

For example:

> #SA does not only have a power crisis it as a #Justice crisis to. Both are failed institutions. #Eskom #LoadShedding #Dewani #oscarpistorius

compares Eskom with Shrien Dewani and Oscar Pistorius. Both Shrien Dewani (BBC, 2014) and Oscar Pistorius (McGroarty, 2014) were on trial for murdering their wife and girl friend respectively. Both trials were high profile and both trials had unexpected results in the eyes of many South African resulting in outrage in social media.

The price of petrol (gasoline) is controlled in South Africa. South Africans consider the price of petrol to be high and increases often illicit anger in the public. Tweets such as:

> If oil companies in RSA was managed like eskom, pumps at the petrol stations would run dry every time they did maintenance

express anger by comparison.

In fact, a handful of unrelated terms such as Nkandla, eTolls, Guptas, and Zimbabwe all indicate a certain degree of anger.

> #Eskom do you sometimes visit nkandla
>
> I'll only sympathize with Eskom's load shedding when it switches the etoll gantries off
>
> The guptas and eskom are using our hard eaned money to sponsor TV programs
>
> The Zimbabweans are making Eskom jokes

For readers who are not based in South Africa, these terms all relate to political issues, events, or situations with which the public is quite vocal.

10. Geo-Location Difficulties

Twitter provides a number of pieces of geolocation data with the returned tweets. These include the longitude and latitude of the person when he or she posted the tweet and the general location of the person.

The original research reported in (Butgereit, 2015) attempted to map rolling blackouts or load-shedding. However, the geolocation data returned by Twitter was not sufficient to do so. Of the 70,000 tweets which were extracted during the course of the study, only a few hundred had accurate longitudes and latitudes. Although more people (tens of thousands) did have a profile location indicated, that profile location was often very general and/or inaccurate.

The next step was to search the body of the tweet for additional information about location. Tweets occasionally contain the suburb or area name. For example:

> @ZA_Trance_Gamer @Eskom_SA @CityPowerJhb @sandtontimes Power is also still off in Rivonia ... Has been off since 10am!!!!!!

But this was not the norm and not sufficient to actually generate a map.

This contrasts with research about tracking weather activities such as Highveld thunderstorms using Twitter (Butgereit, 2014b). Research has shown that it is quite easy to track summer thunderstorms between Soweto and Pretoria using Twitter.

This is due to the fact that people naturally talk about the weather. It is safe topic of conversation which does not involve personal details or sensitive topics (Harley, 2003). It is common in society for people to talk about past weather, current weather and future weather (Strauss & Orlove, 2003). It is common for complete strangers to converse about the weather. In such conversations between complete strangers, the people exchange geographical information such as “We had 5 cms of rain in Sandton” or “It hailed in Randburg”. Because of this natural tendency, it is easy to extra geolocation from such tweets.

Such is not the case with attempting to track anger or general sentiment.

11. Evaluation Difficulties

It is important that the output of research is evaluated in a way that is free from researcher personal bias. Content Analysis as defined by Krippendorf (Krippendorff, 1980) is a research technique “for making replicable and valid inferences from text.” Krippendorf describes three different levels of reliability with respect to results: stability, reproducibility, and accuracy.

Krippendorf describes stability as the weakest form of reliability. Research results could be considered to be stable if one person evaluates the data, waits a certain period of time, and the re-evaluates the same data again. If the results obtained between the two evaluations are the same, the results can be considered to be stable (Krippendorff, 1980, p. 130). According to Krippendorf, results can be considered to be reproducible if two or more independent people evaluate the data and obtain similar results (Krippendorff, 1980, p. 131). Results can be considered to be accurate if they are compared against some known standard (Krippendorff, 1980p. 131).

Many research projects which use Twitter data as a base can compare results against known standards. For example, the research by Sakaki et al searched Twitter to find earthquakes (Sakaki et al., 2010). Such results could be compared against a known standard such as seismographic data. Research by Bollen et al searched twitter in an attempt to predict the stock market (Bollen et al., 2011). Such results could be compared against a known standard of the stock market values themselves. Such projects could be considered to be accurate or not accurate depending on the results.

Evaluating research projects which attempt to determine emotion or sentiment based on Twitter data, however, do not have a known standard against which the results can be compared. Even if the results could not be considered to be accurate, it is important that the results be at least reproducible. In order for that, two ore more people need to evaluate the data and have similar results.

In the original research reported in (Butgereit, 2015) this was done by creating another mechanical turk similar to the first mechanical turk used to attempt to create training data. In that original research, two people working independently evaluated another one thousand tweets comparing them against the results of the artifact which was the basis of that research. It is important to note that the two people only agreed between themselves in 69% of the tweets. Eventually four people working independently were used to evaluate the data. Because human emotions vary so much between people, it is often difficult to even generate reproducible results.

12. Conclusion

There is an abundance of data on Twitter which is available to researchers free of charge. There have been numerous research projects which extract data from Twitter and analyse the data to determine the weather (Cox & Plale, 2011), to predict the outcome of elections (Tumasjan et al., 2010), to flag events during soccer matches (Van Oorschot, Van Erp, & Dijkshoorn, 2012), and to monitor rising flood levels (Vieweg, Hughes, Starbird, & Palen, 2010). In many cases, the results of such research projects can be compared against data from some unbiased external organisation such as the actual weather bureau reports, the outcomes of the elections, or even the outcomes of soccer matches.

But when research projects attempt to determine sentiment or emotion by monitoring Twitter, it is much more difficult to evaluate those results in an unbiased manner. This is due to a number of reasons included lack of training data, differences of human perceptions, language differences, social differences, and difficulties in generating reproducible results.

13. References

Alsever, J. (2007). What is crowdsourcing? BNET.Com, March, 7

Amazon. Amazon mechanical turk website.

Archer, E., Engelbrecht, F., Landman, W., Le Roux, A., Van Huyssteen, E., Fatti, C., et al. (2010). South African risk and vulnerability atlas Department of Science and Technology.

BBC. (2014, Dec 8, 2014). Shrien Dewani murder case thrown out by South African judge. BBC News,

Bollen, J., Mao, H., & Zeng, X. (2011). Twitter mood predicts the stock market. Journal of Computational Science, 2(1), 1-8.

Butgereit, L. (2014a). Crowdsourced weather reports: an implementation of the µ model for spotting weather information in twitter. IST-Africa 2014 Conference Proceedings,

Butgereit, L. (2014b). Tracking Gauteng thunderstorms using crowdsourced Twitter data between Soweto and Pretoria. TD: Journal for Transdisciplinary Research in Southern Africa, 10(3), 293-309.

Butgereit, L. (2015). An algorithm for measuring relative anger at Eskom during load-shedding using Twitter. Proceedings of the 12th IEEE Africon 2015, Sept 14-17, 2015, Addis Ababa, Ethiopia. pp. 878-882.

Carte, A., & Held, G. (1978). Variability of hailstorms on the South African plateau. Journal of Applied Meteorology, 17, 365-373.

Cox, J., & Plale, B. (2011). Improving automatic weather observations with the public Twitter stream. IU School of Informatics and Computing,

Eskom. Eskom corporate website, company information.

Harley, T. A. (2003). Nice weather for the time of year: The British obsession with the weather. In S. Stauss, & B. Orlove (Eds.), Weather, climate, culture (pp. 103-120). Oxford: Berg Publiishers.

Hevner, A. R. (2007). The three cycle view of Design Science Research. Scandinavian Journal of Information Systems, 19(2), 87-92.

Hevner, A. R., & March, S. T. (2003). The information systems research cycle. Computer, 36(11), 111-113.

Howe, J. (2006). The rise of crowdsourcing. Wired Magazine, 14(6), 1-4.

Java, A., Song, X., Finin, T., & Tseng, B. (2007). Why we Twitter: Understanding microblogging usage and communities. Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 Workshop on Web Mining and Social Network Analysis, August 12-15, 2007, San Jose, California, , 56-65.

Krippendorff, K. (1980). Content analysis: An introduction to its methodology Sage Publications, Inc.

Kruger, A., Goliger, A., Retief, J., & Sekele, S. (2010). Strong wind climatic zones in South Africa.

Kwak, H., Lee, C., Park, H., & Moon, S. (2010). What is Twitter, a social network or a news media? Proceedings of the 19th International Conference on World Wide we, April 26-30, 2010, Raleigh, North Carolina, USA, , 591-600.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. Decision Support Systems, 15(4), 251-266.

McGroarty, P. (2014, Sept 12, 2014). Oscar Pistorius convicted of culpable homicide. Wall Street Journal,

Mesthrie, R. (2002). South Africa: A sociolinguistic overview. In R. Mestrhie (Ed.), Language in south africa () Cambridge University Press.

Oates, B. J. (2006). Researching information systems and computing Sage Publications Ltd.

Pak, A., & Paroubek, P. (2010). Twitter as a corpus for sentiment analysis and opinion mining. Paper presented at the Lrec,

Sakaki, T., Okazaki, M., & Matsuo, Y. (2010). Earthquake shakes Twitter users: Real-time event detection by social sensors. Paper presented at the Proceedings of the 19th International Conference on World Wide Web, pp. 851-860.

Sikdar, S. K., Kang, B., O'Donovan, J., Hollerer, T., & Adal, S. (2013). Cutting through the noise: Defining ground truth in information credibility on Twitter. Human, 2(3), pp. 151-167.

Standage, T. (2002). The Mechanical Turk. Nova Iorque: Penguin Books,

Strauss, S., & Orlove, B. (2003). Up in the air: The anthropology of weather and climate. Weather, Climate, Culture.Berg, Oxford, , 3-16.

ThinkNook. (2012). ThinkNook WordPress blog. Retrieved Jan 31, 2015, 2015, from http://thinknook.com/twitter-sentiment-analysis-training-corpus-dataset-2012-09-22/

Tumasjan, A., Sprenger, T. O., Sandner, P. G., & Welpe, I. M. (2010). Predicting elections with Twitter: What 140 characters reveal about political sentiment. Icwsm, 10, 178-185.

Vaishnavi, V., & Kuechler, W. (2007). Design Science Research methods and patterns: Innovating information and communication technology CRC Press.

Van Oorschot, G., Van Erp, M., & Dijkshoorn, C. (2012). Automatic extraction of soccer game events from Twitter. Paper presented at the Proc. of the Workshop on Detection, Representation, and Exploitation of Events in the Semantic Web, 17. pp. 15.

Vieweg, S., Hughes, A. L., Starbird, K., & Palen, L. (2010). Microblogging during two natural hazards events: What Twitter may contribute to situational awareness. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1079-1088.

Zhao, S., Zhong, L., Wickramasuriya, J., & Vasudevan, V. (2011). Human as real-time sensors of social and physical events: A case study of Twitter and sports games. ArXiv Preprint arXiv:1106.4300,

Zwane, T. (2014, Nov 3, 2014). Eskom: Majuba coal silo collapse has "significant consequences". Mail & Guardian

Measuring cyber security awareness among cell phone users in South Africa

T B Shabe[1], E Kritzinger[2], M Loock[3]

School of Computing, University of South Arica, Pretoria , South Arica
shabetb@hotmail.^{com1},Kritze@unisa.ac.za[2],loock@unisa.ac.za[3]

Abstract

The cell phones currently on the market present users with an array of excellent functionality. Some of the functionalities include online shopping, cell phone banking, taking pictures and recording videos, reading, downloading applications (or "apps") and participating in social networks. Other functionalities include sending and receiving email, allowing internet connection, and GPS navigation. However, this level of functionality means that huge amounts of personal and business information is often stored on cell phones, making them attractive targets for cyber attacks. Users can often be victims of such cyber attacks if they lack cyber security knowledge. One-hundred-and-forty questionnaires were distributed among residents of Rocklands, Bloemfontein, South Africa in order to determine their level of cyber security awareness. Upon analysis, the results indicated that most respondents were either slightly or not aware at all of cyber security threats against their cell phones. Practicable solutions to improve users' awareness levels are presented.

Keywords

Cell phones, social networking, cyber-attacks, cyber security, cyber criminals, security breaches, Security awareness, malware, WI-FI, Bluetooth, Education.

1. Introduction

Through their ability to connect to the internet, cell-phones enable users to download mobile applications and games, send and receive email, surf websites, participate on social networks and send and receive text messages (Oulasvirta, Rattenbury, Ma & Raita, 2012). In addition to these capabilities, many users use cell phones to share files via Bluetooth. Likewise, the presence of in-built GPS functionality and Wi-Fi makes it easy for cell phone users to use road maps and access the internet freely. Cell phones are useful for both business and personal purposes because of these capabilities. These capabilities very conveniently allow users to store very sensitive information such as their physical addresses, email addresses, important dates like anniversaries, their list of contacts, as well as photographs on the devices. However, having such sensitive information stored on the device, coupled with a generally careless attitude towards cell phone security, has made cell phones attractive targets for ambushers (Furnell, 2009).

McAfee (2012) indicated that there are various attacks ambushers can carry out against cell phone devices. These cyber security attacks pose serious threats to mobile security and have unbearable consequences (Van Grembergen, 2004). Users who are affected often become victims of identity theft, and ultimately also lose money, as their private data had been exposed to 3rd party unauthorized users. There is a need to address the challenge of mobile phone security breaches. Madell and Muncer (2004, p. 360) indicate that sensitizing people to the dangers and threats associated with the use of a mobile phone is the only way in which the challenge can be addressed. In order to address this challenge, a strategy is needed to raise the awareness of cell phone users. (Shipley & Bowker, 2014). This study was conducted to measure the extent to which cell phone users are aware of cyber security threats and risks associated with cell phone use. The results of this study could assist in the future promotion of cyber security awareness. The study will also investigate other related works that focus on finding solutions to cyber security threats. Related work is discussed next.

2. Literature Review

This section presents a succinct review of literature to determine how other researchers have previously dealt with the issue of cyber security awareness. Andy Favell, supervisor of the site Mobithinking, indicated that, in 2010, 96% of cell phones and tablets did not have any security programming (Favell, 2011). This shows the enormity of the challenge, as large numbers of mobile service users who should be taking responsibility for their cyber safety are not doing so. According to comScore M: Metrics (2008), some studies focusing on mobile phone security issues and services have raised the issue of modern cell phone increased vulnerability to security risks. Crawford (2013, p. 20) indicates that there are attempts to reduce data security threats through search engines that mobile phone users use to acquire information from the internet. However, these channels are usually also used by cyber criminals. Androulidakis (2011) also indicated that the security of mobile phones has been proven not to be adequate. Ivan & Wang (2009) are of the view that it has become all but impossible to put in place measures which can ensure that cyber threats are fully controlled or prevented. The only remaining option is to inculcate a culture of security awareness in respect of cell phone use. This means that users know the risks facing them, and can, therefore, protect themselves from harmful effects of such threats (Shi & Silvius, 2010). This study aims to determine the extent to which people are aware of cyber threats, the measures that can be taken to raise their awareness thereof, and to determine how these measures can be used to educate other mobile device users (Peterson, 2008). The remainder of this paper is organized as follows. Next is Section 3 which examines the methodology used for the survey. Research Findings are presented in Section 4, and lastly, Section 5 offers a conclusion and suggested future research paths.

3. Methodology

a. Demographics

The sample consisted of 139 respondents classified in the following manner:

- Gender: Male (45%); female (55%)

- Schooling level: No schooling (<1%); up to Grade 7 (<1%); up to Grade 12 (40%); post-matric qualification (58%)

- Age in years:18 to 25 (65%); 26 to 30 (22%); 31 to 35 (7%); 36 to 40 (4%); 41 to 46+ (2%)

- Employment: Student (57%); Part-time (4%); Full-time (29%); Unemployed with income (1%); Unemployed with no income (7%); Other (2%)

- Income per annum: R0 to R12 000 (70%); R12001 to R24 000 (10%); R24 001 to R36 000 (3%); R36 001 to R48 000 (4%); R48 001 to R60 000 (1%); R60 001 to R120 000 (1%); R120 001 to R350 000 (7%); R350 000+ (3%)

b. Data collection

The Structured questionnaires were given to a sample of cell phone users in this study. The convenience sampling technique was used. This is a type of non-probability sampling technique in the sampling units are selected using as criteria the place and time of the data collection process (Dillon, Madden, & Firtle, 1993). This is thus an unrestricted form of sampling (Cooper & Emory, 1995). The convenience sampling method helps in testing and gaining ideas about the subject of interest (Cooper & Emory, 1995) which, in this case, is knowledge cell phone users have about cyber security threats. The respondents were selected on the basis of convenience which, in this case, meant individuals who were available and who were willing to spare some of their time to participate in the survey. This method of selection meant that all participants gave their consent by implication. The anonymity of the respondents was ensured to so as to avoid any ethical dilemmas and also to ensure candid responses, so as to have a better and clearer understanding of the issue at hand. The survey was conducted and limited to Rocklands, Motheo district, Mangaung, and Bloemfontein in South Africa. The target group of the survey was residents of Rocklands from ages 18-25, 26-35, 35, 36-40, 41-46, 46 and above. The self-test questionnaire contained some questions which had to be answered by choosing between the options “not sure”, “yes” and “no”. Other questions had to be answered on a 5-point Likert scale, with the responses weighted as follows: 1 = disagree strongly; 2 = disagree; 3 = undecided; 4 = agree; 5 = agree strongly.

4. Results

In the following section, the survey results are explained with the help of tables for each question. This enables a detailed analysis of the responses of the respondent and the inferences made from those responses. This section shows the responses to the questions on the questionnaire which allowed the researcher to make inferences regarding the usage profile of the cell phone users, and their level of cyber security awareness in respect of emails, social networks, banking, internet surfing, and file sharing. It also shows their willingness to be educated on the issue.

4.1 Usage profile of respondents

The first question inquired about respondents’ daily usage. This is determined by classifying the various types of cell phone use, and it prevalence for each respondent. The results gained indicates that, 79 % of the respondents carry out transactions several times a day using their bank account which must be due to their business/personal needs. 94% respondents reported that they spend 3 or more hours on a regular basis depending on their day to day needs as they emerge. 74% use their cell phone to surf internet while 89% of respondents buy online. 65 % of respondents take pictures with their cell phone. There are also 74% of respondents, who partake in social networking through their cell phone. So, overall majority of respondents spend a lot of time online on a regular basis, which means that the majority of users could be exposed to cyber security threats (Printips, 2011).

4.2 Extent of cyber security awareness related to malware and email phishing attacks.

The second set of questions was designed to determine respondents’ knowledge of spam and phishing emails (table 2).

Table 2: Rating cyber security awareness of users who access emails through cell phone

Questions	**Answer options**		
	Yes	**No**	**Not sure**
Does your mail have a spam filter?	24%	66%	10%
Do you open email if you don't know who the sender is?	52%	48%	0%
Do you open email attachments if you don't know the sender?	67%	23%	10%
Do you use web based email services such as yahoo, hotmail or gmail?	52%	48%	0%

Out of the total responses gathered for this question, only 24% agreed that their emails had a spam filter while 66% did not have, Thus, the majority of the respondents do not know about the security problems that can be caused by fraudulent cyber activities. Such cell phone users still lack complete knowledge of these threats which can affect them and cause the dissemination of their personal information.

4.3 Extent of cyber security awareness related to malware and phishing attacks through social networks.

Phishing scams can also be delivered through texts and social networking sites. Another set of questions (Table 3) were designed to determine whether respondents' practices when participating on social networks could cause them to be victims of cyber threats.

Table 3. Security risk awareness related to using cell phones for social networking

Questions	**Answer options**		
	Yes	**No**	**Not sure**
Do you supply sensitive information about yourself when registering with social networks?	100%	0%	0%
Do you accept friend requests from people you don't know?	84%	16%	0%
When logging in social networks do you run remember me checkbox?	70%	28%	2%
Do you know that friends' weaker passwords on social networks makes you vulnerable as well?	21%	79%	0%

Are you concerned about your social network accounts being hacked?	96%	4%	0%
Are you aware that even people you know can be identity thieves?	22%	78%	0%

As Table 3 above indicates, respondents are concerned about their security on the internet and social networks. They do not feel at risk online and have the impression they will not ever become a victim of cyber crime, suggesting that there is a lack of cyber security awareness around the threat presented by social networking. This shows that, overall, respondents had no or very little knowledge of the possible threats which could lead to their personal information being leaked to cyber criminals.

4.4 Extend of cyber security awareness related to mobile or cell phone banking

In this question, respondents were asked about whether or not they are aware of the cyber security issues that could arise while carrying out cell phone banking. Out of the total responses gathered for this question, only 21% of the respondents knew about the cyber security threats. In fact, the majority, at 54%, had no awareness of security risks. 25% of the respondents affirmed that they were aware of the cyber security issues, but only to some extent, but still lacked the complete knowledge about how these threats could affect their actual transaction amounts and their personal information being leaked.

4.5 Extent of cyber security awareness related to surfing the internet and downloads

This question was designed to identify whether respondents realized that using a mobile internet connection to surf the internet and downloading free apps and games exposed them to a higher risk of cyber insecurity. Only 21% of the respondents noted that they pay attention to cell phone security while surfing the internet and when downloading from the internet. twenty six per cent of the respondents indicated that they do not read the terms and conditions to make sure that they are aware of all the measures they should take, the services that will be provided, and the extent to which their private information can be used by third parties. The rest of the respondents (53%) had no idea. This depicts that respondents are not much concerned about their online security. This might be because of a lack of time or just because of carelessness. But for whatever reason, the respondents' lack of concern for cyber security when using a cell phone is evident from this behaviour .

4.6 Extent of cyber security awareness related to cell phone security breaches.

The next question (the responses to it are tabulated in Table 4) relating to security breaches was designed to gather information about the various suspicious activities in which respondents might get involved intentionally or unintentionally, which could lead to the loss of their secure private information. In this question, respondents were given the choice of selecting more than one option to account for all the possible threats encountered by them which may have lead to threats to information security. Of the respondents, 33% said that they that they did provide their personal information when asked for it. This is a plausible threat to the security measures taken to safeguard that information. Thirty-four per cent of respondents indicated that their identity had been stolen online, 13% indicated that they had fallen victim to financial scams and 10% of respondents knew somebody who had been a victim of phishing. These results depict the carelessness of respondents in securing their personal information.

4.7 Extent of cyber security awareness related to file sharing applications, corporate networks, Wi-Fi and public hotspots..

The next question was designed to identify whether respondents know that using free Wi-Fi connections, hotspots, file sharing through applications like BBM, WhatsApp and via Bluetooth is risky and can lead to identity theft if they don't implement mobile security measures. (Table 4).

Table 4. Rating users attitude towards cell phone security in general and sharing files with peers

Questions	**Answer options**		
	Yes	**No**	**Not sure**
Do you use peer-to-peer file sharing applications like Mixit, BBM, WhatsApp, emule, napster, kazana, Bluetooth?	85%	15%	0%
Do you pay attention to mobile security like setting pin lock and unlock etc when connecting to the internet with a cell phone, using Wi-Fi hotspots or corporate networks?	21%	55%	24%

From the data gathered from table 4, This shows that respondents are not very concerned about their security online. They tend to be less security conscious than they might otherwise be. As a result, they continue to be susceptible to scamming or phishing.

4.8 Rating cell phone users’ attitude towards related cyber security training as protection.

The last question of the survey questionnaire prompted respondents to express an opinion about programmes to educate cell phone users and creating awareness about cyber security concerns, threats and solutions.(Table 5).

Table 5. Attitude cyber security training as protection method

	Disagree strongly	Disagree	Undecided	Agree	Agree strongly
Would you like to receive training in cyber security?	5%	20%	0%	11%	64%
Would you like a booklet about cyber security awareness to be included in all new cell phone purchases?	0%	5%	16%	19%	60%

These results indicate that there is definitely a need to provide cell phone users with more information about threats to their cyber security information, and educate them about the measures they can take to mitigate such risks so as to prevent losses of private and personal information.

5. Discussion on findings

It was found out that making calls was the activity that most of the respondents used their phones for. The other activities in decreasing order of importance included sending and receiving SMSes, surfing the internet, online banking, online purchasing, social networking, and taking pictures. However, it was found out that most respondents did not take appropriate measures to prevent malware installation and phishing attacks through emails. More than 66% of respondents had no spam filters, more than 67% opened email attachments from senders they did not know, and close to 50% used other non-web-based email addresses. Other problems that were detected included the fact that 100% of the respondents supplied sensitive information about them when registering with social networks, 84% accepted friend requests from unknown people and 69% acknowledged running the “remember me” checkbox when logging on to social networks. Surprisingly, 88% of the respondents were not aware that the people with whom they communicated, but did not actually know, could be identity thieves. The findings showed that very few people paid attention to cell phone security while surfing the internet. Only 21% of the people knew that cyber security threats existed and were taking measures to prevent such threats from affecting them. Despite the fact that most of the respondents agreed strongly that there needed to be some form of cyber training programs as measures of protection, most respondents had never been victims of cell phone breaches. Perhaps that is the reason most of them are not keen on taking up measures to prevent such breaches. The need to be vigilant is thus ignored, in effect allowing criminal behavior to. There is, therefore, need for mass education on the need for vigilance while using cell phone services to create further awareness of security breaches.

6. Bibliography

Androulidakis, I. (2011). Intercepting mobile phone calls and short messages using a GSM tester.In: Proceedings of CN2011, Springer Verlag CCIS 160, 281–288

Crawford, D. (2013). Emerging Cyber Threats in the New Year. Communications of the ACM, 56(1), 20.

ComScore M: Metrics. (2008). Smarter phones bring security risks: study. http://www.comscore.com [Accessed 26 December 2011].

Cooper, D.R. & Emory, C.W. (1995). Business research methods, (5th Edition). Chicago: Irwin.

Dillon, W. R., Madden, T. J. & Firtle, N. H. (1993). Essentials of Marketing Research. Illinois: Irwin.

Falaki, H., Mahajan R., Kandula, S., Lymberopoulos, D., Govindan, R. & Estrin, D. (2010). Diversity in Smartphone usage. Mobisystems (10th June 2010).San Francisco

Fleischmann, A. (1995). Personal Data Security: Divergent Standards in The European Union and the United States. Fordham International Law Journal. 19, 143-180.

Furnell, S. (2009). Mobile Security. (1st ed.) Ely: IT Governance Pub.

Ivan P. L. Png, & Qiu-Hong Wang. (2009). Information Security: Facilitating User Precautions Vis-À-Vis Enforcement against Attackers. Journal of Management Information Systems. 26, 97-121.

Lazar, J. Feng, & H. Hocheiser. (2010). Surveys: Research Methods in Human-Computer Interaction, West Sussex, UK, Wiley & Sons, 100-107.

Nusca, A. (2009). Smartphone vs. feature phone arms race heats up; which did you buy? ZDNet. Retrieved May 17, 2015.

Mcafee. (2012). MobileeGuide_Jan2012. http://images.mcafee.com/en-us/advicecenter/pdf/MobileeGuide_Jan2012.pdf Retrieved 26 January 2015.

Oulasvirta, A., Rattenbury, T., Ma, L., & Raita, E. (2012). Habits Make Smartphone Use More Pervasive. Personal Ubiquitous Computing (2012).

Peterson, R. R. (2008). Integration Strategies and tactics for Information Technology Governance, 240-280.

Printips. (2011).The growing importance of smartphones. TechneGraphics Inc.

Shi, N. S., & Silvius, G. (2010). Enterprise IT Governance, Business Value and Performance Measurement. Igi Global. http://www.myilibrary.Com?id=292315&ref=toc. [Accessed 26 September 2015].

Shipley, T. G., & Bowker, A. (2014). Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace. Volume 59, Issue 6, page 1685,

Van Grembergen, W. (2004). Strategies for Information Technology Governance. Hershey, Pa, Idea Group Pub. http://www.books24x7.com/marc.asp?bookid=6523.

Williams, M. (2014). The 5 biggest data breaches of 2014 (so far).P.C World.: Retrieved May 17, 2015, from www.pcworld.com/article/2453400/the-biggest-data-breaches-of-2014-so-far.html..