12-14-2013

A Value Focused Thinking (VFT) Analysis to Understanding Users' Privacy and Security Dynamics in Social Networking Services

Nadine A. Maitland Mrs.
University of Technology Jamaica, nadinemland@yahoo.com

Corlane Barclay
University of Technology Jamaica, clbarclay@gmail.com

Kweku-Muata Osei-Bryson
Virginia Commonwealth University, KMOsei@vcu.edu

A Value Focused Thinking (VFT) Analysis to Understanding Users' Privacy and Security Dynamics in Social Networking Services

Paper Category: Research Paper

Nadine Maitland
nadinemland@yahoo.com
Department of Computing
University of the West Indies, Mona
Jamaica
Kingston 7

Corlane Barclay
clbarclay@gmail.com
School of Computing & Information Technology
University of Technology Jamaica
237 Old Hope Road
Kingston 6

Kweku-Muata Osei-Bryson
kmosei@vcu.edu
School of Business
Virginia Commonwealth University
301 W. Main Street
Richmond, VA 23284
USA

ABSTRACT
The rate of growth of Social Networking Services (SNS) has significant implications for computer and cyber-crime management. In exploring the human side of security, studies have shown that any security response requires more than technical solutions. This is even more so as users are often seen as the key point of vulnerabilities for computer systems including SNS. This study seeks to explore what are the important values in understanding measures to maximize end-user security and privacy concerns in SNS settings. The study applies the Value-focused Thinking (VFT) methodology to determine the users' values and objectives, with an initial focus on a developing context. With online users in developing countries surpassing more developed regions, it is imperative that focused attention to this domain is granted. The study found that privacy, confidentiality, integrity of SNS, security controls, awareness campaigns, corporate social responsibility and personal responsibility are fundamental values in maximizing user security and privacy conditions. Corporate social responsibility was one of the findings from this research which underlined the important role of businesses including the service providers in maintaining the integrity of SNS environment.

Keywords: *Privacy, Cybercrime, Security, Users' awareness, Value-focused Thinking (VFT), developing economies*

1. INTRODUCTION
Protecting the privacy and security of data in networked computer systems is a major challenge in this computer age (Landau, 2008).The exponential growth of the Internet and Social Networking Services (SNS) further exacerbated this challenge. According to (Wire, 2010), social networking accounts for approximately 22% of total time spent on the Internet and its growth trajectory suggests that this is increasing. SNS have revolutionized the communication frontier of the 21st century and this is immeasurable (Asur & Huberman, 2010). Social media reports suggest that in 2012 Facebook had over 900 million users, Twitter over 500 million, and the user community continues to grow at a rapid rate. One such example is LinkedIn. In 2012 LinkedIn

had a membership of approximately 150 million. According to reports, in February 2013 their membership increased to 200 million. Research also reveals that there is a spike in the use of SNS in developing countries. According to Tam(2012)the use of social media in developing countries is increasing at a faster rate than in developed countries. The explosion of social networks has not only changed the way we communicate but has also opened an avenue for antisocial and criminal behavior in ways that would not have been possible without technology (Podgor, 2004).While growth in SNS and the use of these services are reflective of development, the threats and vulnerabilities that come with using them also negatively impact national and global development. It can therefore be argued that developing countries are more vulnerable and therefore require an urgent assessment to enable improved end-user security and privacy in SNS.

1.1. Research Problem and Opportunity Statement

According to Young and Quan-Haase (2009), SNS are very easy and convenient to use, however these systems poses privacy concerns and risks to its members. The relative ease at which information can be accessed has made social networks a prime target for criminals(Choo& Smith, 2009). There is a significant increases in cyber-attacks in SNS, as social networks have become the new target for cybercriminals (Hickey, 2011; Saini et al., 2012). The lack of a cyber-army, cyber savvy policy makers and the relative lack of awareness of many SNS users further complicates this situation (Malar, 2012). At the regional level, attempts are being made to address this issue through for example, the harmonization of cybercrime policies and legislation across the Caribbean, and the introduction of the 2001Convention on Cybercrime in Europe(Keyser, 2002). However, based on multiple global and regional reports, cybercrime is an epidemic and SNS is becoming a prime target for these attacks.

Users of SNS in many cases tend to reveal more information than they should and in most of these cases this information is not appropriate in public forums(Al Hasib, 2009).Releasing of private information into the public domain increases the level of vulnerabilities and threats to social networking users. Gharibi(2012) made the point that, end-user's behavior can result in increased privacy and security threats. According to Gross and Rosson (2007), numerous studies have shown that users are the weak link in computer security. While there may be a debate as to whether end-users are a weak link in security, Gross and Rossen (2007); Furnell et al., (2009) pointed out that there exists a point of vulnerability from the end-users. Social networking sites are likened to a "central repository of personal information", and many users are not aware of the dangers that these online social sites pose (Furnell et al., 2009). The Internet makes it easier for information thieves to gather information used to bait and lure targets (Power, 2001). Increased exposure to security threats from online use is primarily attributed to the lack of knowledge and understanding of the imminent threats(Gross & Rossen, 2007).

The lack of, or insufficient end-users' awareness of privacy and security concerns, risks and threats in SNS has resulted in a significant growth of cybercrimes being committed in the social media domain. According to Ho et al., (2009) the privacy setting in SNS are inflexible and this has contributed significantly to the exposure of private information and led to other vulnerabilities. An analysis of the global crime statistics shows an alarming increase in incidences of crimes such as cyber-bullying, cyber-stalking, identity theft and social engineering (Ho, et al., 2009). The continuing lack of awareness in or understanding of, the proper use and safeguards in using social media increases the risks and vulnerabilities at the individual,

corporate and national levels. This has implications for individual, organizational and national security along with socio-economic issues. As noted by Henderson (2003) and Saini et al., (2012) computer criminals pose not only individual or economic threat but threats to national security.

Technology alone cannot fight cybercrime (Power, 2001). Collaboration among government, private sector and academics is necessary (Landau, 2008). Currently, there is a paucity of research on the implications of cybercrimes on user privacy and security in developing countries, including the Caribbean region and even more so in the social networking domain. An analysis of the literature shows that most studies primarily focus on developed countries (Furnell et al., 2009); Ellison et al., 2007; Kaplan & Haenlein, 2010). There is also a paucity of research as it relates to the application of the Value Focused Thinking (VFT)approach in the social networking domain.VFT is designed to help uncover hidden values of users which can lead to more productive information collection. Such an approach can improve the level of understanding of users' security and privacy dynamics and better enable focused solutions to manage Internet and SNS security, and cybercrime.

The purpose of this study is to examine how to maximize users' general security and privacy threats in the social networking domain. This may be garnered through an appreciation, awareness or increased responsibility in end-user security. In biological psychology, awareness is a human's perception and cognitive reaction to a condition or event (Wikipedia, 2013). In this context, it is the users' perception and cognition to privacy and security in SNS. The study therefore seeks to determine *what are the conditions or events that are necessary to maximize security and privacy conditions/dynamics?* And *what are the values that are important in security and privacy and the means to achieve them?* It is important to note that the study on awareness is not about what the users know or do not know about security and privacy, but rather what do they need to know to maximize their security and privacy dynamics to minimize risks, threats and concerns in SNS and what are the important values in achieving this.

The current study will focus on the developing country context, with initial assessments done in the Caribbean island of Jamaica. The Value-Focused Thinking (VFT) approach is used to determine diverse categories of users' values and objectives within the decision context of the users' awareness of privacy and security threats on social networking sites. In other words, the study is to determine the users' values in maximizing their security and privacy experiences in SNS. The VFT is designed to focus the decision-makers, including users in this context, on the essential activities that must occur prior to solving a decision problem (Keeney, 1994). According to Keeney (1994) this alternative approach of identifying alternatives and then considering the values or criteria to evaluate those objectives is reactive and limit the effectiveness of the decision-making process. The study is therefore motivated to utilize a proactive process in understanding values, means to achieve them and thereby enhancing the decision-making process related to users' security and privacy concerns in SNS. The VFT technique makes it an appropriate methodology to discovering answers to our research goal, and has been used successfully to solve decision problems in multiple contexts(Barclay &Osei-Bryson, 2009; Dhillon & Torkzadeh, 2006; Dervin et al., 2007).

The rest of the paper is organized as follows: a literature review of social media and networks , its development, benefits and threats; discussion on the research methodology which is the VFT approach being applied to assess user awareness of security threats on SNS; the application of the VFT approach is discussed highlighting the steps undertaken to derive the means-end network; the preliminary results are discussed; and concluding remarks relating to the research implications, limitations and future related studies are made.

2. LITERATURE REVIEW

2.1. Social Media and Social Networks

The analysis of social networks in the social sciences dates back nearly a century (Kane et al., 2012). The reliance on a computer network as a central construct makes social networks unique among the social sciences (Borgatti, 2003). A network is a set of nodes that are interrelated by "dyadic ties", the nodes or actors can take any form ranging from individual to collective (Borgatti, 2003).According to Barnes(2006) social media is a term used to refer to an "*umbrella concept that describes social software and social networking*". Social software refers to variegated, heterogeneous applications that allow individuals to communicate and also track communication across the web as they happens Barnes (2006).According to Borgatti (2003) ties conceptualizes a social relationship; example "*Friend of" or "boss of*" can be loosely connected such as "*talk to*" and so on.With the changing landscape there are many categories of social media, with one popular classification being by its characteristics. According to Ellison, et al.,(2007), these sites can be oriented towards work-related contexts (e.g., LinkedIn.com), romantic relationship initiation (the original goal ofFriendster.com), connecting those with shared interests such as music or politics(e.g., MySpace.com), or the college student population (the original intentionofFacebook.com).

2.2. Benefits, Challenges & Risks in Social Media

Businesses use social media to engage their customers since this tool has proven to be more cost effective and efficient than traditional means of communication (Kaplan & Haenlein, 2010). The potential gains that can be derived through the application of this tool for business at different levels, are in no way trivial (Kaplan & Haenlein, 2010). For example Dell is reported to have made one million from sales alerts in Twitter (Kaplan & Haenlein, 2010).

With the advent of the Internet as a digital multi-media communications platform, companies from all sectors and regions have sought to take advantage of the business opportunities that SNS can provide. With globalization and the digital economy, government agencies are also taking advantage of doing business online and on social networks. In Jamaica, anecdotal data reveals that many agencies, including tax administration, have begun to collect benefits from this medium. Banks and Financial Services not only utilize e-banking services, but also have a social network presence to reach current and prospective clients and market and promote their products and services. Analysis of social networks shows these companies using pages for basic promotions and marketing.

Designing of security and privacy controls is not the priority of SNS designers (Echaiz& Ardenghi, 2009).SNS are designed with relatively weak security and access control mechanisms because these are not key factors in the development of SNS and, this has resulted in the emergence of key security risks in online social networking sites(Echaiz & Ardenghi,

2009).According to Cutillo et al., 2009) online users of social networks are adversely affected from various security and privacy issues because of the exposure on these online sites. In the last year there have been multiple media reports of hacking, site defacement and other types of crimes on social networks. The recent defacement of Burger King's slogan and the hacking of its Twitter account are examples of security threats on social media(Jones, 2013). In Jamaica, for example, there have been growing incidences of hacking and defacement of sites which is counter to the general perception that companies are safe because of the history of no known incidences (Robinson, 2013). Recent media reports reveal that several government agency sites have been hacked, including the Office of the Director of Public Prosecution (Luton, 2013). The challenges are compounded by lack of sufficient reporting and awareness of security threats. This can be illustrated by the example that user accounts on Twitter were hacked and only 250,000 of the 200 million users were warned or informed of the attack (Jones, 2013).

2.3. Security and Privacy Threats in Social Media

An analysis of business reports has shown that social media is categorized among one of the top security threats for 2013.According to Liu et al., (2003) and Whitman (2004)the nature of the Internet has created new opportunities for businesses and organizations to share information across networks, and this dynamic environment has created more complex security and privacy issues both internally and externally. The problem of security and privacy is even greater as most techniques that were developed for data protection are geared towards the "earlier" generations of computing that operated in a single, closed and well-defined boundary (Liu et al., 2003). According to Landau (2008) resolving cyber privacy and security issues are difficult and have proven to be a major challenge of our time. Landau (2008) pointed out that technological solutions are not always "clear-cut" as these involve technical and societal concerns. The lack of universally accepted information security critical factors taxonomy and indicators makes security management a tough one. This coupled with the lack incentives for designing these policies, have resulted in failure in this regard (Landau, 2008; Torres et al., 2006). According to Echaiz and Ardenghi (2009) the development of technological tools such as data mining, content-based image retrieval, image tagging and cross profiling opens the door for breaches of privacy. These tools can be used to create a digital file of personal information, link images across services and websites and deduce locations from anonymous profiles(Echaiz & Ardenghi, 2009; Al Hasib, 2009. The information gathered through these medium are often used in cases of blackmail, identity theft, stalking, corporate espionage and even lost job opportunities (Rosen, 2010; Echaiz & Ardenghi, 2009; Al Hasib, 2009).

According to Whitman (2004) combating this problem begins with understanding the threats. Solutions for privacy and security are not mathematical, but are instead tied up in human behavior (Landau, 2008). Yet, even in light of this, information security continues to be ignored by many managers, employees and on a personal level (Whitman, 2004). This negligence has resulted in more frequent security breaches that often result in more damage than necessary (Whitman, 2004). Therefore, users regardless of age, socio-economic background or purpose of use, are at risk and vulnerable. The lack of awareness by users further exacerbates the security threats and risks.

Barnes (2006) stated that the lack of awareness of users of social networking sites is further complicated becausethe public versus private boundaries of social media space are unclear.

Users of social networks reveal too much personal information not realizing the danger of social online sites(Barnes, 2006).A survey that was conducted at Carnegie Mellon University revealed that users of Facebook provided information ranging from their date of birth to their cell-phone number. The survey further revealed that 90.8% of the profiles contain an image, 87.8% of the users reveal their birth date, 39.9% listed a phone number and 50.8% listed their current residence (Luo et al., 2009).

Social network users readily share personal information without having a clear idea who is accessing the information (Krishnamurthy & Wills, 2008). This trend will likely persist as users have the misconception that social networks are secure (Luo et al., 2009). For example, Luo et al., (2009) noted that Facebook gives unaware users no choice; instead they have adopted an all or nothing approach. Researchers pointed out that even though the public is updated regularly about the threats in relation to privacy, a significant amount of social network users are still unaware of the potential threats to privacy and even apt to expose personal information (Luo et al., 2009). According to researchers Goecks et al., (2009) social navigation systems should provide users with easy to understand guidance to help them make "informed" security and privacy decisions instead of requiring them to understand low-level technical details.

3. RESEARCH METHODOLOGY

The research employs the Value-focused Thinking (VFT) methodology to better understand how users can maximize their awareness of security and privacy concerns, issues and threats in SNS.VFT is a decision technique developed by Keeney (1994)where values are the primary focus of the decision-making process. One principal benefit of this approach is that better alternatives for a decision problem can be generated once objectives have been established over the more traditional method where alternatives are first identified after which the objectives are specified(Keeney, 1994). Therefore the VFT approach further enhances the decision-making process. VFT is designed to focus the decision maker on the essential activities that must occur prior to solving a decision problem (Keeney, 1994). In our study context, we attempt to obtain from the participants some of the essential activities that must occur to improve or maximize end-users awareness of security and privacy issues, concerns and threats in SNS. It is therefore an appropriate approach to achieve our research objectives.

The VFT approach involves several steps, (figure 1):

1. The identification of the stakeholders. Stakeholders in this context are individuals that have a vested interest in the security of the social networking domain.
2. The stakeholders are questioned about their values concerning the specific area under consideration. Values are those principles that one strives for, and these define the entire considerations one cares about in a specific situation (Keeney, 1994).
3. The identified values are converted into objectives. An objective is characterized by three features, namely a decision context, an object and a direction of preference (Hassan, 2004). Multiple objectives can be derived from a decision statement.
4. The objectives are determined by the process of distinguishing between means and fundamental objectives. Fundamental objectives refer to the objectives underlying the essential reasons for the problem under consideration, while means objectives are regarded as

those whose attainment will help achieve the fundamental objectives (Hassan, 2004). To perform this step, the "*why is this important?"* procedure is performed. At this stage each objective is evaluated against this question and if an objective is found to be important because it helps achieve another objective, it is categorized as a means objective; otherwise it is a fundamental objective.

5. A means-ends objective network is constructed to show the inter and intra relationships among the means and fundamental objectives, (Figure 2). The network is then used to derive cause–effect relationships and to generate potential decision opportunities.

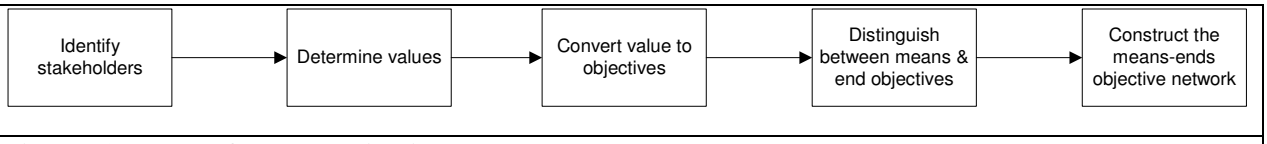

Figure 1: Value-focused thinking process

The VFT has already been applied successfully in identifying stakeholders' values in a particular decision context in multiple domains. For example, Hassan (2004) applied it to the environmental selection of wall structures, Sheng, et al., (2005), used the approach to describe the value of mobile applications, Drevin, et al.,(2007) applied it to the assessment of ICT security awareness in academic environment, and Barclay &Osei-Bryson(2009)used it to determine project objectives and measures across different project contexts.

4. APPLICATION OF VALUE FOCUSED THINKING

The VFT methodology was applied in a university environment with students as the principal target population. According to Lawler and Molluzzo (2010), students in academic institutions spend between 1 and 5 hours weekly on social networking sites, and 90% of university students use networking sites daily. SNS have become an integral part of the lives of the youth and young adult population, and they tend to be more vulnerable to risks due to relative lower level of awareness of security (Furnell, 2009). This age group correlates with the age group interviewed and motivates the use of students to determine values associated with security and privacy dynamics.

A group of 10 students were selected to be interviewed. Similarly to Drevin, et al., (2007), discussion documents were used to elicit information from the participants. VFT guidelines were followed to determine the participants' values based on the questions below. The questions were supplemented by the "why it is important?" question to determine the category of objectives.

The issues discussed in the interviews included:

1. What is important to you regarding the use of social networking sites?
2. What is important to you regarding security awareness in social networking sites?
3. What are your current concerns relating to security threats on social networking sites?
4. What can be done to raise awareness of security and privacy threats in social networking sites?
5. What are some of the issues that prevent safer use of social networking?
6. How would you evaluate awareness of security threats on social networking sites?
7. What would you tell other users to do to keep safe on social networking sites?

8. What can the owners of social networking sites do to increase your awareness of security threats?

The steps highlighted in figure 1 were followed and a preliminary network of means and fundamental objectives was derived (figure 2) that highlights key areas that can be addressed in better understanding the end-users' security and privacy values in using SNS.

5. PRELIMINARY RESULTS

The means-end network was derived from the information collected from the discussion questions and is presented in figure 2. The steps in the VFT process were followed to identify the set of means and fundamental objectives. The fundamental or end objectives show the values and ultimate concerns of the users of the SNS. During the discussion segment students identify multiple values such as privacy on sites, security of data and communication of threats or awareness campaigns. These values were translated to common form of objectives and the rationale for its importance test applied to determine the hierarchy of the objectives. For example they were asked why profile protection was important and responses such as the need to feel safe or to enhance controls were identified. The end or fundamental objectives and the means or facilitating objectives were identified and were structured resulting in the means-end network.

The fundamental objectives identified were shown to be aligned to the goals of information security i.e. integrity, confidentiality and privacy (ISO 27001). These goals also underlined issues at the management, organizational and society levels i.e. individual and corporate social responsibility, education awareness and security measures and controls. The study confirmed that general issues of information security impacts social networking. The important issue of responsibility was further explicated to include not only individual responsibility but also corporate social responsibility which suggests that all levels of society have an important role to play in minimizing the effects and economic impact of cybercrime. Integrated stakeholder-based solutions are therefore imperative to effectively addressing these threats.

Table 1: Fundamental objectives

1. Maximize privacy • Personal data security, prevent sharing too much information, safeguarding personal information,
2. Maximize confidentiality of personal information • prevent sharing too much information, safeguarding personal information, security of user profile, strong password
3. Maximize integrity of SNS • user awareness campaigns, security assurance of personal data
4. Maximize security controls • security protocols, safeguarding of personal information, security of user profile, protecting self, strong password, data security
5. Maximize security awareness campaigns • prompts, public awareness drive, educate users of potential threats, broadcast messages, forums, organized campaigns
6. Maximize organizational social responsibility

• prompt users about security threats, inform users about dangers, provide adequate security controls
7. Maximize individual responsibility • personal data security, prevent sharing too much information, safe guarding personal information, protecting self, strong password

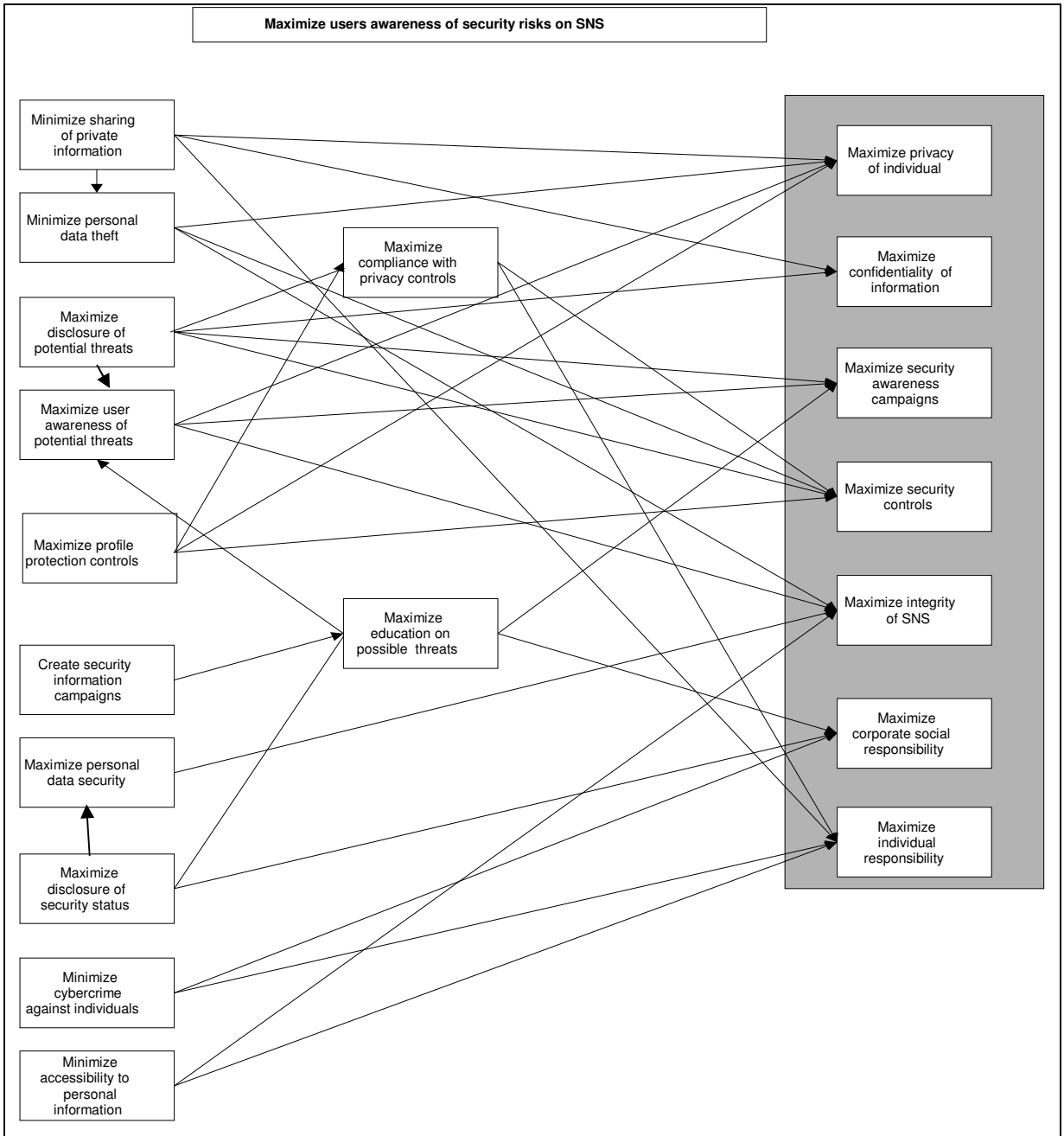

Figure 2. Means-End Network (Preliminary)

Discussion on Fundamental Objectives

Seven fundamental objectives were identified (Table 1) and these indicated the values important to the participants and are necessary in enhancing their security and privacy experiences in SNS: maximize privacy; maximize confidentiality of personal information; maximize integrity of SNS; maximize security controls; maximize security awareness campaigns; maximize organizational social responsibility; and maximize individual responsibility.

Maximize confidentiality of personal information

Confidentiality is to ensure that the information is not made available or disclosed to unauthorized entities (ISO 27001: 27002).The users on social networking believe that it is important that their personal information is not disclosed to unauthorized or unintended persons. Objectives such as minimizing public access to profiles, profile and password controls and measures were identified.

Maximize privacy of individual

Privacy is the state or condition of being free from being observed or disturbed by other people (freedictionary.com). We extend the definition to consider not simply "other people" but rather "unauthorized persons". Privacy can also be seen as the right to "control the dissemination of personal information" and freedom from surveillance (Hugl, 2011).This is distinguished from confidentiality as privacy applies not only to the information but also the individual. The protection of privacy is very relevant in SNS context. As such, persons do not want to be watched or intruded on by authorized persons. Minimize sharing of personal information and minimize accessibility to private information were values discussed by the participants.

Maximize integrity of SNS

Integrity is to protect the accuracy and completeness of information and the methods that are used to process and manage identities (ISO 27001: 27002). The integrity of the service providers and their information infrastructure were key considerations for the participants.

Maximize security controls

Controls are safeguards or countermeasures. These may be any administrative, management, technical, or legal method that is used to manage risk entities (ISO 27001: 27002). Rules, policies and laws are important methods to help minimize security threats and while the participants primarily identified administrative and technical measures, organizations and regulatory agencies need to identify and implement effective control mechanisms. While there may be challenges in encouraging or motivating users to observe policies and procedures establishing suitable controls and facilitating awareness of controls are imperative (Hugl, 2011; Warkentin& Johnston, 2008).

Maximize security awareness campaigns

Education campaigns sensitizing users to the dangers and vulnerabilities on SNS are an important value for the participants. The participants thought that formal awareness campaigns by different stakeholders, including service providers, were important to maximizing awareness

and improving experiences in the SNS environment.

Maximize individual responsibility

Responsibility is something for which one is responsible, i.e. a duty, obligation, or burden (freedictionary.com). Users have a duty and obligation to maximize their understanding and awareness of security threats and help safeguard cyberspace. Objectives such as minimizing sharing of private information impact the possible reduction in threats such as identity theft and fraud.

Maximize organizational social responsibility

Social responsibility is the obligation of an organization's decision-makers towards the welfare and interests of the society in which it operates (businessdictionary.com). With the proliferation of cybercrime, each stakeholder has a part to play in improving the security of cyberspace. Objectives such as information on possible security threats and disclosure of security status and implications were found to be important considerations for participants.

The means objectives are summarized in table 2. Several mean objectives were identified and included minimizing sharing of private information, minimizing personal data theft, maximizing the creation of information campaigns to educate users, maximizing disclosures of security breaches and maximizing profile protection.

Table 2: Means objectives

1. Minimize sharing of private information
2. Minimize personal data theft
3. Maximize compliance with privacy controls
4. Minimize crime
• Hacking, phishing, frauds, imposters, virus
5. Maximize disclosure of potential threats
6. Maximize user awareness of potential threats
7. Maximize profile protection controls
8. Maximize education on possible threats
9. Create security information campaigns
10. Maximize personal data security
11. Maximize disclosure of security status
12. Minimize accessibility to personal information

6. Concluding Remarks

The users on social networks continue to grow exponentially across all regions of the globe. This makes it a prime target for cybercriminals as they use various techniques to exploit the vulnerabilities of users. The human side of security forms crucial dimensions of information systems security (Loch et al., 1992). Therefore understanding the social behavior of cybercrime is one strategy to help stem the proliferation of incidences. Since user awareness and understanding has been shown to be a major vulnerability in fighting cybercrime, it is essential to understand users' security and privacy values in this domain. The Value-focused Thinking

(VFT) methodology was applied to this study to determine the security and privacy values and objectives of users of SNS. It focuses on understanding the implications of user security and privacy dynamics to end-user and other stakeholders. This initial study targeted university students as studies have shown that this demographic is a significant stakeholder in SNS (Lawler &Molluzzo, 2010). The results of the study revealed that individual privacy, confidentiality of personal information, integrity of social networks, security measures, awareness campaigns, individual and corporate social responsibilities are important values that are fundamental in maximizing security and privacy conditions in SNS. In addressing these concerns there is a likely chance that security and privacy risks and threats will be reduced or better managed, from the individual and service provider perspectives, thus resulting in a safer cyber environment. It is important to note that several of the fundamental objectives identified are aligned with information security goals (ISO 27001), and can serve as a basis for decision-making and to guide the planning, shaping and development of security awareness strategies and promote healthy use on SNS (Dervin, 2007).

The study, although in its preliminary stages, has significant implications for both research and practice. The study extends the academic discourse in cybercrime and implications of user awareness. Corporate social responsibility, a novel finding, has implications for service providers, organizations and legislations. It suggests that not only individual users have a responsibility, but organizations have a responsibility to ensure the integrity of their service, provide effective awareness campaigns to and for their users, and government needs to implement suitable actions and legislations to promote social responsibility. Although the study is focused on developing economies with data from the Caribbean region, the results have implications for other regions.

This study is important in the research and practitioner domains. This research will contribute to the body of knowledge as very few studies have focused on the implications of end-users' privacy and security concerns, risks or threats on social networks. Further, there is no known study that focuses or uses the developing country context. Therefore information gathered from this study can extend the knowledge base both in terms of contextual representation and the discourse in the psychological or human perspectives in security. It is also hoped that the study can help initiate discussions on the topic and develop solutions to stem this serious and growing vulnerability. Similarly, it can help organizations to design more proactive policies and government can develop appropriate security guidelines and frameworks for online use.

Future research opportunities include extending the category of social networking participants beyond students to further refine the means-end network, develop associated measures and priorities based on multi-criterion decision techniques, examine the implications of corporate social responsibility to the prevention of cybercrime, and studying the implications of user awareness on other decision contexts in the cybercrime domain.

7. REFERENCES

1. Al Hasib, A. (2009). Threats of online social networks. *IJCSNS International Journal of Computer Science and Network Security*, *9*(11), 288-93.

2. Asur, S., & Huberman, B. A. 2010. Prediction of the future with social media. HP Laboratories, 53:492-499. Doi: 10.1109/WI-LAT. 2010.63.
3. Barclay, C., & Osei-Bryson, K. M. (2009). Project performance development framework: An approach for developing performance criteria & measures for information systems (IS) projects. *International Journal of Production Economics*, 124(1), 272-292.
4. Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9).
5. Borgatti, S. P. (2003). The state of organizational social network research today. *Dept. of Organization Studies. Boston College, Boston, MA*.
6. BusinessDictionary (2013). http://www.businessdictionary.com/definition/social-responsibility.html, retrieved on March 2, 2013
7. Choo, K. K. R., and Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. *Asian journal of criminology*, *3*(1), 37-59.
8. 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.
9. Dhillon, G., &Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16(3), 293-314
10. Drevin, L., Kruger, H. A., &Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security*, 26(1), 36-43.
11. Echaiz, J., &Ardenghi, J. R. (2009). Security and online social networks. In *XV CongresoArgentino de Ciencias de la Computación*.
12. 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(4), 1143-1168.
13. Furnell, S., Papadaki, M., & Thomson, K. L. (2009). Scare tactics–A viable weapon in the security war?.*Computer Fraud & Security*, *2009*(12), 6-10.
14. Gharibi, W., &Shaabi, M. (2012). Cyber threats in social networking websites. *arXiv preprint arXiv:1202.2420*.
15. Goecks, J., Edwards, W. K., &Mynatt, E. D. (2009, July). Challenges in supporting end-user privacy and security management with social navigation. InProceedings of the 5th Symposium on Usable Privacy and Security (p. 5). ACM.
16. Gross, J. B., &Rosson, M. B. (2007, July). End user concern about security and privacy threats. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 167-168). ACM.
17. Hassan, O. A. (2004). Application of value—focused thinking on the environmental selection of wall structures. Journal of environmental management, 70(2), 181-187.
18. Henderson, K. (2003). Can the rule of law and technology corral international cyber crime and corruption balance national privacy and security concerns,Available : (http://www1.worldbank.org/publicsector/egov/cyberlaws.pdf
19. Hickey, A. R. (2011, January 2011). Social Networking A Major Threat, Cybercriminals Eye Facebook. Retrieve from www.crn.com/news/security/2290000883/social-networking-a-major-security-threat-cybercriminals-eye-facebook.htm
20. Ho, A., Maiga, A., &Aïmeur, E. (2009, May). Privacy protection issues in social networking sites. In *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on* (pp. 271-278). IEEE.
21. Hugl, U. (2011). Reviewing person's value of privacy of online social networking. *Internet Research*, 21(4), 384-407. Kane, G. C., Alavi, M., Labianca, G. J., Borgatti, S. P., & Center, L. I. N. K. S. (2012).What's Different About Social Media Networks? A Framework and Research Agenda.
22. ISO 27001/ISO 27002, ISO Definitions, http://www.praxiom.com/iso-27001-definitions.htm
23. Jones, C. R. (2013, February 02). Twitter's most serious security threats.BBC News Technology, Retrieved from http://www.bbc.co.uk/news/technology-21305106
24. Kane, G. C., Alavi, M., Labianca, G. J., Borgatti, S. P., & Center, L. I. N. K. S. (2012).What's Different About Social Media Networks? A Framework And Research Agenda.

25. Kaplan, A. M., and Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, 53(1), 59-68.
26. Keeney, R. L. (1994). Creativity in decision making with value-focused thinking.*Sloan Management Review*, 35, 33-33.
27. Keyser, M. (2002). Council of Europe Convention on Cybercrime, The. *J. Transnat'l L. &Pol'y*, *12*, 287.
28. Krishnamurthy, B., and Wills, C. E. (2008, August). Characterizing privacy in onlinesocial networks. In *Proceedings of the first workshop on Online social networks* (pp. 37-42). ACM.
29. Landau, S. (2008). Privacy and security A multidimensional problem. *Communications of the ACM*, *51*(11), 25-26.
30. Lawler, J. P., &Molluzzo, J. C. (2010). A study of the perceptions of students on privacy and security on social networking sites (SNS) on the internet. *Journal of Information Systems Applied Research*, *3*(12), 3-18.
31. Loch, K. D., Carr, H. H., &Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, 173-186.
32. Liu, L., Yu, E., & Mylopoulos, J. (2003, September). Security and privacy requirements analysis within a social setting. In *Requirements Engineering Conference, 2003. Proceedings.*
33. Luo, W., Xie, Q., &Hengartner, U. (2009, August). Facecloak: An architecture for user privacy on social networking sites. In Computational Science and Engineering, 2009. CSE'09. International Conference on (Vol. 3, pp. 26-33). IEEE.
34. Luton, D. (2013, February 3). Hackers attack at least four state bodies in two weeks, Jamaica Gleaner, p 1.
35. Malar, M., N. (2012). "Impact of Cyber Crimes on Social Networking Pattern of Girls", *International Journal of Internet of Things*, Vol. 1 No. 1, 2012, pp. 9-15. doi: 10.5923/j.ijit.20120101.02.
36. Podgor, E. S. (2004). Cybercrime: National, Transnational, or International. *Wayne L. Rev.*, *50*, 97.
37. Power, R. (2001). 2001 CSI/FBI computer crime and security survey. *Computer Security Journal*, *17*(2), 29-51.
38. Robinson, G. (2013, February, 20). Digicel's hack-wack, Jamaica Gleaner, p 1.
39. Rosen, J. (2010, July 21). The Web Means the End of Forgetting. New York Times.
40. Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-Crimes and their Impacts: A Review.
41. Sheng, H., Nah, F. F. H., &Siau, K. (2005). Strategic implications of mobile technology: A case study using Value-Focused Thinking. *The Journal of Strategic Information Systems*, 14(3), 269-290.
42. Tam, D. (2012).Developing nations adopting social media quickly]. CNET News. Retrieved from news.cnet.com/8301-1023_3-57558851-93/developing-nations-adopting-social-media-quickly.
43. Torres, J. M., Sarriegi, J. M., Santos, J., & Serrano, N. (2006). Managing information systems security: critical success factors and indicators to measure effectiveness. In Information Security (pp. 530-545). Springer Berlin Heidelberg.
44. Warkentin, M., and Johnston, A. C. 2008. "IT Governance and Organizational Design for Security Management," in *Information Security: Policies, Processes, and Practices*, D. W. Straub, S. Goodman, and R. L. Baskerville (eds.), Armonk, NY: M. E. Sharpe, pp. 46-68
45. Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, *24*(1), 43-57.
46. Wikipedia (2013). http://en.wikipedia.org/wiki/Awareness: *Retrieved on February 10, 2013*
47. Wire, N. (2010). Social networks/blogs now account for one in every four and a half minutes online. http://www.nielsen.com/us/en/newswire/2010/social-media-accounts-for-22-percent-of-time-online.html: *Retrieved on August17*, 2011.
48. Young, A. L., &Quan-Haase, A. (2009, June). Information revelation and internet privacy concerns on social network sites: a case study of facebook. In *Proceedings of the fourth international conference on Communities and technologies* (pp. 265-274). ACM.