BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)
ISSN (P): 2348-0513, ISSN (E): 2454-471X
Vol. 4, Issue 11, Nov 2016, 67-74

SURVEY ON CYBERCRIME IN STAKEHOLDERS PERSPECTIVE

K SAI PRASANTHI & M CHANDRA SEKHAR

Assistant Professor, Computer Science and Engineering, GIET Gunupur, India

ABSTRACT

Nowadays, Cybercriminal activities are increasing in a faster rate showing an impact on communities as the electronic communication is has increased. In this survey different users views are collected and are analyzed using concept analysis and mapping techniques to make a discrete form of major issues and areas of concern and to provide useful help. This survey shows that there are stakeholders with genuine concerns about information security breaches and malware incursions. Awareness plays a vital role in electronic communication. Cyber bullying is also one of the deep concerns identified by few stakeholders.

KEYWORDS: Survey on Cybercrime in Stakeholders Perspective

INTRODUCTION

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that has no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide. Cybercrime and cybercriminal activities continue to impact communities as the steady growth of electronic information systems enables more online business. The collective views of sixty-six computer users and organizations, that have an exposure to cybercrime, were analyzed using concept analysis and mapping techniques in order to identify the major issues and areas of concern, and provide useful advice. The findings of the study show that a range of computing stakeholders have genuine concerns about the frequency of information security breaches and malware incursions (including the emergence of dangerous security and detection avoiding malware), the need for e-security awareness and education, the roles played by law and law enforcement and the installation of current security software and systems.

Since 1980's , users have been subjected to a raft of electronic security risks and attacks in the forms of information theft, malicious software (malware) deployment, financial scams, extortion, and illegal underground cyber networks. ([1], [2],[3]).

Stakeholder's Perspective

Some ten years later, we believe it is time to revisit the issue of cybercrime, but from a computing stakeholders' perspective. In adopting this stakeholder-based approach, this paper achieves **two major aims**. **First,** we understand the major issues or areas of concern that confront computer users. This under-standing allows us to identify and understand cybercrime and activities by identifying the pressure points (i.e. areas of discomfort) of users. Also comparing the governmental directions in the same regard with the major stakeholder issues or areas of concern. **Second,** through understanding the issues or areas of concern, we are able to offer useful advice and recommendations on what actions to take to reduce the risk of cybercrime. These aims raise some research questions as:

What are the major issues or areas of concern for stake-holders that are exposed to cybercrime?

What steps might be taken by stakeholders to minimize the emerging cybercrime risks or threats?

Are future governmental directions for dealing with cyber-criminal activities consistent with stakeholder concerns?

By better understanding the issues and concerns of computer users at the individual and business levels; and provide useful and positive advice on the avoidance of cybercrime events (i.e. consistent with the aims of Computers & Security). This is a contribution to a broader understanding of cybercrime and cybercriminals, while adding support for the growing number of management protocols and tools being established to address cyber security (e.g. aware-ness campaigns, skills programs, automated technical security processes). This study combined concept analysis and mapping techniques with stakeholder analysis in order to determine the 'actual' issues and concerns of computing stakeholders.

CONTEMPORARY LITERATURE

- In United States law enforcement agencies reported heightened financial losses in the areas of computer based crime and security.
- In another survey of North American business, unauthorized systems breaches resulted in steep rises in financial fraud (up 38%) and reported financial losses (up 115%), compared with the previous year's data [4].
- Other studies highlighted the problems of cybercrime in personal and business settings, while also offering advice and legal mechanisms for victims of cybercrime including taking fast and stealthy actions, concentrating on recovery of funds over criminal prosecution, vigilance and monitoring of criminal activity, and seeking third party disclosure of criminal assets and whereabouts.
- At the governmental level, economic and national security interests were also considered in the strategic context of cybercrime, cyber warfare and the growing threats from cyber terrorism and electronic attacks on key public infrastructure.
- Further studies advocated the use of widespread communication and education programs, urged managerial vigilance and environmental scanning, and offered threat and staff profiling as key cybercrime prevention tools ([5],[6],[7],[8],[9]).

In summary, the extant literature specific to the cyber-crime discipline concentrates on how these criminal activities impact individuals and organizations and what measures (e.g. education, legal, law enforcement) might be enacted to assist stakeholders. This is particularly relevant in the Australian context with some estimates suggesting that individuals and organizations lose up to A$650 million each year due to cybercrime events [10].

RESEARCH METHOD

The research method adopted in this study is based on Concept analysis and mapping (CAAM) techniques.

CAAM is defined as "a structured six-step process, focused on a topic or construct of interest, involving input from one or more participants, that produces an interpretable pictorial view (concept map) of their ideas and concepts and how these are interrelated" [11].

In essence, the ideas, comments, issues and opinions of participants or stakeholders are captured through an elicitation process, and integrated into a consolidated analytical and pictorial schema using CAAM software. The analyses and maps are typically utilized in advisory or decision-making processes or procedures related to the issue under investigation. In the broadest sense, these types of research and evaluation programs can be abstracted to other enquiries, particularly community based problems and issues, like the impacts of cybercrime.

CAAM Procedures and Processes

The CAAM software acquired for this study allowed us to classify the cybercrime concepts and themes, characterize and sort the written inputs, identify the patterns and relationships between cybercrime concepts and themes, and process out any asymmetric information. The Leximancer CAAM software product was selected for use in this study [12].The software allows researchers to select and load stakeholder input files, extract the key cybercrime concepts from the input statements, edit the identified cybercrime concepts prior to reprocessing, undertake the automatic location and coding of cybercrime concepts within the stakeholder inputs and, construct the cybercrime concept maps and statistics profiles. The CAAM software provides three primary information arte-facts [12]. First, the software extracts and outputs a frequency distribution and statistical summary of identified cybercrime concept terms. Also, these concept terms are further grouped into concept themes (i.e. major issue or direction of the collective concept terms, for example ‘web-sites’, within the grouping) and are visible as large circles on the concept maps. Second, the software measures the associative behaviors between the cybercrime concept terms, with the central concepts being those that most frequently co-occur within the stakeholder inputs (also identified on the map as larger concept dots). Third, the software measures conceptual similarity and specific attraction (i.e. clustering of cybercrime concept terms). The software settings points are in accordance with the Leximancer manual and other research studies [12], [13], [14].

The individual and organization inputs were collected on 18 August 2010 from the Parliament of Australia web pages that were established for the Inquiry into Cybercrime, conducted by the House of Representatives Standing Committee on Communications [15]. Importantly, the scope of the cybercrime enquiry provided an aggregated source of stakeholder data for this study. The 66 written stakeholder inputs to the enquiry were grouped and compiled into a 307,000 word file (cybercrimes-tudy.doc) for analysis, with a breakdown of stakeholder.

RESEARCH PROCEDURE

The generation of the cybercrime concept terms, statistics and maps was completed using a two-step research procedure. In the first step, the concept terms (or points) and themes were set to the maximum level (i.e. 100%). This allowed the major cybercrime concept terms within the sixty-six stakeholder inputs to be readily identified and recorded. In the second step, the CAAM software’s Multi-Dimensional Scaling (MDS) feature was used to steadily reduce the concept theme size until a workable cybercrime concepts map, inclusive of the major concept clusters, was developed. Also, the CAAM software’s concept co-occurrence mapping feature was activated to record the strongest associations between the cybercrime concept terms (and the related text/statement) using the text coding function.

Table 1: Summary of Cybercrime Enquiry Stakeholders (Commonwealth of Australia, 2010a)

Stakeholder Group	Stakeholder's Function and Description	Number of inputs	Percentage of Total Inputs (%)
Government	4 State governments (up to 390,000 staff)	25	37
organizations (GOs)	4 Federal research agencies (up to 6600 staff)		
	4 Federal legal and financial regulation agencies (up to 25,000 staff)		
	3 Federal and State Privacy Commissioners (up to 30 staff)		
	2 Domestic law enforcement agencies (up to 7000 staff)		
	2 International law enforcement agencies (up to 600 staff)		
	2 Military and National security organizations (up to 120,000 staff)		
	2 Federal technology policy and regulation agencies (up to 5000 staff)		
	1 International government organization (up to 2300 staff)		
	1 Government business enterprise (up to 34,500 staff)		
Non government	8 Information and technology special interest groups	19	29
organizations (NGOs)	(rep. up to 250 businesses and over 20,000 individuals)		
	5 Financial industry special interest groups (rep. up to 120 businesses)		
	3 Not-for-profit businesses (covering standards and technology advisory)		
	2 Tertiary level research centres (covering technology and law)		
	1 High school level advocacy group (covering state funded education)		
Public and private	7 Large to medium sized security software businesses (up to 17,400 staff)	19	29
companies	7 Large to medium sized technology, media and film		
	businesses (up to 89,000 staff)		
	3 Medium to small consulting businesses (up 200 staff)		
	1 Large telecommunications business (up to 45,300 staff)		
	1 Medium sized bank (up to 700 staff)		
Individuals	3 adult males between the ages of 30 and 50 yo commenting	3	5
	on Internet domain, education and security issues.		

Table 2: Cybercrime Concept Statistics Summary

Concept Statistic	Data Set: Cybercrime Enquiry Written Submissions	
Cybercrime	74	
concepts		
identified (No.)		
Total words	4150	
analysed/		
cybercrime		
concept		
Cybercrime		
concept count		
High	Information (1046)	
Low	Study (105)	
Cybercrime concept	[information] [cyber] [computer]	
themes (No.)	[education] [website] [online] [people] (7)	

Central cybercrime concepts (absolute concept count)	[information] (1046)	[services] (521)
	[security] (939)	[risks] (466)
	[cyber] (864)	[internet] (452)
	[online] (839)	[identity] (446)
	[crime] (747)	[data] (445)
	[computer] (671)	[fraud] (429)
	[users] (626)	[theft] (424)
	[consumers] (525)	[Australian] (452)

RESULTS

Descriptive Statistics – Cybercrime Concept Terms

In Table 2 , as seen amongst the 74 identified cybercrime related concept terms, the most common term raised by stakeholders was 'information' with an observed occurrence rate of 1046. The concept map showed that the stakeholder inputs yielded 16 central (i.e. most frequently co-occurring) concepts. The linear maps also showed that the cybercrime terms were enfolded within seven major concept themes (see Figure 1).

Cybercrime Clusters – Major Issues and Areas of Concern

Activation of the CAAM software's concept co-occurrence mapping feature identified six major cybercrime related clusters (i.e. cybercrime issues and areas of concern). The cluster summaries show high concentrations of concept terms (i.e. 5043e2247 cybercrime concept terms per cluster) within each cluster (note, average concept occurrences ranging from 561 to 281 terms). The clusters and central terms were concentrated in the areas of information security breaches (e.g. personal identity theft), security systems and software, the role of law and law enforcement agencies, awareness of risks of online fraud and scams, malicious software and website attacks, electronic security education and IT literacy, and, the reporting of cyber bullying of young people at school.

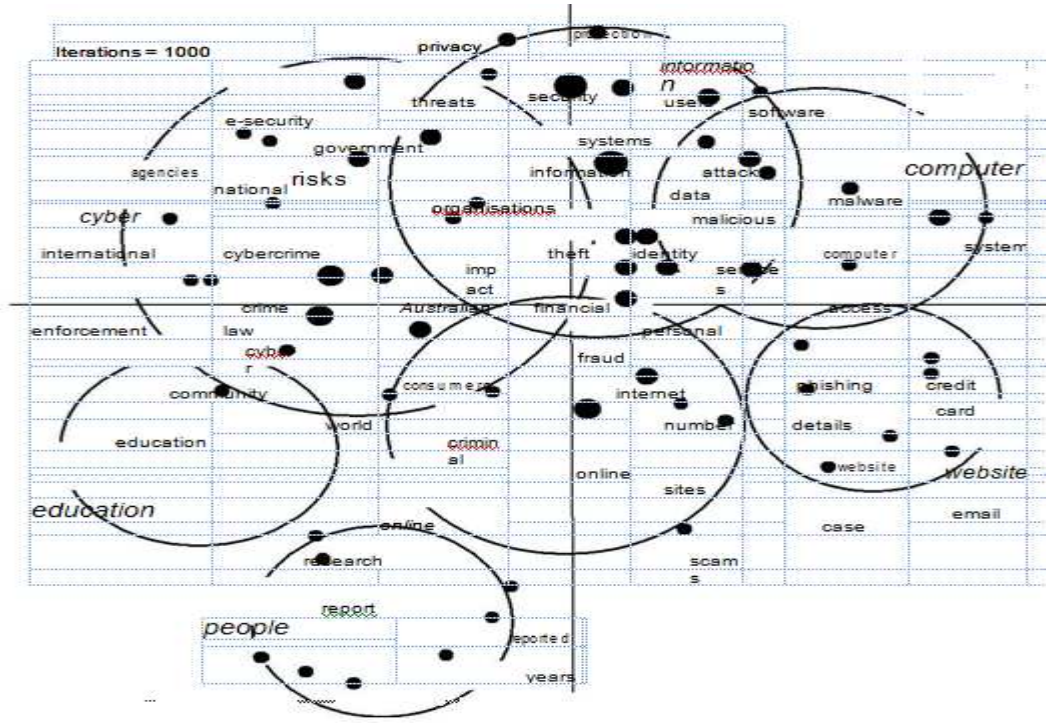

Figure 1: Cybercrime Terms and Themes.

CONCLUSIONS

In this report it asserts that the use of stakeholder analysis and CAAM techniques in cybercrime research represents a valuable contribution and extension of qualitative research into the field of computers and security. We also acknowledge the limitations of research that uses a relatively small number of stakeholder inputs, when compared with the 5 million households that use computers in Australia today. This study also recommends the use of the CAAM techniques and stakeholder analysis methodologies to other researchers in the field of information security. The analysis exposed the genuine uncertainties and concerns of computing stakeholders in relation to the prevalence of information security breaches and malware, requirements for ongoing e-security awareness and education programs, the legitimate role of law and law enforcement, and the requirements for security software and systems. The Australian government is looking to strengthen its approach to cybercrime and accede to the Council of Europe Convention on Cybercrime in the near term [16]. It is also advisable that stakeholders can take up various initiatives and measures to reduce the risks of cybercrime events, including improving awareness and education or cooperating with law enforcement.

In closing, cyber bullying remains a serious human and mental health issue in our communities. And the growing number of high profile bullying incidents exposed using the online environment (see the international YouTube profile of bullied Australian schoolboy, Casey Heynes) [17].We were also clearly moved by the account of the cyber bullying and subsequent suicide of teenager Ryan Halligan in Kowalski et al. [18] There is a sincere hope that, with the help of governments (including new laws, like those proposed in the Australian state of Victoria) and communities, any form of bullying will find suitable remedies in the future [19][20].

REFERENCES

1. Amoroso EG. Fundamentals of computer security technology. Upper Saddle River, NJ: Prentice Hall; 1994.
2. Spafford EH. Computer viruses as artificial life. Journal of Artificial Life 1994; 1(3):249-65.
3. Jain A. Cyber crime issues, threats and management. Delhi, India: Isha Books; 2005.
4. Computer Security Institute (CSI). CSI/FBI computer crime and security survey. 5th ed. New York, NY: CSI; 2000.
5. Computer Security Institute (CSI). CSI/FBI computer crime and security survey. 14th ed. New York, NY: CSI; 2009.
6. Nykodym N, Taylor R, Vilela J. Criminal profiling and insider cyber crime. CLSR Computer Law and Security Report 2005; 21: 408-14.
7. Nykodym N, Kahle-Piasecki L, Marsillac E. The managers guide to understanding, detecting and thwarting computer crime: an international performance issue. Performance Improvement Journal 2010; 49(5):42-7.
8. Nykodym N, Ariss S. Fighting cybercrime. Journal of General Management 2006; 31:63-70.
9. Nykodym N, Taylor R. Communication: a vital tool to combat cyber crime. CLSR Computer Law and Security Report 2007; 2: 185-9.
10. Richards K. The Australian Business Assessment of Computer User Security (ABACUS): a national survey. Research and public policy series no. 102. Canberra: Australian Institute of Criminology (AIC); 2009.

11. Trochim WKM. An introduction to concept mapping for planning and evaluation. Evaluation and Program Planning 1989; 12(1): 1-16.
12. Leximancer. Leximancer user manual version 2.25. Brisbane, Australia: Leximancer; 2005.
13. Martin NJ, Rice JL. Profiling enterprise risks in large computer companies using the Leximancer software tool. Risk Management: International Journal 2007; 9(3):188-206.
14. Smith AE, Humphreys MS. Evaluation of unsupervised semantic mapping of natural language with Leximancer concept mapping. Behaviour Research Methods 2006; 38(2):262-79.
15. Commonwealth of Australia. Inquiry into cybercrime, House of Representatives standing committee on communications. Available from: http://www.aph.gov.au/House/committee/ coms/cybercrime/index.htm; 2010a [accessed 18.08.10].
16. Commonwealth of Australia. Review into treaties (report no. 116), joint standing committee on treaties. Available from: http:// www.aph.gov.au/house/committee/jsct/1march2011/report. htm; 2011 [accessed 20.05.11].
17. Klein N. Casey heynes breaks silence over bully video from chifley college and thoughts of suicide. Available from:. Australia: Daily Telegraph http://www.dailytelegraph.com.au/news/ casey-heynes-breaks-silence-over-bully-video-from-chifley-college-and-thoughts-of-suicide/story-e6freuy9-1226024997247; 2011 [accessed 21.03.11].
18. Kowalski RM, Limber SE, Agatston PW. Cyber bullying: bullying in the digital age. Malden, MA: Wiley/Blackwell; 2007.
19. Butcher S. Brodie's suicide prompts law on bullying. Available from:. Australia: The Melbourne Age http://www.theage.com. au/small-business/brodies-suicide-prompts-law-on-bullying-20110405-1czub.html; 2011 [accessed 05.04.11].
20. Parliament of Victoria. Crimes amendment (bullying) bill (5.04. 2011); 2011.