Impact of Cybercrime on SMEs

Robin Raju
Eastern Institute of Technology
Napier, New Zealand
Robin.r86@gmail.com

Michael Verhaart
(Supervisor)
Eastern institute of Technology
Napier, New Zealand
mverhaart@eit.ac.nz

ABSTRACT

Organisations of all sizes are now increasingly dependent upon information and communication technology for their business activities. The number of cybercrimes also rises with the advances in technology and it needs organisation to make sure their systems are completely secure from all external attacks. But evidence shows that cybercriminals concentrate more on SMEs because of the security practices within small and medium enterprises. In this research proposal the impact of cybercrime on SMEs in different countries were reviewed. The research proposal also contains a detailed comparison of the cost associated with cybercrimes and reasons behind the increase in its number. The findings clarify the need for conducting a research on the impact of cybercrime on small and medium scale businesses particularly in New Zealand.

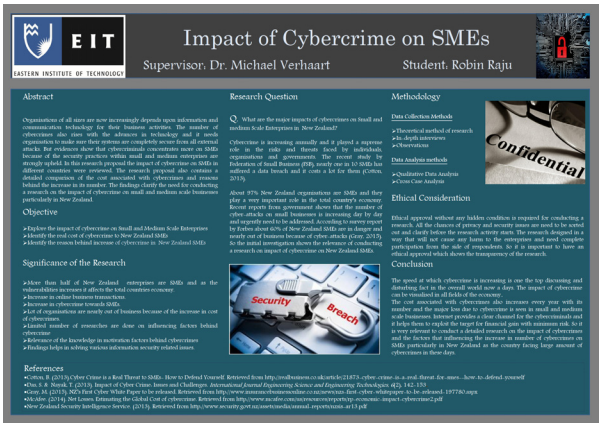
Keywords: Cybercrime, Security, SME, Impact on business, Cost.

1. INTRODUCTION

Information systems security is the critical issue and major concern for any enterprises regardless of size, shape or industry. Security breaches cause huge financial loss to an organisation particularly in Small and Medium Scale Enterprises (SMEs). The threats against SMEs are increasing at an alarming rate and most of the times crimes remain invisible and criminals are not prosecuted. Small and Medium Scale Enterprises (SMEs) plays a very important role in the economy of many countries and so the threats and attacks against the SMEs made great impact on a countries economy.

Majority of SMEs are in trouble because of the continual increase in cost of cybercrimes. In New Zealand about 97% of the businesses are SMEs and it amounts more than quarter of the country annual GDP. So the vulnerabilities to SMEs due to cybercrimes seriously affect the economy and very crucial to the country's overall security which needs to be addressed immediately.

While considering the impacts of cybercrime on different fields all over the world, it is important to find out a perfect method to regulate or controls its presence. There are large number of researches are conducted on the technical aspects of cybercrime but the reasons or motivational factors behind the cybercrimes are not yet clearly identified.



This poster appeared at ITx 2016, incorporating the 7th annual conference of Computing and Information Technology Research and Education New Zealand (CITRENZ2016) and the 29th Annual Conference of the National Advisory Committee on Computing Qualifications, Wellington, New Zealand, July 11-13, 2016. Michael Verhaart, Emre Erturk, Aaron Steele and Scott Morton (Eds).

2. LITERATURE REVIEW

Internet and computer technology makes life so speedy and fast but also in danger because of the threat from the deadliest type of criminality termed as Cybercrime. This means computers and computer networks are act as a tool, a target or a place of cybercrimes (Das & Nayak, 2013).There is no generally agreed definition for Cybercrime. Cybercrimes are considered as those activities with the use of computers to steal or retrieve information stored online or from another database or damage of data and equipment through trespassing in to others network and computer (Saini, Rao & Panda, 2012).

Cyber risk ranked third by Lloyd's Digital Risk Index in 2013 when considering the largest risk facing the global business. As per the recent survey by Marsh & McLennan Companies cyber risk become the second largest emerging threat affecting New Zealand businesses within two years (Akshay, 2013).

Most of the small businesses are not install proper security measures against threats and these cause criminals attracted towards small businesses and also act as a major reason for majority of small business failure (Bressler, 2009). According to McAfee the annual cost to the global economy from cybercrime is estimated to be more than $400 billion which is equal to more than the national income of most countries and governments (McAfee, 2014). New Zealanders costs 463 million dollars in the 2012 due to cybercrime and the major reason for it was poor security practices followed in organisations (Hall, 2013).

Lack of training and knowledge on cybercrimes, spending more on other business matters and less on IT security and using old version systems without updating are considered to be some of the major reasons for rise in cybercrime in New Zealand (Robert & Wolfe, 2015).

3. OBJECTIVES

The objectives of the research are:

- To explore the impact of Cybercrime on Small and Medium Scale Businesses
- To identify the real cost of Cybercrime to New Zealand SMEs
- To identify the reason behind increase of cybercrimes in New Zealand SMEs

4. RESEARCH QUESTION

For this research the question being addressed is "What are the major impacts of cybercrimes on Small and medium Scale Enterprises in New Zealand?"

Cybercrime is increasing annually and it played a supreme role in the risks and threats faced by individuals, organisations and governments. The recent study by Federation of Small Business (FSB), nearly one in 10 SMEs has suffered a data breach and it costs a lot for them (Cotton, 2013).

About 97% New Zealand organisations are SMEs and they play a very important role in the total country's economy. Recent reports from government shows that the number of cyber-attacks on small businesses is increasing day by day and urgently need to be addressed. According to survey report by Forbes about 60% of New Zealand SMEs are in danger and nearly out of business because of cyber-attacks (Gray, 2015). So the initial investigation shows the relevance of conducting a research on impact of cybercrime on New Zealand SMEs.

5. METHODOLOGY

The purpose of this research is to identify the impact of cybercrimes in Small and Medium scale Enterprises (SMEs). The theoretical research method is used to collect information about impact of cybercrimes in SMEs from different countries. The secondary research sources like previous research paper, company reports, journals and websites are going to use for the purpose. The study also aims to interview IT specialists and managers in various New Zealand SMEs for the purpose of collecting required data on cybercrimes. And observe various organisation activities and documents to find the reason for increase in cybercrimes and also to identify the monetary loss due to cybercrimes.

The research proposes to use qualitative data analysis methods and to employ inductive and deductive approaches to categorise the data. The main aim of the research is to find the data common to different organisations and to identify the reason behind the increase in number of cybercrimes.

The results from different countries collected from different sources are then proposed to categorise and analyse using cross case analysis method. This might help to understand the existing cybercrimes in various countries and also the style of cybercriminals.

6. ETHICAL CONSIDERATION

Ethical approval without any hidden condition is required for conducting a research. All the chances of privacy and security issues are need to be sorted out and clarify before the research activity starts. The research designed in a way that will not cause any harm to the enterprises and need complete participation from the side of respondents. So it is important to have an ethical approval which shows the transparency of the research.

7. CONCLUSION

The speed at which cybercrime is increasing is one the top discussing and disturbing fact in the overall world now a days. The impact of cybercrime can be visualised in all fields of the economy.The elevation in the number of cybercrime shows that it is almost impossible for the law enforcement agencies and IT specialists to completely eliminate its effects. It is mainly because high level of technical knowledge holds by cybercriminals and they always use different methods and prefer most advanced tools and technologies.

The cost associated with cybercrimes also increases every year with its number and the major loss due to cybercrime is seen in small and medium scale businesses. Internet provides a clear channel for the cybercriminals and it helps them to exploit the target for financial gain with minimum risk. So it is very relevant to conduct a detailed research on the impact of cybercrimes and the factors that influencing the increase in number of cybercrimes on SMEs particularly in New Zealand as the country facing large amount of cybercrimes in these days.

8. REFERENCES

Akshay, S. (2015). Safeguarding Business from Cyber Threats Embracing Cyber Risk Management. Retrieved from http://www.deltainsurance.co.nz/portals/71/Delta_Cyber.pdf

Bressler, M. S. (2009). The Impact of Crime on Business: A Model for Prevention, Detection & Remedy. *Journal of Management & Marketing Research, 3*(2), 1-12

Cotton, B. (2013).Cyber Crime is a Real Threat to SMEs-How to Defend Yourself. Retrieved from http://realbusiness.co.uk/article/21873-cyber-crime-is-a-real-threat-for-smes--how-to-defend-yourself

Das, S. & nayak, T. (2013). Impact of Cyber Crime: Issues and Challenges. *International Journal Engineering Science and Engineering Technologies, 6*(2), 142-153.

Gray, M. (2015). NZ's First Cyber White Paper to be released. Retrieved from http://www.insurancebusinessonline.co.nz/news/nzs-first-cyber-whitepaper-to-be-released-197780.aspx

Hall, C. (2013). Identify the Real Cost of Cyber Crime to New Zealand. Retrieved from http://blog.netsafe.org.nz/2013/05/16/identifying-the-real-cost-of-cyber-crime-to-new-zealand/

McAfee. (2014). Net Losses: Estimating the Global Cost of cybercrime. Retrieved from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

New Zealand Security Intelligence Service. (2013). Retrieved from http://www.security.govt.nz/assets/media/annual-reports/nzsis-ar13.pdf

Robert, D. & Wolfe, H. B. (2015). Cybercrime Concerns and Readiness for New Zealand Businesses 2014-2015. Retrieved from http://www.citrenz.ac.nz/conferences/2015/pdf/2015CITRENZ_1_Roberts_Cybercrime_v2.pdf

Saini, H., Rao, Y. S. & Panda, T. C. (2012). Cyber-Crimes and their Impact: A Review. *International Journal of Engineering research and Applications (IJERA), 2*(2), 202-209.