SIMPLIFIED COMPUTER INCIDENT RESPONSE MODEL FOR PREMIUM PENSION LIMITED NIGERIA

ABUBAKAR MOHAMMED

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2014

This project report is dedicated to my parents and the entire family for their endless support and encouragement.

ACKNOWLEDGEMENT

In the name of Allah, the most gracious and the most merciful Alhamdulillah, all praises to Allah for the strengths and blessing in completing this project report. I would like to express heartfelt gratitude to my supervisor Dr. Norafida Ithnin for her constant support during my study at UTM. I have learned a lot from her and I am fortunate to have her as my supervisor. Not forgotten, my project examiners Dr. Maheyzah Binti Sirat and Dr. Shokur for their support regarding this project.

My special appreciation goes to my parents and the entire family for their endless support, love, caring and prayers throughout my study. May Allah (S.W.A) continue to bless you my parents. I would like to thank Pension Premium Limited, Nigeria for their support during this project, especially to Mr Imran Hassan.

Finally, I would like to thank all my fellow friends who have helped and supported me throughout my study and who their names are not stated here are also thanked.

ABSTRACT

One of the greatest challenges facing today's IT experts is planning and preparing for the unprepared or unexpected, especially in response to a security incident. An incident is described as any violation of policy, law, or unacceptable act that involves information assets such as computers, networks. In an organization which is activity involved in management or administration work, information and data is the most valuable assets in organization. Therefore, without accurate preparation and sufficient knowledge of information security, those assets will be exposed and destroyed. Premium Pension Limited Nigeria (PPLN) manages much information that is very confidential regarding customers such as government retirement savings account (RSA) salary pensions. That information needs to be accurate and should not be compromised by other parties, unless the authorized access to the information can to do the changes. However, without good care on customer's information, information may not be handled properly and this will lead to loss of valuable data. Moreover, information security management needs to be considered in the organization to avoid anything unwanted situations. An incident response has become an important component of IT security management, because it provides process for discovering and maintaining computer incidents. The proposed incident response model can help the organization to reduce the number of attacks and assist the organization towards securing their data confidentiality, integrity and availability. The proposed model has been validated by PPLN experts through the use of questionnaire and feedbacks were analysed and changes were made. The final result shows that the new model can be used in PPLN.

ABSTRAK

Salah satu cabaran terbesar oleh pakar-pakar IT ialah merancang dan bersedia untuk sesuatu yang tidak diduga atau sesuatu yang tidak dapat diramal terutamanya dalam menangani kejadian keselamatan. Suatu kejadian digambarkan sebagai apa jua pelanggaran polisi, undang-undang atau kelakuan yang melampau yang melibatkan aset informasi seperti komputer dan jalur lebar. Dalam sesebuah organisasi yang terlibat secara aktif dalam pengurusan atau kerja pentadbiran, informasi dan data ialah aset yang paling bernilai dalam organisasi tersebut. Oleh itu, tanpa persediaan yang tepat dan pengetahuan yang cukup berkenaan dengan keselamatan informasi, asset-aset tersebut akan terdedah dan musnah. Premium Pension Limited Nigeria (PPLN) menguruskan banyak informasi yang sangat sulit berkenaan pekerja seperti duit pencen akaun simpanan persaraan (RSA) kerajaan. Informasi tersebut perlu tepat dan tidak boleh didedahkan oleh mana-mana pihak melainkan akses yang diberi terhadap informasi membolehkan membuat perubahan. Walau bagaimanapun, tanpa penjagaan yang rapi terhadap informasi pelanggan, informasi mungkin tidak diuruskan sebaiknya dan ini akan mengakibatkan kehilangan data berharga. Tambahan pula, pengurusan keselamatan informasi perlu diambil kira untuk mengelakkan apa-apa situasi yang tidak diingini. Suatu tindakbalas kejadian telah menjadi komponen penting dalam pengurusan keselamatan IT kerana ia membekalkan suatu proses untuk mengesan dan penyelenggaraan kejadian komputer. Cadangan model tindakbalas kejadian komputer ini boleh membantu orgaisasi untuk mengurangkan bilangan serangan dan menolong organisasi itu ke arah memelihara kesulitan data, integriti data dan kesediaadaan data. Cadangan model tindakbalas kejadian komputer ini telah disemak oleh pakar PPLN menerusi soal selidik dan maklum balas telah dianalisa dan perubahan telah dilakukan. Keputusan akhir menunjukkan model baru boleh digunakan dalam PPLN.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

A	Availability
C	Confidentiality
CSIRTs	Computer Security Incident Response Teams
FBI	Federal Bureau of Investigation
I	Integrity
IRP	Incident Response Process
IRT	Incident Response Team
NIST	National Institute Standard of Technology
PDCA	Plan Do Check Act
PPLN	Premium Pension Limited Nigeria
RSA	Retirement Saving Account
SANS	Small Angle Neutron Scattering

LIST OF APPENDIX

CHAPTER 1

INTRODUCTION

1.1 Overview

The rapid increased of information system technologies, its advanced simplifies our daily lives and make it difficult for interdependent systems to successfully manage information security controls of assets included technology, people, documentation, financial information and so on. Hence, due to its difficulties, these control the lifeline of most of the organizations. Therefore, those assets need to be protected from any kind of attacks and it must be secured enough.

According to Schneier and Anderson (2005), when we hear about information security usually focusing on single events like credit card information, email viruses, website hacking and more of them. The fact is that these are only the tips of the information security. So, to fully appreciate the importance and scope of information security, we need to expand our view significantly on information security and we should think how can we protect our valuable assets and make sure that the information security goals confidentiality, integrity and availability (CIA) are not being compromised or access by unauthorized user.

Most organizations have been connected their systems, and networks to the outside world online. However, this will bring special requirements on computer and information security. Therefore, a lot of organizations have suffered enough from common incidents such as vulnerabilities, threats, viruses, worms, financial fraud, theft of information, and system penetration by outsiders or insiders.

Hence, since not all of these attacks can be prevented, due to that incident response has become an important component of IT security management, because it provides process or steps for discovering and maintaining security incidents. An incident response requires a systematic way and the well-organized method to prevent unprepared, disordered, unplanned and possible damages to an organization (Russell,2010).

The main goal of incident response is to handle the situation in a systematic way so that it will reduce costs, times, and limits damages. An incident response process defines policies and also provides a step by step process that should be accomplished when any incident has occurred in the organization.

Finally, building a computer incident response model in an organization is very important nowadays, because it will help to minimize the impact of the organization and avoid any unwanted situation that may occur.

1.2 Project Background

The PPLN is a licensed pension fund administrator in Nigeria and was established in December 2005. The organization manages a pension fund portfolio of over hundred billions Nigerians Naira. However, it was among the first set of pension fund administrators licensed by PenCom in December 2005 and it started registering employees for the purpose of managing their retirement savings account in February 2006. Therefore, their vision is to be the best pension fund

administration in Nigeria and among the best in the world in terms of security of assets, and services.

The internet usage is growing in most businesses and it is the most important component of the organization for managing daily business operations. Because, they need internet to provide 24 hours online accesses to monitor markets, users' accounts, communicate and collect contributions from staffs, and communicate with their funds protectors. So, due to risks of uncontrolled access when employees in careless or deliberately access sites containing unsuitable, dangerous content or illegal, the organization may loss productivity, and exposed. At the same time they have to make sure that there is no intentional or unintentional misuse of the internet, and network is clean and well protected.

This project will investigate how incidents are attended in PPLN, and how the organization's team uses incident response to support learning and collaboration in cyber protection. Because lack of proper protection of organization information asset will compromise the entire organizational vision and mission. An incident response model ensures that the protection of data confidentiality, integrity, and availability of organizing information is not compromised. The proactive management of information security vulnerabilities, thread and risk refers to information security management. Having valuable information in an organization, there is a need to have an up to date on incident response planning in place. This is because a good incident response plan in place will help to limit the attacks both from inside and outside the company.

1.3 Problem Statement

PPLN is the one of the organizations in Nigeria whereby, the organization is handling, the government retirement savings account (RSA) salary pensions. However, computer and software vulnerabilities, threats are growing and the sophistication of attacks is increasing.

However, due to that, a lot of information was stored in the computer system and as we all know nowadays system is not 100% trust and reliability, because incident can happen at any time without any notification. Therefore, the incident could be a natural disaster, man-made or any kind of incidents. Due to IT infrastructure organization needs to have strong security protection in place to ensure that data is safe and well protected. In this case, information security management needs to be addressed in the organization to avoid anything unwanted situations. Currently PPLN has an incident response plan, but it is incomplete and no documented plan in place and no proper model that will guide them.

So based on the above scenarios this indicates that the PPLN is a very big organization and has many branches nationwide and it is the fact that the incident response plan should be implemented to determine information security controls in the organization. Furthermore, the organization needs to have a comprehensive incident response model that will surely protect their sensitive information and also to make sure that nothing will affect organization assets. Besides, to handle a proper information security, yet incidents response plan must be considered and also to ensure that information security goals C-I-A is not compromised.

1.4 Project Aim

The main aim of this project is to implement an incident response model for PPLN by improving the existing process.

1.5 Project Objectives

The following are the main objectives of this project and the final result would be depending on the objectives as follows:

i. To study various existing incident response model and analyses which process can be best appropriate to the organization.
ii. To propose a computer incident response model for the organization.
iii. To validate the proposed computer incident response model, whether it meets the organization needs.

1.6 Project Scope

The scope of this project focuses on the following:

i. The main scope of this project is to apply information security and incident response process related to all information, data, networks and assets of the organization.
ii. The study will focus on only incidence response model based on the existing processes that were mostly proposed by other researchers.
iii. To design and propose a computer incident response model to PPLN.

1.7 Significant of the Project

This study will provide an in depth analysis into an incident response process in a public-private structure and the protection of critical information infrastructures and how the process supports cyber security by reporting incidents in an appropriate synchronization.

1.8 Project Organization

This project is divided into six chapters. Each and every chapter describes different kinds of information.

The first chapter one elaborated introduction of the project that give an overview of the whole research which contains project background, problem statement, project objectives, project scope and also the significance of the project. This chapter provides deep understanding about the whole idea of the project.

Chapter two, this chapter actually concentrates on reviewing the existing incident response model.

Chapter three highlights the research methodology that is going to be used throughout the research and to ensure the research methodology is merged with objectives.

Chapter four provides detailed design of the model. This section also describes the enhancement being implemented in the model. The initial result which is subject to validation by expects from the area of an incident response team.

This is second to the last chapter five is the validation process goes through an analysis and the result was discussed based on the feedback from experts.

Final chapter six discussed about conclusion and future research of the project, especially the parts that can be improved later on.

1.9 Summary

In summary, this chapter describes the overall understanding of this project such as introduction, problem background, problem statement, objectives, project scope, significance of the project, and summary of chapters. All information contained in this chapter used as input to all chapters.

REFERENCES

Audrey, D., Georgia, K., Robin, R., and Mark, Z. 2004. Defining Incident Management Processes for CSIRTs: A Work in Progress. *U.S.* Christos Scondras. CMU/SEI-2004-TR-015

Avison, D., & Fitzgerald, G. 2003. *Information systems development: methodologies, techniques and tools*. McGraw Hill.

Bishop, M., 2003. Computer Security Art and Science: Boston: Pearson Education, Inc

Castera, Laurent, et al. "FibroScan and FibroTest to assess liver fibrosis in HCV with normal aminotransferases." *Hepatology* 43.2, 2006: 373-374.

Chen, D., & Zhao, H. 2012. Data security and privacy protection issues in cloud computing. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 1, pp. 647-651). IEEE.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. 2012. Computer Security Incident Handling Guide. NIST Special Publication, 800, 61.Chicago

Department of the Navy. *Computer Incident Response Guidebook, Module 19* (NAVSO P-5239-19). <http://www.nswc.navy.mil/ISSEC/Guidance/P5239-19.html> 1996.

Foster, Chloe, Len Bowers, and Henk Nijman. "Aggressive behaviour on acute psychiatric wards: prevalence, severity and management." *Journal of advanced nursing* 58.2 2007.: 140-149.

Gordon, Lawrence A., and Martin P. Loeb. "The economics of information security investment." *ACM Transactions on Information and System Security (TISSEC)* 5.4 2002.: 438-457.

Guanfu, Song, and Zhong Ershun. "Research and Development of Components Geographic Information Systems [J]." *Journal of Image and Graphics* 4 1998.

Hall, S., Ward, R., Cunningham, T., & Marciani, L. 2008. Developing a new curriculum in sport security management. *Journal of Homeland Security and Emergency Management, 5*(1), 1-10. doi: 10.2202/1547-7355.1439

Hillemacher, T., Frieling, H., Hartl, T., Wilhelm, J., Kornhuber, J., & Bleich, S. 2009. Promoter specific methylation of the dopamine transporter gene is altered in alcohol dependence and associated with craving. *Journal of a psychiatric research*, *43*(4), 388-392.

Hong, Grace L. *Sandplay Therapy: Research and Practice*. Routledge, 2010.

Howard, Michael, and Steve Lipner. *The security development lifecycle*. Vol. 11. Microsoft Press, 2009.

Innella, Paul. "National Institute Standard Technology." *SecurityFocus–2001*.

Jaatun, Martin Gilje, et al. "A framework for incident response management in the petroleum industry." International Journal of Critical Infrastructure Protection 2.1 2009: 26-37.

Jacobs, J., & Clemmer, L., & Dalton, M., & Rogers, R., & Posluns, J 2003. SSCP: Systems Security Certification Practitioner: Rockland: Syngress Publishing, Inc.

Jäntti, M., 2011. Improving Incident Management Processes in Two IT Service Provider Companies.

Jeong, K. et al., 2008. A Security Coordination Model for an Inter-Organizational v Information Incidents Response Supporting Forensic Process. 2008 Fourth International Conference on Networked Computing and Advanced Information Management, pp.143-148. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4624132 [Accessed October 8, 2013].

Karnouskos, S., 2010. Stuxnet Worm Impact on Industrial Cyber-Physical System Security.

Kazemi, M., Khajouei, H. & Nasrabadi, H., 2012. Evaluation of information security management system success factors : Case study of Municipal organization. , 6(14), pp.4982-4989.

Kent, K., Chevalier, S., Grance, T., & Dang, H. 2006. Guide to integrating forensic techniques into incident response. *NIST Special Publication*, 800-86.

Khurana, H. et al., 2009. Palantir : A Framework for Collaborative Incident Response and Investigation.

Kjaerland, M., 2006. A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers & Security, 25(7), pp.522-538. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404806001234 [Accessed November 12, 2013].

Kobayashi, H. et al., Development of Information Security-Focused Incident Prevention Measures for Critical Information Infrastructure in Japan. , pp.22-33. Kvale, S., Publications,S. & California, T.O., 1996. Interviews : An Introduction to Qualitative Research Interviewing.

Kotulic, Andrew G., and Jan Guynes Clark. "Why there aren't more information security research studies." *Information & Management* 41.5 (2004): 597-607.

Kruse II, W. G., & Heiser, J. G. 2001. *Computer forensics: incident response essentials*. Pearson Education.

Kruse, Warren G., II & Heiser, Jay G. *Computer Forensics, Incident Response Essentials*. Reading, MA: Addison-Wesley, 2002.

Liu, P., Yu, H. & Miao, Q., 2010. Automated Planning for Incident Response Based on CBR.

Mandia, Kevin, Chris Prosise, and Matt Pepe. "Incident response and computer forensics." *McGrawHi1l Osborne Media* 2003.

McClure, S., & Shah, Saumil & Shah, Shreeraj 2003. Web Hacking : Attacks and Defense. Boston: Pearson Education, Inc

Michael, E. 2003. *Disaster Recovery*. (1st ed.) United States.: Cengage Learning. (pp. 190 –202).

Mitsonis, C. H., Kararizou, E., Dimopoulos, N., Triantafyllou, N., Kapaki, E., Mitropoulos, P., ... & Vassilopoulos, D. 2008. Incidence and clinical presentation of neurosyphilis: a retrospective study of 81 cases. International Journal of Neuroscience, 118(9), 1251-1257. Chicago

Modiri, Nasser, and Yosef Masoudi Sobhanzadeh. "Information security management." *Computational Intelligence and Communication Networks (CICN), 2011 International Conference on*. IEEE, 2011.

Mohr, L. B. 1969. Determinants of Innovation in Organizations. The American *Political Science Review, 63*(1), 111-126.

Richardson, Robert. "CSI computer crime and security survey." *Computer Security Institute* 1 2008: 1-30.

Russell, C. L. 2010. A clinical nurse specialist-led intervention to enhance medication adherence using the plan-do-check-act cycle for continuous self-improvement. *Clinical Nurse Specialist*, *24*(2), 69-75.

Saint-Germain, Rene. "Information security management best practice based on ISO/IEC 17799." *Information Management Journal* 39.4 2005: 60-66.

Scheel, W. C., Blatcher, W. J., Kirschner, G. S., & DENMAN, J. J. 2002. Is the efficient frontier efficient?. In *Casualty Actuarial Society* (p. 236).

Schneier, B., & Anderson, R. 2005. Guest Editors Introduction: Economics of Information Security. IEEE Security & Privacy, 3(1), 0012-13. Chicago

Schultz, Eugene & Shumway, Russell. Incident Response: A StrategicGuide to Handling System and Network Security Breaches. Indianapolis,IN: New Riders Publishing, 2011.

Shedden, P., Ahmad, A., & Ruighaver, A. B. 2010. Organisational learning andq incident response: promoting effective learning through the incident response process. Chicago

Silberschatz, Abraham, Peter B. Galvin, and Greg Gagne. *Operating system concepts*. Vol. 8. Wiley, 2013.

The SANS Institute. *Computer Security Incident Handling Step-by- Step*. The SANS Institute, October, 2012.

Veiga, A. D., & Eloff, J. H. 2007. An information security governance framework. Information Systems Management, 24(4), 361-372. Chicago

Whitman, M., & Mattord, H. 2011. *Principles of information security*. Cengage Learning.

Whitman, Michael E., and Herbert J. Mattord. "Designing and teaching information security curriculum." *Proceedings of the 1st annual conference on Information security curriculum development*. ACM, 2004.

Yu, H., Powell, N., Stembridge, D., & Yuan, X. 2012. Cloud computing and security challenges. In *Proceedings of the 50th Annual Southeast Regional Conference* (pp. 298-302). ACM.

Zou, Y., Shi, G., Shi, H., & Zhao, H. 2011. Traffic incident classification at intersections based on image sequences by HMM/SVM classifiers. *Multimedia Tools and Applications*, *52*(1), 133-145.

Denis, A, Wixom, B & Roth, R 2006, *Systems analysis design*, third edition, Wiley & Sons Inc, Hobeken.