FRAMEWORK FOR INCIDENT RESPONSE PROCESS IN NIGERIAN POSTAL SERVICE

ALIYU MOHAMMED ABALI

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

JANUARY 2013

This work is dedicated to my Parents for their endless support, May the blessings of Allah continue to shower on them both here and the hereafter.

ACKNOWLEDGEMENT

All praises is due to Allah, the Creator. I am profoundly thankful to my supervisor Dr. Norafida Ithnin for her kindly support and guidance all these years of my study at UTM, she has taught me and improve my research skills. I also want to cease this opportunity to extend my appreciation to Dr Anazida Zainal for her support and patience in dealing with us and all academic and non academic staff in faculty of computing and the entire UTM at large.

My profound gratitude goes to my parents and the entire family for their moral and financial support.

To my friends both here in Malaysia, especially my class members and colleagues in federal Polytechnic Mubi Nigeria, words cannot express my appreciation; you are too generous to me.

Finally, my appreciation goes to Dr. Ahmad Halilu Abba and all people who their names are not mentioned here. Thank you all.

ABSTRACT

As the dependant of organizations to Information Technology increases and government agencies reliance on private organizations to protect critical information infrastructure, National government in some quarters began not to merely outsource services from the private but to equally provide protection to information resources. Nigerian postal service (NIPOST) is a large government agency responsible for postal services in the country, following the government recommendations NIPOST partners with a number of private sector organizations to provide services to its customers. Incident response is a key aspect of information security and it is not well attended in most organizations, The focus of this study is to investigate the computer security incident response process in NIPOST, shared responsibility and coordinated incident response capability and how NIPOST utilizes the incident response teams to support its information security learning and a general support for cybersecurity protection. The project is a case study based with interviews, documentation and questionnaire as the key to improve NIPOST incident response process and any similar organisation to provide a knowledge feedback to the agency and the cybersecurity community at large through a collaborative workspace. A detail investigation was conducted in the second phase of the research, the investigation revealed that the organization incident response does not support learning from the past incident and there was no any collaboration with outside teams. The proposed enhanced framework supports incident learning and coordination between teams at all levels and this improves organizational learning and coordination, which finally improve cyber security. To validate the proposed enhanced framework, expert's feedback through a questionnaire were analysed with modification of the initial result. This result can be improved to build a framework for national computer security incident response framework.

ABSTRAK

Disebabkan kebergantungan organisasi kepada Teknologi Maklumat (IT) meningkat dan agensi-agensi kerajaan pula bergantung kepada pemeliharaan infrastruktur maklumat yang kritikal, kerajaan Nasional dalam sesetengah pihak tidak sewenang-wenangnya memonopoli perkhidmatan daripada sektor swastatetapi utuk bersama-sama memberi perlindungan kepada sumber maklumat. Perkhidmatan Pos Nigeria (NIPOST) adalah sebuah agensi kerajaan yang besar yang bertanggungjawab menyediakan perkhidmatan pos kepada di negara ini, berikitan daripada cadangan kerajaan untuk NIPOST untuk membuat rakan kongsi dengan sektor swasta untuk menyediakan perkhidmatan kepada pelanggan-pelanggannya. Tindakbalas insiden merupakan aspek utama keselamatan maklumat namun ia tidak diambil berat oleh kebanyakan organisasi. Fokus kajian ini adalah untuk menyiasat insiden keselamatan komputer tindakbalas dalam proses NIPOST, tanggungjawab bersama dan keupayaan tindakbalas insiden diselaraskan dan bagaimana NIPOST menggunakan respon insiden pasukan untuk menyokong pembelajaran keselamatan maklumat dan sokongan umum untuk perlindungan keselamatan di alam siber. Projek ini adalah satu kajian kes berdasarkan dengan temubual, soal selidik dan dokumentasi sebagai kunci untuk memperbaiki sistem tindakbalas insiden NIPOST dan mana-mana organisasi yang bekerjasama untuk memberikan maklum balas pengetahuan kepada agensi dan komuniti keselamatan di alam siber yang besar. Satu siasatan terperinci telah dijalankan pada fasa kedua penyelidikan dan hadil siasatan mendapati bahawa sambutan organisasi tersebut tidak menyokong pembelajaran daripada insiden yang telah berlalu dan tidak wujud kerjasama organisasi dengan mana-mana pihak luar. Rangka kerja yang telah dipertingkatkan dan dicadangkan adalah untuk menyokong pembelajaran insiden dan koordinasi di antara pasukan pada semua peringkat dan ini akan meningkatkan pembelajaran dan penyelarasan dalam organisasi yang akhirnya akan meningkatkan keselamatan siber. Untuk mengesahkan rangka kerja yang dipertingkatkan seperti yang dicadangkan, maklum balas daripada pakar soal selidik dianalisis dengan pengubahsuaian hasil awal. Keputusan ini boleh diperbaiki dengan membina satu rangka kerja bagi keselamatan tindakbalas kejadian komputer antarabangsa.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Information systems technologies advance rapidly, simplifies our daily lives and make it difficult for interdependent systems to successfully manage information security controls (People, Technology and Organization) due to its complexities, these controls are the lifeline of many organizations, therefore it must be managed proactively to secure organization's information resource. Compromise to information will lead to lose of the overall organization's resources, manpower and reputaton. "Information security" is to protect information, to ensure that the information security goals (confidentiality, integrity and availability) are not compromised. The Internet is being the network that links the entire planet so responding to security incidents often requires the coordination of organisations, government intervention and international coordination efforts. The Computer Emergency Response Team/ Coordination Center (CERT/CC) at Carnegie Melon University has set the first milestone by providing a central location for the reporting and evaluation of such incidents as well as for providing the appropriate solutions (Mitropoulos *et al*, 2006). "information security management" is a management of information security risks, threats and vulnerabilities (Kritzinger and Smith, 2008).

Incident response (IR) is a managerial function for planning and establishing a framework for computer security incidents to structurally detect and resolve incidents to minimize the impact to the organisation's resources and return back to a normal operation, it is an ability of an organisation to react to suspicious and unacceptable actions targeting a computer or network infrastructure in a timely approach. Incident response (IR) requires a systematic and well organised approach to prevent unprepared, chaotic and possibly a devastating incident (Freiling, 2007). Computer incident response team is responsible for organising and conducting a responses to a computer related abuses. The team comprise of experts of different background not only within the field of information security but may include experts from other field who may not actively take part in the operation but contribute a lot to the success of the operation to guarantee computer security incident response capabilities (CSIRC). Computer security incident is complex, it includes but not limited to denial of service (DoS), organisations relies on the responsible team to resolve incident which might be critical to its existence.

Interdependent systems exists alongside with each other and internet of a thing is a channel that facilitates transfer of information from different entities, the network is not reliable and it is no longer a matter of deploying security that lock up a domain to prevent unwanted guest into the network, today security incident can emanates from within a domain and create devastating disaster to the organisation. Information security is extremely difficult especially to a socio-technical organisation where technology, organisation people exist. The challenge of building information security incident response includes both formal and informal controls that can build around technical controls to ensure security of information.

Finally building incident response in a government owned enterprise where service delivery models relied on outsourced private enterprise systems will foster both national and international incident response management and cooperation on cyber security respectively. Local and international collaboration with peer enterprise can enhance the current state of information security community at all levels.

1.2 Problem Background

Critical hardware and software systems that control critical information are owned by both public and private enterprise in a so called Public-private partnership model, information flows from a public system to private system, and to users as well, and these dependancies is critical to the Services rendered by cooperation between the public and the private. Information travels along unsecured network and computer security incidents are evolving and this necesiatiate the need to respond against the Incident that occurs on the organisational system and to jointly respond to global trends of cybercrime.

Different frameworks exists for incident response, this include framework for critical infrastructure of process oriented systems that supports proactive incident response (Jaatun *et al*, 2009), Palantir system constitutes both technological and conceptual incident response and it is first to implement multi site incident response (Khurana *et al*, 2009), others are internationally adopted best practices like NIST and SANS. However there is no complete standard of incident response, either as a dedicated document or an enterprise wide information security standard (Mitropoulos *et al*, 2006) and incidents can happen in different dimensions based the organisational culture and environment especially the organisational models of Public-Private. It is difficult to have a timely incident response framework without considering the organisational information flow and interdependencies these would not only provide a trust mechanism but also provide a Sharing formula for an incident response. Customers rely on public for the services but most of these services emanates from private systems, sometimes the customers experience a downtime which shows that the link is not always available, there must be likelihood for an attack to occur, and therefore how this attack can be mitigated without knowing the responsibilities attached to various entities. Based on the above scenario, the project will investigate how incidents are attended in Nigerian postal service and how the agency uses its incident response team to support learning and collaboration in cyber protection.

The international efforts in fighting against cybercrime, typically, the International Telecommunication Union (ITU) - Global Cyber-security Agenda (GCA) in handling threats and vulnerabilities at global stage and cooperation between all member states is one of the efforts demonstrated at international height. All these efforts cannot yield positive result except it is been checked at organisational level. Developing a framework for incident response will have impact on the other federal agencies to follow the suite, these will effectively enhance the reporting capabilities to cybersecurity communities and provides a basis for an indebt analysis of threats and inputs the knowledge back for unexpected event in the future, eventually this would reduce the number of incidents in the cyberspace. The responsibility to fight against cybercrime rests on the customers, Public and private entities and a responsibility for all.

The level of authority, roles and responsibilities defined in organisational structure should includes the authority of incident response team, this was identified by (Cichonski et al, 2012) to includes monitoring of suspicious activity, reporting certain types of incidents and general guidelines of what can be shared with whom, when and over what medium of communication, dividing incident response responsibilities and restricting access to certain information that are regarded as not only confidential but sensitive to outsiders especially in an event of attack. Users including implementation manergers, customers and other internal employees relies on services provided by public systems and success of service delivery depend the private systems. Attacks are imminent, users reports the obscurity to internal response team, incidents are either resolved internally or escalate to the private partners. However, a collaborative framework of shared responsibilities with the partners who provide immediate services and other third party organisations is a very good indication for success in addressing issues of public-private interdependent systems and future network of the cloud computing (Yamaguchi, 2011).

1.3 Problem Statement

It is difficult to manage incidents in an organisations that are independent of one another which may outsource only internet connection from internet service providers (ISP), on the other hand government agencies in most part of the world through a public-private model come together with private sector organisation and outsource most of its services including those agencies that operates critical national infrastructures, failure of critical systems may lead to a failure of the entire country, survival of a nation is crucial to critical national information infrastructure (Zahri and Syahrul, 2010), consequently it is difficult to manage incident in such a model of interdependency. Additionally, an explosive growth of cyber attack has a great impact on organization critical information systems because attack can come from any part of the world and the interaction of people and technology in an organization (Cusick and Ma, 2010) made it more difficult to determine the security requirement of incident response. Computer security incident response team is usually notified when an incident happen in a particular organization, the team is expected to respond in a timely and proactive mode. In such case, even though the model of PPP defines the Response Team (RT) it is difficult to determine roles and responsibilities and establish trust between entities involved, all these are eminent to the protection of organisation's sensitive information. A large number of incident response processes have been proposed and they are varied according to the size, structure, mission and type of the organization. (Naseri and Azmoon, 2012) in this context, we can understand that computer security incident response is difficult to establish because of different requirement by different domain like government, commercial, military, research and development centres.

Therefore different structures are proposed for computer security incident response based on the organizational missions, goals requirement and services with coordination at national level. Additionally, it is important to highlights the need for regional and global coordination and incident learning.

In any organizational set up both private and public always do not like to share some information with their outsourcer or service provider therefore without a standard measure of who own what and at what level can both have access to devices during, before and after incident will make it difficult to investigate and re-evaluates incidents. Nigerian Postal Service have about 5,000 post offices nationwide with a number of business ventures apart from percel services,which includes, E-registration and NIPOST PostCash. Information system technologies used to support these services are outsourced from the private sector organisation.

1.4 Research Questions

(i) How team of incident response is organised in public-private to support the protection of critical information infrastructure.

(ii) What is a suitable incident response process framework for public-private interdependent Systems in a particular organization's culture and environment?

(iii) How incident response is coordinated to support incident learning and reporting to improve cybersecurity.

1.5 Objective of the study

The following are the main objective of the project and the final outcome would depend on the objectives.

(i) Study various existing incident response processes and analyse which process can be best suited to the requirement of the case study.

(ii) To propose a framework by enhancing incident response process models.

(iii) To evaluate the proposed enhanced framework with the selected incident response process.

1.6 Scope of the project

Generally, the current research on information security management addresses two broad areas of technical and non-technical information security management; however this project will address the non technical part of information security. Thus, the scope of the project focuses on the following;

(i) The study will only consider an incident response planning and the effects of private partners on critical information infrastructure protection of a government agency.

(ii) The study will consider computer security incident in a public organization and coordination with outside teams.

(iii) Only the incidence response process will be considered in the design of new framework.

1.7 Significance of the Project

The threats to global information network is quite alarming and many organizations rely on information technology to support and share information within and outside their domains. The complexities and integration of poorly standard systems and technology makes it very difficult to manage information securely and this gave chance to sophisticated attackers to continually launch attack, this makes organizations to begin responding to incidents as they occur (Cichonski, 2012). Organisations at various levels began to accept and implement computer security incident response. However some organizations not only outsource the IT services but also rely on each other organisation for systems implementations, this makes it difficult to define level of responsibilities and trust between the organisations especially in a public-private domain in which both agreed on a clear terms to work for the benefit of one another and to support critical infrastructure systems.

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

1.8 Organization of the Project

This project contains six chapters, this is the first chapter and it introduces the project work, problem background, research questions and objective of the project. Chapter two, the next chapter which covers the literature review. Chapter three states the methodology used to achieve the objectives of the project. Chapter four provides the initial result which is subject to validation by experts from the case study organisation and in the field of incident response community. Chapter five describes the expert feedback and analysis of the result. The last chapter, chapter six concludes the project by stating the achievements and future direction of the project in terms of areas that can be improved.

REFERENCES

Ahmad, A., Hadgkiss, J. & Ruighaver, A.B., 2012. AC SC. *Computers & Security*. Available at: http://dx.doi.org/10.1016/j.cose.2012.04.001.

Alberts, C., 2004. Management Processes for CSIRTs : A Work in Progress. , (October).

Anderson, A.K., 2005. Intelligence-based Threat Assessments for Information Networks and Infrastructures.

Anuar, N.B. et al., 2010. An investigation and survey of response options for Intrusion Response Systems (IRSs).

Avina, J., 2011. Public-private partnerships in the fight against crime: An emerging frontier in corporate social responsibility. *Journal of Financial Crime*, 18(3), pp.282-291. Available at: http://www.emeraldinsight.com/10.1108/13590791111147505 [Accessed May 8, 2012].

Baldwin, A. et al., 2006. A model-based approach to trust, security and assurance. , 24(4).

Bartolini, C., Stefanelli, C. & Tortonesi, M., 2010. SYMIAN : Analysis and Performance Improvement of the IT Incident Management Process. , 7(3), pp.132-144.

Bryman, A., 2012. Journal of Mixed Methods Research.

Chang, K.-chung & Wang, C.-ping, 2010. Information systems resources and information security. *Information Systems Frontiers*, 13(4), pp.579-593. Available at: http://www.springerlink.com/index/10.1007/s10796-010-9232-6 [Accessed March 24, 2012].

Cichonski, P. & Scarfone, K., Computer Security Incident Handling Guide (Draft) Recommendations of the National Institute of Standards and Technology. , 2.

Cook, D.M., 2010. Mitigating Cyber-Threats Through Public-Private Partnerships : Low Cost Governance with High- Impact Returns.

Cormack, A., JANET Guidance Notes Effective Incident Response. , 009.

Cusick, J.J. & Ma, G., 2010. Creating an ITIL Inspired Incident Management Approach : Roots , Response , and Results. , pp.142-148.

Daley, R. et al., 2011. Operationalizing the Coordinated Incident Handling Model. , pp.287-294.

Egan, M.J., 2010. Private goods and services contracts: Increased emergency response capacity or increased vulnerability? *International Journal of Production Economics*, 126(1), pp.46-56. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0925527309003636 [Accessed April 11, 2012].

El-Gayar, O.F. & Fritz, B.D., 2010. A web-based multi-perspective decision support system for information security planning. *Decision Support Systems*, 50(1), pp.43-54. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167923610001077 [Accessed April 20, 2012].

Eusgeld, I., Nan, C. & Dietz, S., 2011. “System-of-systems” approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*, 96(6), pp.679-686. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0951832010002668 [Accessed March 26, 2012].

Farahmand, F. et al., Assessing Damages of Information Security Incidents and Selecting Control Measures , a Case Study Approach. , pp.1-11.

Ghernaouti-Hélie, S., 2009. An Inclusive Information Society Needs a Global Approach of Information Security. *2009 International Conference on Availability, Reliability and Security*, pp.658-662. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5066543 [Accessed March 5, 2012].

Goeken, M. & Alter, S., 2009. Towards Conceptual Metamodeling of IT Governance Frameworks Approach - Use – Benefits. , (Cmmi), pp.1-10.

Gunter, P. & Philip, H., 2003. Managing Vulnerabilities of Information Systems to Security Incidents. , pp.348-354.

Hunton, P. & Police, C., 2011. The stages of cybercrime investigations : Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review*, 27(1), pp.61-67. Available at: http://dx.doi.org/10.1016/j.clsr.2010.11.001.

Jaatun, M.G. et al., 2009. A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, 2(1-2), pp.26-37. Available at: http://dx.doi.org/10.1016/j.ijcip.2009.02.004.

Jeong, K. et al., 2008. A Security Coordination Model for an Inter-Organizational 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 May 8, 2012].

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

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.

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 March 12, 2012].

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.

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

Metzger, S., Hommel, W. & Reiser, H., 2011. Integrated Security Incident Management -- Concepts and Real-World Experiences. *2011 Sixth International Conference on IT Security Incident Management and IT Forensics*, pp.107-121. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5931116 [Accessed April 21, 2012].

Milicevic, D. & Goeken, M., Application of Models in Information Security Management.

Milicevic, D. & Goeken, M., 2010. Ontology-Based Evaluation of ISO 27001. , pp.93-102.

Modiri, N. & Sobhanzadeh, Y.M., 2011. Information Security Management. *2011 International Conference on Computational Intelligence and Communication Networks*, pp.481-484. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6112913 [Accessed May 8, 2012].

Muhren, W., Eede, G.V.D. & Walle, B.V.D., ORGANIZATIONAL LEARNING FOR THE INCIDENT MANAGEMENT PROCESS : LESSONS FROM HIGH RELIABILITY ORGANIZATIONS. , pp.576-587.

Naseri, A. & Azmoon, O., 2012. Proposition of Model for CSIRT : Case Study of Telecommunication Company in a Province of Iran. , 9(1), pp.156-160.

Networks, C. et al., "Collective C2 in Multinational Civil-Military Operations" Title of Paper Coordinated Cybersecurity Incident Handling Name of Author (s) Point of Contact. , (240).

Nowey, T., 2007. Collection of Quantitative Data on Security Incidents.

Ogedebe, P.M. & Jacob, B.P., 2012. THE ROLE OF INFORMATION TECHNOLOGY IN COMBATING. , 2(1), pp.124-130.

Olav, F., Torres, J.M. & Sarriegi, Jose M, 2009. Blind information security strategy. *International Journal of Critical Infrastructure Protection*, 2(3), pp.95-109. Available at: http://dx.doi.org/10.1016/j.ijcip.2009.07.003.

Osorno, M. et al. 2011, Point of Contact Coordinated Cybersecurity Incident Handling Roles , Processes , and Coordination Networks for Crosscutting Incidents. , (240).

Pereira, R. & Mira, M., 2011. 2011 15th IEEE International Enterprise Distributed Object Computing Conference Workshops A Maturity Model for Implementing ITIL V3 in Practice.

Port, D., Kazman, R. & Takenaka, A., 2008. Strategic Planning for Information Security and Assurance. *2008 International Conference on Information Security and Assurance (isa 2008)*, pp.466-471. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4511612 [Accessed April 15, 2012].

Prautzsch, F. et al., 2011. Commercial SATCOM in support of protected connectivity for the Warfighter and First Responder. , pp.2296-2301.

Qingguo, L. & Wei, Z., 2009. Strengthen Military Academy's Information Security Management. *2009 International Conference on Multimedia Information Networking and Security*, pp.182-186. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5368495 [Accessed March 5, 2012].

Refahi, A. et al., 2011. A CBR-based Approach to ITIL-based Service Desk. , 2(10), pp.476-484.

Ross, B.S.J., 2008. Enforcing information security : architecture. , (February).

Salomon, J.M. et al., Computer security incident response grows up. , pp.5-7.

Shedden, P. & Ahmad, A., 2011. Informal Learning in Security Incident Response Teams.Singh, B., 2010. Security Policy :

Sveen, F.O., Sarriegi, Jose Mari & Gonzalez, J.J., 2009. Incident Response and User Awareness. , pp.161-172.

Taylor-powell, E. & Steele, S., Collecting Evaluation Data : Direct Observation.

Thomson, K.-lynn, Solms, R.V. & Louw, L., 2006. Cultivating an organizational information security culture. , (October), pp.49-50.

Wack, J.P., 1991. Establishing a Computer Security Incident Response Capability (CSIRC) NIST Special Publication 800-3.

Wang, C.-hsiang, 2009. Integrated Installing ISO 9000 and ISO 27000 Management Systems on an Organization. , pp.265-267.

Wood, C.C., 1988. A Context for Information Systems Security Planning. , 7, pp.455-465.

Xuemei, L., Yan, L. & Lixing, D., 2009. Study on Information Security of Industry Management. *2009 Asia-Pacific Conference on Information Processing*, pp.522-524. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5197108 [Accessed May 8, 2012].

Yamaguchi, S., 2011. New Era for Management to Deal with Scalability, Invisibility and Shared Responsibility. *2011 IEEE/IPSJ International Symposium on Applications and the Internet*, pp.352-352. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6004184 [Accessed May 8, 2012].

Yang, Z., Research on The Key Techniques of Wireless Communication for Emergency Information System. , pp.432-435.

Yuan, S. & Wang, W., 2010. A Campus Network Security Emergency Response Technical System Based on Emergency Log. , pp.3-5.

Zili, Z., Xi, G. & Jinming, C., 2009. Research on Architecture and Key Technology of Information Security Emergency Response. , pp.1-4.

Zivic, P., 2011. Structuring Incident Types to Streamline Incident Response. *2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks,* pp.456-462. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6117465 [Accessed May 8, 2012].

G. B. White, E. A. Fisch, and U. W. Pooch, "Cooperating security managers: A peer based intrusion detection system," *IEEE Network*, vol. 10, pp. 20-23, 1996.

Patton, M. Q. (1987). How to use qualitative methods in evaluation. Newbury Park, CA: Sage, printer publication, New York, 10010.

Kvale, Steinar. Interviews An Introduction to Qualitative Research Interviewing, Sage Publications, 1996