International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

A Framework for Optimizing the Computer Security Incident Business Continuity Plan

Nnebe S. E. [1], Iyafokhai I. U [2], Sadiq. M. N.[3]
[1,2] Department of Computer Science,
Ambrose Alli University,
Ekpoma

***Abstract*:- As information technology systems evolve, they also need to be protected against today's considerable amount of threats to the information they process, transmit and store. So any failure or disaster in information technology system could have a serious consequences for a company (Botha and Solms, 2004). As a result of dependency on technology, majority of these companies on these systems, cannot afford to ignore the need for business continuity and disaster recovery planning regardless of the company's size, revenues, or number of staff. The need to plan for potential disruptions to technology services had increased exponentially and business continuity and disaster recovery planning has become imperative (Snedaker, 2007). Growing dependence upon computer information systems has created vulnerabilities that have not been uniformly addressed. Then computer security incident management plan is required to tackle issues that lead to system failure. In this paper, a framework is established to secure the network of a company from unknown attack, detect and monitor events that may lead to business disruption, as well as respond to plan so that business operations can continue within a shortest possible instant. By implementing this framework therefore, the effectiveness of various business continuity and disaster recovery practices will be explored to increase information systems resiliency.**

Keywords: Information System, Business Continuity, security incident, and incident recovery plan.

1. INTRODUCTION

Information systems are complex and vital to modern infrastructure. Loss of computer information system availability can financially cripple companies and potentially cause basic necessities such as clean water to be unavailable. In many cases, organizations fail to implement business continuity measures due to the high cost of remote failover systems and training. According to the recommendations of the U.S. National Institute of Standards and Technology, an incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

The Information Technology (IT) industry has advanced rapidly over the years, so that it now forms a vital component for conducting business (Botha and Solms, 2004). Nowadays, individuals and corporations have become increasingly reliant upon information technology to the extent that it is difficult to find a corner of a company that IT does not touch. Majority of these organizations cannot operate without computer systems (Barbara, 2006).

Aside from IT professionals, very few organizations think about the impacts of information system failure. The illusion is that there is nothing new about information system security since they are already used to some threats which occur at any point in time, for instance the malware, spyware, virus and other advanced persistent threats. But these threats can come in different forms to disrupt or interrupt business continuity, thereby making a financial institution to lose performance in operation. Hence, a response to a information system security incident should be planned properly in advance. Of course, no plan can handle every contingency. However, a general plan can be developed to handle the majority of incidents.

As computer information systems continues to become more integral to corporate operations at every level of the organization, the job of information technology has expanded to become almost all-encompassing. As businesses increasingly rely on data, information and technology, new threats are constantly emerging that affect all corporations. Many companies have experienced or witnessed the devastation that occurs when an information technology disaster strikes (Barbara, 2006).

Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented since new types of security-related incidents always emerge. The recent Global State of Information Security Survey 2016 shows that the number of security incidents has increased in the recent years and that most of the interviewed companies follow a risk-based cybersecurity framework managed by an external firm.

In particular, the survey claims a general increase in the number of computer security incidents being reported. This is directly translated into an increased awareness by organizations of the need for security policies and practices as part of their overall risk-management strategies.

Cyber infrastructure resiliency is dependent upon creating practical, attainable implementations. Computer security incident management response plan is an iterative process designed to secure company critical applications and endorse policies, procedures, processes and plans to ensure the continuation of these functions in the event of an attack

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

or disaster. Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur.

Consequently, the IT unit of companies which is usually responsible for the management of information systems needs to deal with security compliance, data confidentiality, access management, protection of the network from vulnerabilities or attacks and much more. To meet these requirements, this unit establishes a Computer Security Incident Response Team, which handles or manages the company's networks thus preventing them from being compromised.

2. LITERATURE REVIEW

To understand the concept of computer security incident management plan, it is important to consider business continuity management/plans and their importance in the financial institution, which also involves one to have an appreciation of the dynamics and factors that led to the development and promotion of the concept. Every organization is faced with a variety of threats and vulnerabilities and these continue to evolve. Business continuity has been defined by some notable researchers.
British Standards, 2008a defined it as "a pro-active process which identifies the key functions of an organization and the likely threats to those functions". Wikipedia, 2008b defined it as "a progression of disaster recovery, aimed at allowing an organization to continue functioning after (and ideally, during) a disaster, rather than simply being able to recovery after a disaster".
NFPA 1600, 2007 defined it as "an ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies, recovery plans, and continuity of services".

In a study of companies that experienced a major data loss without having solid Business Continuity/Disaster Recovery plan in place, 43% never reopen, 51% closes within two years, and only 6% survives long-term (Cummings *et al*, 2005).
In August 2002, the American Management Association released a study indicating that more than half of the surveyed companies had no disaster recovery or crisis management plan in place. Another report from Gartner, Inc. in 2002, indicated that less than 10% of small and medium businesses had disaster plans, and that 40% of companies that experience a disaster without a disaster recovery plan goes out of business within five years.

Organizations have been exploring numerous solutions for implementing security incident response. As a result, several incident response approaches and best practice guidelines have been published in both industry (British Standards Institution 2011; Cichonski et al. 2012; European Network and Information Security Agency 2010) and academia. Many of these approaches are based on a linear plan-driven model. Within these models, preparation for incident handling leads to incident detection and containment.

In turn, a security incident response team can eradicate and recover from the incident and provide feedback into the wider organizational security posture. However, researchers have noted that there is a lack of consensus as to the standardization of security incident response (Alberts et al. 2004). As a result, there is currently no single de-facto approach which can truly be classified as an industry standard for handling security incidents.

Werlinger, et al. (2007) conducted an exploratory study to investigate the security incident activities of practitioners in various organizations. The objective of the study was to determine what skills, tools and strategies were required to manage and handle security incidents. The results showed that practitioners often used pattern recognition and hypothesis generation during the analysis of security incidents.
In a separate study, Werlinger, et al. (2010) added that current security incident response tools do not appropriately support the highly collaborative nature of incident investigations and that incident handlers often need to develop their own tools to perform specific tasks.

Ahmad, et al (2012) argued that the work of a Security Incident Response Team is usually completed by the issuance of a report, detailing the investigation findings and any lessons learned along with the distribution of information internally or externally. Time is a critical factor in security incident investigations (Ahmad et al. 2012). The ability to swiftly respond and investigate why a security incident has occurred can reduce system downtime, subsequent financial losses, as well lowering the cost of returning the organization to its normal security posture (Killcrece et al. 2003).

Information security incidents are unwanted occurrences, yet at the same time they present an opportunity to learn about the risks and vulnerabilities which can exist in both technical and socio-technical systems (Line et al. 2009). Any lessons learned from security incidents and security incident handling processes can then be used by an organization to improve its wider information security posture. However, researchers have argued that organizations do not pay enough attention to incident learning (Ahmad et al. 2012; Shedden et al. 2011). These researchers go on to claim that organizations are more concerned with eradication and recovery (Ahmad et al. 2012; Shedden et al. 2011).

Hove, et al (2014) studied three large organizations in an attempt to investigate the plans and procedures for handling security incidents within the studied organizations. The results from the study showed that although the organizations have plans and procedures in place, based on industry best practices, many procedures were missing from the organizational structure. The authors identified two organizations in which security incident reporting procedures were not established, while

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

the respondents in another organization indicated that staff deficiencies impeded efficient response to incidents (Hove et al. 2014).

Line, et al (2014) examined how distribution service operators within the power industry planned and prepared for security incidents. The findings showed that many of the surveyed organizations had little or no documentation regarding the investigation of security incidents. Furthermore, Line, et al (2014) reported that the majority of their studied organizations did not have a clear definition for a security incident. This is a finding that is shared by Tan, et al (2003), who had also reported that the organization in their case study did not have a clear definition for a security incident.

Identifying security event/incident sequences at the start of the lifecycle, allows an incident response team to increase the amount of data potentially being captured, therefore enhancing the technical excellence of incident learning (Grispos et al. 2014). Security incident investigations can provide information that can be instrumental in avoiding a recurrence of the incident. A security incident response process should, therefore, include provisions for an incident response team to access richer information to perform a more complete investigation.

From the views above, this concept of computer security incident management response plan has become widely accepted and implemented as such requires a system which optimizes the incident discovery, response and recovery in cases of unexpected disasters or attacks. Hence, this research paper provides an architectural framework which when deployed optimizes computer security incident management response plan, and ensures that all response teams can easily be contacted through a link for effective security event monitoring and incidents investigations.

3. METHODOLOGY

This research paper proposes a system framework for the optimization of computer security incident management plan that enables the IT staff, top management staff and incident management response team to communicate easily through a link. The architectural framework also provides process overview that defines how management can control an incident, and the stages were incident occurrence can be tackled and managed for business operation to continue effectively. Because an organization needs to detect, manage and avert incidents detrimental to software aspect of a business operation and continuity, our proposed architectural framework is derived from two separate perspectives-the incident discovery phase and the response to incident phase for easier optimization of the continuity plan.

3.1 The proposed system Architectural framework

Figures 1, 2 and 3 depict the security incident management process that gives a formal description and representation of a system. It shows the various phases of incident system development from event trigger to incident response. To generate our proposed architectural framework we conceptualized two phases of security incident management process (incident discovery and response phases) and generated two separate architectures which could work as integral units and modeled to yield the proposed architectural framework depicted in figure 3.

At the Incident discovery phase shown in figure 1, in the occurrence of an incident, a digital broadcast signal (in audio/textual form - an alarm and email) from the node/terminal/affected department discovering the incident is sent to the 24/7 reachable grounds security incident response team. The signal constitutes of two categories thus;

i. Incident Alert Signal which constitutes an electronic alarm signal, an email containing the following crucial information-the ID of the Signal (this constitutes of the department and resources targeted), Time of the Signal, the nature of the incident, what equipment or persons involved, the damage impact or severity of the incident (High, Medium, Low).

ii. Incident Detail Signal that constitutes an electronic alarm signal, an email containing the following crucial questions- is the incident real or perceived? Has the incident occurred or still in progress? What data or property is threatened and how critical is it? What is the impact on the business should the attack succeed?

The above information will be selected from the application software of the department or terminal that discovered the incident.

The software application to be deployed should be a network-based and should be available for both mobile phones (Android) and PC (windows) platforms; hence barrier of location and portability is eliminated.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

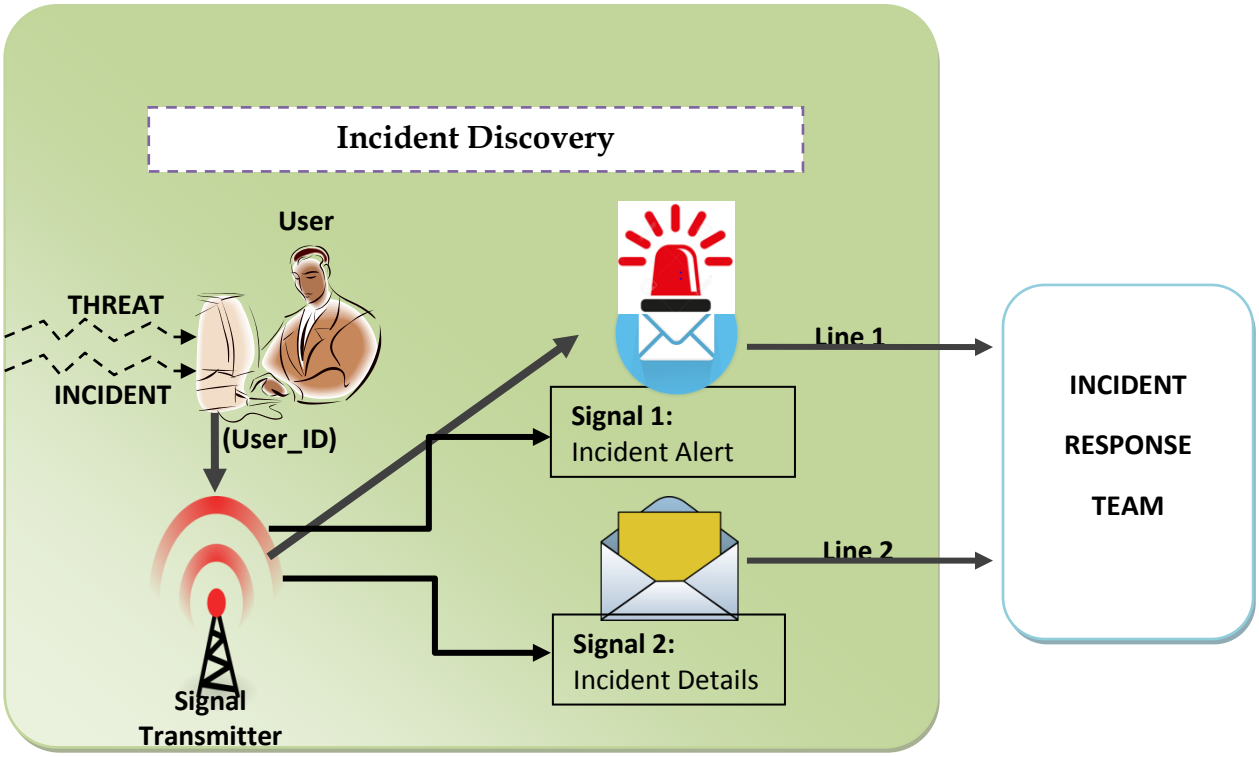

Figure 1: Proposed System Architecture of Incident Discovery Phase

At response to incident phase, carrying out your carefully planned incident responses according to your playbooks requires precise coordination and implementation. As such incident response team is required. This team members are assigned specific roles with individual responsibilities to help improve the efficiency of the team and to help mitigate as much damage as possible in the event of an attack.

Obviously, these roles and the extent of their duties vary among businesses (according to budget, scope of risks and assets, complexity of systems, etc.). However, we considered the main roles which most companies will consider necessary for any incident response team- the Incident Response Manager (IRM), Incident Analysts (IA), Incident Coordinator (IC), Incident Assignment Group Manager (IAGM), and the Incident Process Owner (IPO).

The team members mentioned above easily interact through an application software. The developed software should consist of a log that records the time of call, the department that initiated the call and the date of the incident. The incident or threats discovered should also be recorded by a voice recording system. If any of the incident response teams was not able to respond to his/her calls at the time the incident occurred, a voice message of all the conversation made is sent to him automatically.

The architectural framework as depicted in figure 2 is such that the system offers a first aid response to an incident by shutting down access to targeted resource(s) temporarily, as instructed or activated by the IT incident response team. This ensures other departments are not affected, and also to a large extent reduces the operational barrier of the whole business system.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

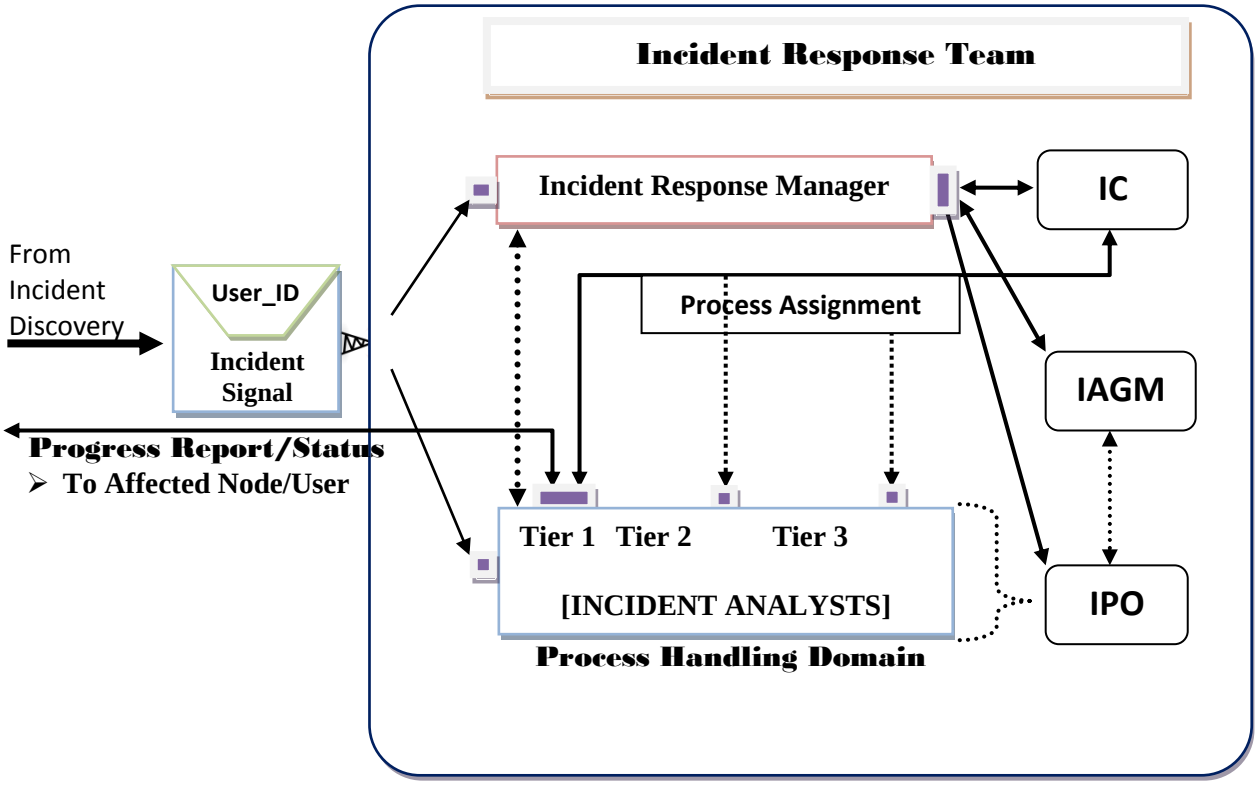

Figure 2: proposed architecture of Incident Response Phase

The proposed system architectural frame work is composed of four major stages carefully considered which are subsummed under the two major phases described earlier. The basic concept of the system architecture is shown in figure 3. The Preventive measure stage secures the system from any attack, using any good software security measure. The Monitoring and detecting stage keeps eyes on the operation of the organization so as to meet the demand, and to know when activities are under threats paraventure the first stage was beaten. The reporting and investigation stage forwards the compliance to the appropriate team, and trace the course of the incident. Of course, the formulation of strategic Plan/Tested and Implemention suggests possible solution to a given problem and put it into practice before execution. After execution re-examines it before implementation.

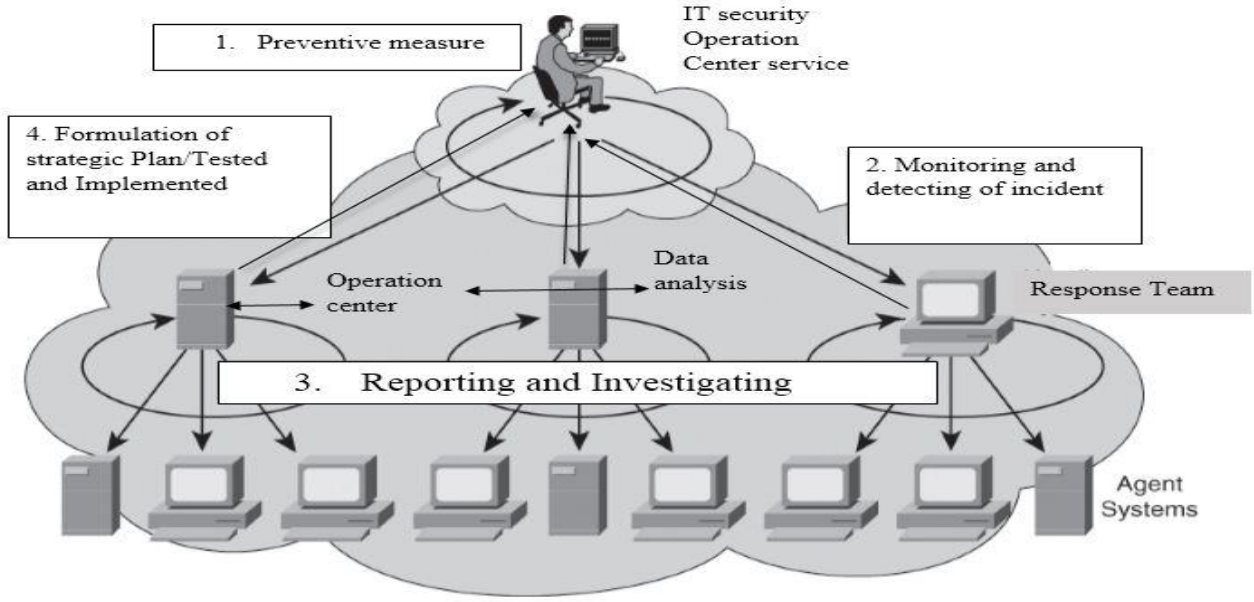

Figure 3. Proposed system architectural framework

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

Figure 3 shows a client/server based architectural system framework for optimizing Computer Security Incident Management Plan. It has a workflow engine where information is being stored and processed, with a notification service given as at when necessary to the response team. It also houses an incident management engine (software agent) where problems or attacks can be monitored, detected or prevented, and all information in the database being secured from any threats. It equally has a monitoring queue were system setting and reconfiguration modules are triggered for the purpose of recovering the system from any attack.

4. CONCLUSION AND RECOMMENDATION

It is observed that even with the best of controls, there is no guarantee that an organisation can prevent disruptive and possibly damaging information security incidents arising from either internal or external sources. Security Incident response management and response processes can enable an organization to respond effectively when security incidents occur, to continue operations and, if necessary, perform critical forensic assessments in the event of attack or disruption.

This research paper presents a unique system architectural framework for merging the incident discovery application with incident response application to generate a robust application that optimizes the computer security incident management plan which enables organization to have an almost instant job recovery and continuity in cases of emergency.

As organization embraces the latest innovations in Information and Communication Technology (ICT), we recommend that they should also be prepared to make provision for efficiently handle security breaches as well. This framework if implemented and deployed will also help to standardize the computer security incident response and recovery in these organizations.

REFERENCES

[1] Ahmad, A., Hadgkiss, J., and Ruighaver, A. B. (2012). "Incident Response Teams–Challenges in Supporting the Organisational Security Function," Computers & Security (31:5), pp. 643-652.

[2] Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., and Zajicek, M. (2004). "Defining Incident Management Processes for Csirts: A Work in Progress,").

[3] Barbara, Michael, (2006). “Determining the Critical Success Factors of an effective Business Continuity/Disaster Recovery Program in a Post 9/11 World: a Multi-Method Approach.”, M BA Thesis, Concordia University.

[4] Botha, J. and R. Von Solms (2004). “A Cyclic Approach to Business Continuity Planning. “Information Management & Computer Security 12(4): 328-337

[5] British Standards (2008a). BS25999. Available from: http://www.bs25999.com/BS25999-Part-1/Business-Continuity-Glossary.html, [Obtained April, 14 2008]

[6] British Standards Institution. (2011). "Bs Iso/Iec 27035:2011 - Security Techniques. Information Security Incident Management." BSI.

[7] Cichonski, P., Millar, T., Grance, T., and Scarfone, K. (2012). "Computer Security Incident Handling Guide V2." NIST.

[8] Cummings, J. (2005). “Nurturing a Culture of Continuity”. Network World, Vol. 20, Issue42, pp. S4-S6.

[9] European Network and Information Security Agency. (2010). "Good Practice Guide for Incident Management." ENISA.

[10] FireEye. (2013). "The Need for Speed” 2013 Incident Response Survey.

[11] Gartner Inc.(2002). Press release. *Gartner Says That Less Than 25 percent of Global*

[12] Grispos, G., Glisson, W. B., and Storer, T. (2014). "Rethinking Security Incident Response: The Integration of Agile Principles," in: 20th Americas Conference on Information Systems. Savannah, Georgia, USA.

[13] Hove, C., Tarnes, M., Line, M. B., and Bernsmed, K. (2014). "Information Security Incident Management: Identified Practice in Large Organizations," IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on: IEEE, pp. 27-46.

[14] Killcrece, G., Kossakowski, K.-P., Ruefle, R., and Zajicek, M. (2003). "Organizational Models for Computer Security Incident Response Teams." DTIC Document.

[15] Line, M. B., Albrechtsen, E., Jaatun, M., Tøndel, I., Johnsen, S., Longva, O., and Wærø, I. (2009). "A Structured Approach to Incident Response Management in the Oil and Gas Industry," in Critical Information Infrastructure Security. pp. 235-246.

[16] Line, M. B., Tondel, I. A., and Jaatun, M. G. (2014). "Information Security Incident Management: Planning for Failure," IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on: IEEE, pp. 47-61.

[17] NFPA 1600 (2007). *Standard on Disaster/Emergency Management and Business Continuity fs*. 2007 Edition, National Fire Protection Association.

[18] Shedden, P., Ahmad, A., and Ruighaver, A. B. (2011). "Informal Learning in Security Incident Response Teams," in: Australasian Conference on Information Systems. Paper-37.

[19] Snedaker, S., (2007). Business Continuity and Disaster Recovery Planning for IT Professionals, Syngress Publication, Inc.

[20] Tan, T., Ruighaver, T., and Ahmad, A. (2003). "Incident Handling: Where the Need for Planning Is Often Not Recognised," in: 1st Australian Computer, Network & Information Forensics Conference.

[21] Werlinger, R., Botta, D., and Beznosov, K. (2007). "Detecting, Analyzing and Responding to Security Incidents: A Qualitative Analysis," in: 3rd symposium on Usable privacy and security. ACM, pp. 149-150.

[22] Werlinger, R., Muldner, K., Hawkey, K., and Beznosov, K. (2010). "Preparation, Detection, and Analysis: The Diagnostic Work of IT Security Incident Response," Information Management & Computer Security (18:1), pp. 26-42.

[23] Wikipedia (2008). Available from: http://en.wikipedia.org/wiki/Business_continuity. [Obtained May 9, 2008]

(This work is licensed under a Creative Commons Attribution 4.0 International License.)