*Malik LGURJCSIT 2019*

LGU International Journal for
**Electronic Crime Investigation**

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

Research Article Vol. 3 Issue 3, July - September 2019

# Cyber Security - Incident Response and Management

Muhammad Shairoze Malik
shairozemalik@lgu.edu.pk
Lahore Garrison University

**Abstract:**
Today, Information Technology has bought a lot of benefits for the mankind but it has also made us susceptible to failures and attacks as well. This article discusses the increasing complexity of cyber-security threats and capabilities of information security teams in applying controls required to effectively respond to threats. In this article, the main stages of managing information security incidents and events are discussed, designed to help create an effective response process to security incidents and as a result to reduce losses and quickly restore performance in dynamically changing IT infrastructure and threat landscape.

**Keywords:** Cybersecurity Incident Response, Cyber Threats, Incident Logging, Incident Management, Cyber-Security Warning Systems, Organization Security.

## 1. Introduction

As organizations become more and more technology dependent, they become more vulnerable to information security attacks. The situation can be summarized by following quotes:

"It is inescapable at some phase that associations will endure a data security incident. Such an incident may bring about numerous negative effects, for example, loss of organization reputation and client confidence, legal issues, lost efficiency and direct monetary loss. [1]"
It is not economically feasible for an organization to implement unbreakable security measures to protect their assets [2], so they need to prepare for a response in case of a security attack on their ICT infrastructure.

An information security incident can be defined as;

"An identified occurrence of a system, service or network state pointing to a possible breach in information security, policy or failure of controls or a previously unknown situation that may be related to the security, and has a significant probability of compromising business operations and threatening information security. [3]"

Reducing the potential risks of violation of the availability, integrity and confidentiality of information resources due to information security incidents can be achieved by their timely detection in conjunction with the response. Moreover, responding to information security incidents is often less expensive and more effective than investigating them. An information security incident can lead to malfunctioning of systems, services, networks and as a result prolonged unavailability of critical business processes, loss / modification of the transmitted or stored information without the possibility of its recovery, reputational risks of the owner of the information resources and contractors.

A practical approach to building a reference process is described in detail in following international standards:

- ISO / IEC 27001: 2013 Information Security Management System.

A standard that contains both recommendations for the construction, implementation, use and support of the information security management system as a whole, and approaches to managing information security incidents [4].

- ü NIST SP 800-61 Computer Security Incident Handling Guide.
  A comprehensive security incident handling guide that describes various approaches to incident response and handling [5].
- ü CMU / SEI-2005-TR-015 Defining incident management process for CISRT.
  A document for evaluating the performance of the CISRT (Critical Incident Stress Response Team) unit that provides prevention, processing and response to information security incidents [6].
- ü ISO / IEC TR 18044: 2004 Information Security Incident Management.

  The document established recommendations for information security incident management regarding planning, operation, analysis and improvement of the process [7].

- ü NIST SP 800-83 Guide to Malware Incident Prevention and Handling.
  A guide to preventing and handling malware incidents involving workstations and laptop infections [8].
- ü NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response.
  A guide to investigative techniques for responding to identified incidents [9].
- ü ISO / IEC 27035-2:2019 Guidelines to Plan and Prepare for Incident Response.
  It points to the development of guidelines to enhance an organization's actual readiness to respond to a security incident [10].
  These two can be regarded as the main guidelines related to incident management;
- ü ISO-IEC 27035 [10]
- ü NIST Special Publication 800-61 [5]

They offer a structured approach to planning and preparing for incident response, what to do when incident strikes and how to extract lessons afterwards.
SANS [11] and ENISA [12] also provided


**Fig 1: NIST-SP 800-61 r2 Incident-Response-Life-Cycle**

In general case, the life cycle of managing events and incidents of information security is usually divided into following stages:

1. Plan & Prepare
2. Detection & Reporting
3. Assessment & Containment
4. Incident Response
5. Lessons learnt

Next, we consider each stage of the information security incident and event management process in more detail.

## 2. Plan & Prepare

Planning and preparing is presumably the most significant step in incident response. An association that is not set up to deal with an incident is more likely to fail in detecting and in turn responding to an information security incident in their vicinity. A main recommendation is the establishment of a security response team based on the experiences at LRZ-CSIRT [13]. The planning phase includes the formation of an incident response program including procedures, policies, compliance and governance documents, etc. For effective execution, the socializing of the different aspects of this program is also required. The studies and experiences provided by Werlinger et al. [14], Metzger et al. [13], Ahmad et al. [15], hove and Tarnes [16], gives an overview of many technical measures that can be taken to prepare for incident detection and response. They can be summarized in following steps:

- Organize a round the clock call-tree among

all departments in the organization, so a breach can be communicated as soon as possible.
- Implement IDS / IPS and other monitoring systems.
- Make sure that incident response team is fully equipped with required equipment, access, software, chain of custody forms, secure storage and a control room.
- Train incident responders with the organization's IT infrastructure including installed software, policies, protocols & permitted ports, etc.
- Use a single email address with shared mailbox vs. a distributed list for better achieving. The access to the mailbox should only be for the incident response team members.
- Organize internal and external training sessions for the staff members.
- Run mock realistic breach scenarios to test the detection tools and response process.

### 2.1 Detection & Reporting

The purpose of detecting computer attacks is to timely respond to incidents related to them in order to further take measures to eliminate the consequences of such incidents.

The timely detection of a security breach is a major problem in implementing security measures. An observation made by researcher Koivunen [17] was that in majority of the incidents studied none to the victims discovered the security breach own their own, but they had to rely on automated tools for timely detection of breaches.

In the course of activities to detect computer attacks, the following processes should be implemented:
- Monitoring the implementation of uniform operating rules for the detection of computer attacks on information resources.
- Control over centralized updating of decision rule databases for computer attack detection tools.
- Detection of previously unknown computer attacks at the network level, including the use of network traffic analysis tools on communication channels.
- Detection of previously unknown computer attacks conducted using malicious software, including using methods of behavioral analysis of software.
- Develop decisive rules for unknown computer attacks.

### 2.2 Assessment & Containment

The analysis of an incident can be done in two stages:

i. Initial Incident Analysis
ii. Comprehensive Incident Analysis.

The objective of the initial analysis of the incident is the establishment of the circumstances and possible consequences of the incident.

The objective of the comprehensive incident analysis is the point out the causes of the incident and the actual consequences to the infrastructure.

The purpose of the analysis of the data on security events is to identify information security incidents, including those related to previously unknown computer attacks, as well as incidents related to the insufficient effectiveness of the measures taken to protect information.

Information is collected from results of all information protection tools used in accordance with the security policies adopted in information systems. These are sources such as:

- Attack detection tools and firewalls used on communication channels through which information resources are accessed.
- Network traffic analysis tools using data mining techniques.
- Detection tools for attacks and firewalls used in local area networks in which the components of information resources are located.
- Software Behavioral Analysis Tools.

The collection of information from these sources is recommended in an automated mode. In this case, the rules for normalizing information security events are implemented. Information about security events is compared with information about the vulnerabilities of components of information resources to predict the possible actions of an attacker during computer attacks.

When analyzing data about security events using automated tools, correlation rules are applied [14]. Correlation rules are determined by responsible employees or, a third party security firm, taking into account information obtained during the inventory and identification of vulnerabilities in information resources. In the process of functioning, constant work is carried out to adapt the sources of data on security events with the means of their analysis to increase the efficiency of detection of computer attacks, as well as work on formation of new correlation rules and signatures.

It is suggested that incidents be recorded utilizing computerized methods for accounting and processing dependent on markers that influence the level of negative effect of an incident, since the manual procedure of incident handling is ineffective as they prompt a high asset utilization of work force and altogether increase the reaction time to information security incidents of high criticality.

It is particularly challenging to handle an incident when IT operations are outsourced among several suppliers. In such cases, priority handling to incidents becomes a major issue, i.e. "what does it mean for the customer, when a server is down? (de Souza et al., 2011) [18].

### 2.3 Incident Response

Different organizations have different approaches to handle an incident. For some, it is important that the incident is handled properly and its future occurrence must be controlled or any other similar vulnerability in system should be rectified. While for others, it is important to minimize the damage of business operations by fast recovering of systems using temporary means if necessary [16].

Software and hardware documentation were identified as the most important information for dealing with incidents, Kurowski and Frings (2011) [19].

An organization's information security incident response process can be divide into following stages:

- Fixing the state and analysis of objects of information resources involved in the incident.
- Coordination of activities to stop the impact of computer attacks, the conduct of which caused the occurrence of the incident.
- Fixation and analysis of network traffic circulating in the information resource involved in the incident.
- Determining the causes of the incident and its possible consequences for the information resource.
- Localization of the incident.
- Collection of information for the subsequent establishment of the causes of the incident.
- Planning for incident response.
- Disaster management.
- Control of liquidation of consequences.
- Formation of recommendations for improving regulatory documents ensuring security of information resources.

### 2.4 Lessons Learnt

An incident is deemed completed after all measures have been taken, provided that the establishment of the causes of the incident has shown the adequacy of the measures taken. Analysis of the results of the elimination of the consequences of the incident includes and assessment of the following aspects:

- Damage caused to the information resource and its owner as a result of the incident.
- Shortcomings in ensuring the security of information that did not allow to prevent the incident.
- Timeliness of incident detection.
- Personnel actions in localizing the incident and liquidating its consequences.
- The timing of the aftermath of the incident.
- When assessing the harm caused to an information resource and its owner as a result of an incident, the following are taken into account:
- Personnel labor and other costs associated with the elimination of consequences.
- Damage caused to the public interests and interests of the owner of the information resource, including those related to violation of confidentiality.
- When assessing deficiencies in ensuring information security, the following are determined:
- Regulatory requirements, non-compliance, lack of effectiveness which made the incident possible.
- Additional protective measures that are not

mandatory in accordance with the current regulatory documents, but which could prevent the incident.

## Conclusion

Depending on the organization's activities, methodological recommendations of international standards, which describe a fairly complete set of measures necessary to build the process of managing incident and information security events, can be the optimal choice of application. Regardless of which methodology is selected or developed for managing incidents and information security events, it should:

- Take into account the needs of the organization.
- Be as automated as possible.
- Run non-stop (24 hours a day, 7 days a week).
- Be applicable to the organization, taking into account the corporate culture and available resources.
- Reflect in the form of a model the real landscape of information security threats relevant to the organization.
- Be transparent to all interested parties, including company management, representatives of regulators, external and internal auditors.

## References


[1] Ahmad A, Hadgkiss J, Ruighaver AB. Incident teams - challenges in supporting the organizational security function. Comput Secur 2012;31(5):643-52

[2] Anderson R, Barton C, Bohme R, Clayton R, Eeten M, Levi M, et al. Measuring the cost of cybercrime. In: 11th Workshop on the Economics of Information Security (WEIS'12); 2012.

[3] ISO/IEC 27035-1:2016 Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management. Retrieved on October 2, 2019, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-1:v1:en

[4] ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements. Retrieved October 1, 2019, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[5] Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone - "Computer Security Incident Handling Guide". Retrieved on October 1, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[6] Alberts. Christopher, Dorofee. Audrey, Killcrece. Georgia, Ruefle. Robin, and Zajicek. Mark, "Defining Incident Management Processes for CSIRTs: A Work in Progress," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2004-TR-015, 2004. Retrieved on October 1, 2019, from http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=7153

[7] Hamidovic, Haris. (2011). An Introduction to Information Security Incident Management Based on ISO/IEC TR 18044:2004. VI. Retrieved on October 1, 2019, from https://www.researchgate.net/publication/254864149_An_Introduction_to_Information_Security_Incident_Management_Based_on_ISOIEC_TR_180442004

[8] Murugian Souppaya, Karen Scarfone "Guide to Malware Incident Prevention and Handling for Desktops and Laptops" revision 1, 2013. Retrieved on October 1, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

[9] Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang "Guide to Integrating Forensic Techniques into Incident Response", 2006. Retrieved on October 1, 2019, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

[10] ISO/IEC 27035-2:2016 Information technology - Security techniques - Information security incident management

- Part 2: Guidelines to plan and prepare for incident response. Retrieved on October 2, 2019, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-2:ed-1:v1:en

[11] Kral P. The incident handlers handbook. SANS Institute; 2011. Retrieved on October 2, 2019, from https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

[12] ENISA, Good practice guide for incident management; 2010. Retrieved on October 2, 2019, from https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management/at_download/fullReport

[13] Metzger S, Hommel W, Reiser H. Integrated security incident management e concepts and real-world experiences. In: Sixth International Conference on IT Security Incident Management and IT Forensics (IMF); 2011. pp. 107-21.

[14] Werlinger R, Muldner K, Hawkey K, Beznosov K. Preparation, detection, and analysis: the diagnostic work of IT security incident response. Inf Manag Comput Secur 2010;18(1):26-42.

[15] Ahmad A, Hadgkiss J, Ruighaver AB. Incident response teams - challenges in supporting the organizational security function. Comput Secur 2012;31(5):643 - 52.

[16] Hove C, Tårnes M. Information security incident management: an empirical study of current practice. Norwegian University of Science and Technology; 2013.

[17] Koivunen E. Why wasn't I notified: information security incident reporting demystified. In: 15th Nordic Conference in Secure IT Systems (NordSec 2010); 2010.

[18] de Souza CRB, Pinhanez CS, Cavalcante VF. Information needs of system administrators in information technology service factories. In: Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (CHIMIT '11). New York, NY, USA: ACM; 2011. p. 10. Retrieved on October 3, 2019 from https://dlnext.acm.org/doi/abs/10.1145/2076444.2076447.

[19] Kurowski S, Frings S. Computational documentation of IT incidents as support for forensic operations. In: IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on; 2011. pp. 37- 47.