Cumhuriyet Üniversitesi Fen Fakültesi
Fen Bilimleri Dergisi (CFD), Cilt:36, No: 6 Özel Sayı (2015)
ISSN: 1300-1949

Cumhuriyet University Faculty of Science
Science Journal (CSJ), Vol. 36, No: 6 Special Issue (2015)
ISSN: 1300-1949

Introduction and Evaluation of Computer Security Incident Response Team (CSIRT) in Organizations

Mohammad Mahdi ESTEDLAL

MSc in Information Technology Systems Management

Received: 20.04.2015; Accepted: 09.07.2015

Abstract. With the rapid development of information technology and the continuous changes in the services, information technology has played a key role in organizations. During the past years, a great number of IT infrastructure and particular applications have been employed by the organization. Many organizations have purchased a large number of high-end enterprise applications such as ERP, CRM, etc. to improve their business capacity. At the same time, these organizations a huge amount of time and resources are spent for maintenance applications. At the same time, these organizations are spent a huge amount of time and resources for application's maintenance. since any incident that may result in service interruptions, causes very high costs for organizations, The issue of how organizations can deploy an effective way to manage events, So that costs can be reduced, the occurrence of events can be avoided and the continuity of their business can be guaranteed, is considered. For this purpose, approaches and events management models offered by some mature frameworks such as ITIL, COBIT and standards like ISO / IEC 20000, are accepted widely in many organizations. These frameworks combine extensive management practices in order to support organizations for achieving the desired quality and creating value from IT operations.

For example ITIL provides A set of best process-oriented practices for IT service management. IT service management practices, directly or indirectly causes establishing communication between employees, innovation, finances and domestic business interests.

Keywords: Incident Management, Incident life Cycle, Information Technology Infrastructure Library (ITIL), Computer Security Incident Response Team (CSIRT), Computer Emergency Response Team (CERT)

1. INTRODUCTION

In today's business environment, information is not only a key asset for organizations, but also a decisive factor in gaining competitive advantage. In many cases, information drivers most business processes and employees are involved at all levels from senior management to staff with unskilled jobs [3].

Furthermore, the dependence of organizations around the world to information and communication technologies (ICT) in order to support key operations that lead them to their goals is on the rise. Many organizations with increasing dependency to their information systems are sure that governance (or at least manage) information security is an important part of their management [4]. Thus, using modern technologies, have provided new opportunities for influence, even the best security infrastructure cannot guarantee that a dangerous attack will not happen [1].

ISO / IEC 27001:2005 Standard, which is one of the standards in the field of information security management, information security is defined as "information security, protecting the confidentiality, integrity and availability of information. Well as features such as authenticity, accountability, unquestionable and reliable can be considered [7].

* Corresponding author. Mohammad Mahdi ESTEDLAL

Special Issue: International Conference on Non-Linear System & Optimization in Computer & Electrical Engineering

Thus, information security objectives are confidentiality, integrity and availability. But achieving just these three objectives doesn't mean achieving information security, But security will be achieved through the prevention of attacks against information systems and organization's mission despite the attacks and events [8].

2. LITERATURE REVIEW

2.1. Security Events

A computer security incident is defined as any act that threats computer security in any way: For example, Data security endangerment, system or data flow interruption. Another definition of computer security incidents is provided in the following: unauthorized access, use or modification, disclosure or destruction of information or interference in operation of a computer system. According to the definition given in the Computer Incident Factor Analysis and Categorization Project, a computer incident includes any act or intentional or unintentional event which occurs on sources of information or otherwise includes them and potentially destabilizes, disrupts, or destroys resources, policies, services, data, individuals or society. [1]

The main areas of event management are information security and information technology events. Events which are limited to computers, network equipment, networks and the information those are inside the equipment or transferred by them [10]. Users and customers may be able to report incidents via phone, email, web portal, visiting or by the event management process, therefore, organizations must be able to manage events in the possible shortest time and in an effective manner.Information Security Incident Management is also emphasized in ISO / IEC 27001:2005 Standard which is one of the standards in the Information Security Management field.

In the following, we will discuss the issue of event management from the perspective of ISO / IEC 27001:2005 standard, ITIL framework and explain about forming teams to respond to computer security incidents.

2.2. Management of information security incidents at ISO / IEC 27001:2005 Standard

Controls in the ISO / IEC 27001:2005 Standard is considered, includes 11 paragraph as follows, the total includes 39 major categories of security and an introductory paragraph, including estimating and resolving risk.

Security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, acquisition, development and maintenance of operating systems, , information security event management, business continuity management, compliance

According to definition of stated standard Information Security Incident is: "One or a series of unwanted or unexpected information security events which endanger Business operations and threat Information security with large Probability."

Accordance with paragraph A-13 of the stated standard, information security incidents should be managed in an effective and efficient manner.

According to the provisions of stated standard control document, the following controls on the management of information security events should take place:

A - Reporting information security events and weaknesses includes Reporting information security events and Reporting information security weaknesses.

B - Management of information security incidents and improvements includes Responsibilities and Procedures, Learning from information security incidents, collection of evidence.

2.3 - Incident Management process from the perspective of the ITIL framework

ITIL or Information Technology Infrastructure Library as the most popular framework for IT service management well covers all aspects of IT governance [18]. ITIL as well as a summary of best practices for IT service management is an informal standard [19] and based on the ISO 20000 standard [20].

The third version of ITIL has five main axis includes: service strategy, service design, service transition, service operations, continuous improvement of service [21].

As is shown in the following figure, the operation processes and key activities include: Event Management, Incident Management, Problem Management, Run the application and Management of access rights.

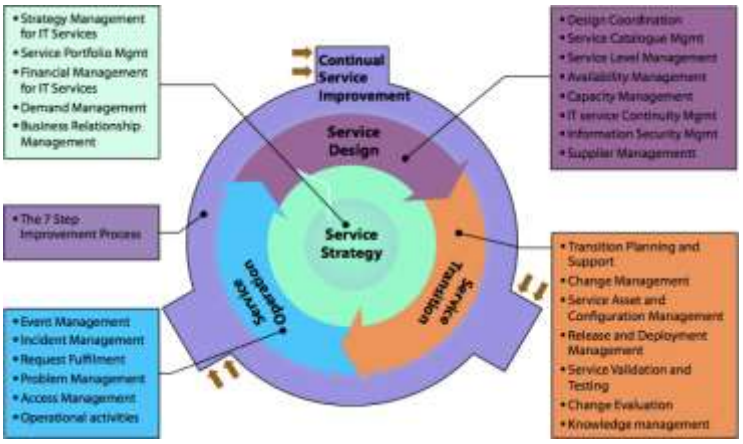

Figure 1. The Service Lifecycle ITIL V3 [22].

In dictionary of Information Technology Infrastructure Library (ITIL), Incident is defined as: an unplanned interruption in presenting IT services or reduction in its quality level. The failure in one of the configuration items (CI) has not yet impacted service is also known as events, for example, the failure of one disk in Mirror RAID ".

Incident Management is a process for dealing with all types of events. These can include damages, inquiries or requests from users (usually by contacting the service desk), technical staff, or items that are automatically detected and reported by the monitoring tools [21].

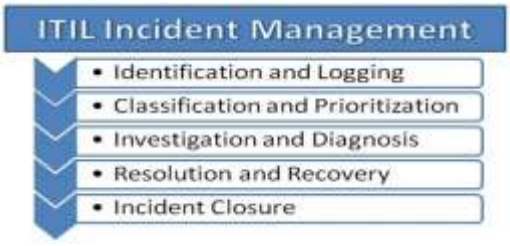

Figure 2. The overall process of incidents management.

The main objectives of this process is restoring normal operation conditions of service, in the fastest possible time, with minimum impact on business and ensure to maintain the best possible level of quality and service availability. Normal Service Operation here is defined as service operation within the limits of a Service Level Agreement (SLA) [21]

2.4 - Handling events by computer security incidents response team (CSIRT)

When an organization (especially with the nature of e-business) is confronted with a problem of computer security, should respond to this problem quickly and effectively. Any amount that organizations can quickly detect attacks, analyzing them successfully and answer them, can reduce damage caused by attacks and repair costs.

A CSIRT is a service organization that is responsible for receiving, reviewing and responding to Submitted reports and activities related to computer's problems and events. The services of this organization are usually defined for a specific range which can be a corporation, government agency, or educational organization, a region or a country. There are different classifications.

Based on the structural and organizational model, the purpose and service or scope of authorization, for CSIRTs.

There are many services that a CSIRT can provide but no CSIRT has provided all of them, selection of suitable services is a crucial decision. CSIRT known services as defined in CSIRT reference books and has been released by the CERT / CC is expressed as follows:

A - Reactive services include warning and alarm management, vulnerability management, management of the debris of the attack.

B - Preventive services include posters, view, and review the technology, Audits and security assessments, configuration and maintenance of tools and applications, and infrastructure and security services, development tools, security, intrusion detection services, distribution of security-related information.

C - security quality management services, including the distribution of information relating to security, risk analysis, failure recovery plan and business continuity, security consulting, creating awareness, training, certifications or product evaluation.

It is clear that, there are many different types of services that a CSIRT can provide. Some Services are directly related to the review of events which are basic services of CSIRT. Other services, such as security training or auditing may only indirectly be related to the review of the event, while the organization's security needs will be considered in a wider area. Due to the large variety, some services may be replaced by other parts of the CSIRT as IT, training, inspection or other available units. Determining the duties and responsibilities depends on the organizational structure of the mother or the host that CSIRT has been established. There is an in-depth analysis of the entire process of managing incidents (Incident Management) and all work flows and involved in the CERT / CC documents «The definition of Incident Management processes for CSIRT." Essentially the incident management follows workflow is shown in Figure 3.

3. STRUGGLE CENTRES WITH SECURITY EVENT

Spreading the Morris worm in 1988 was the main motivation for creating the first CSIRT. Failure of many Internet network communication paths (it was called the ARPANET) was result of this worm attack. After inhibition of worm attack, America's National Computer Security Center (part of the National Security Agency) held meetings to make a decision on preventing and responding to such similar incidents in the future. The meeting turned out that there was no obvious approaches to manage such an attack against a computer security [1].

By recognizing this problem, Defense Advanced Research Projects Agency (DARPA) announced plans to invest on establishing a center for coordination of security incidents on the Internet. This Center was called Computer Emergency Response Team (CERT). Finally CERT was identified as a service to Carnegie Mellon University and renamed the (Cert / CC) Coordination Center CERT [1].

DARPA investigation results showed that a team cannot meet our needs. During the following years, other organizations such as America Department of Energy, National Aeronautics and Space Administration (NASA), the National Institute of Standards and Technology and America's military forces, each one established their own team, similar to CERT / CC, but with a focus on areas of their own business.

In November 1990, CSIRT's 11 groups established (FIRST) Forum of Incident response and Security Teams. The forum Holds an annual conference in order to coordinate communication between teams, sharing information, sharing and analyzing security holes [1].

More information about the forum can be found at the website addressed www.first.org .full list of current members of the FIRST is also available.

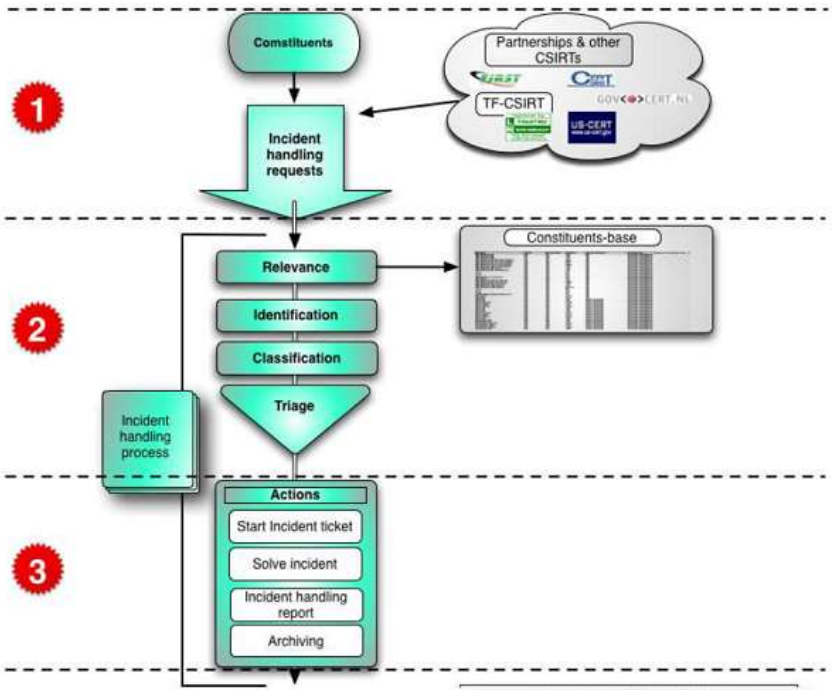

Figure 3. Incident Handling process flow [25].

In 1991 and 1992, the first European CSIRT founded in French at SPAN (Space Physical Analysis Network [1].

In 2001, Trusted Introducer or TC to maintain European CSIRT team's directory and their accreditation were formed [1]. In the year 2003, APCERT (Asia Pacific Security Incident Response Coordination) for coordinating CSIRT Asia-Pacific region teams formed [1].

In Iran, Maher center "(Relief and Coordinating the operation of computer events management)"as a specialized department within the CSIRT / CERT organization as a subset of information technology, is working.

In Iran, "Kashef" (Control of Network Security and response to Bank emergency) as an independent center, is responsible for establishing coordination between banks and providing services In face of relevant emergency in scope of banks and finance – credit institutions.

In Iran, police feta, is responsible for following up and doing legal action in order to identify and arrest criminals effectively after security incidents in country information exchange Space scope.

Some Iranian government and private organizations, also attempt to deploy CSIRT teams.

4. SOME DOCUMENTS IN THIS AREA

Since many research studies in the field of incident management processes based on ITIL V3 framework and CSIRT teams has been done representing importance and the attention of organizations to these issues. Some of them include:

1. The book provided by Carnegie Mellon University [24], one of the valid documents that provide guidance about formation and administration of a rapid response team to computer events.

2. Carnegie Mellon University technical report [26], has been provided in 2004,presents a successful practice model for implementation processes and tasks incident management using the CSIRT.

3. European Network and Information Security Agency (ENISA) technical report [10], gives a clear picture of the incident management process, roles, work flows and policies related to it, based on the successful obtained practices. This report provides a step by step approach to forming a CSIRT teams considering the theme related aspects such as business management ,process management and technical perspectives.

4. The information contained in the Clearing House for Incident Handling Tools (CHIHT), available on the website of the European Network and Information Security Agency, is a repository of many useful tools and guidance provided to organize and improve CERT Services.

5. National Institute of Standards and Technology (NIST), has provided a document in 2012, where responding to computer incident is considered as an important part of IT programs because the effective implementation of response to the event is a complex responsibility and creating a good feature for responding to the event requires planning and principles sources. This publication helps organizations in creating respond to computer security incidents capabilities and effective handling events. This publication also offers advices for handling events, especially for the analysis of the data associated with the event and determine the appropriate response to each event [27].

6. In a book which its summary has been published in an article by passive defense Centre, the definition of CSIRT and its necessity, history, team services, various models and organizational structures to form the CSIRT has been expressed. Also In numerous articles how to deploy teams and implement the necessary frameworks has been studied.

5. DISCUSSION & CONCLUSION

Many organizations are using information technology to deliver services, following the framework for IT service management in their organizations. One of the stated processes in this context is incident management process. Therefore, organizations are looking to implement the framework, are required to have a process for managing their events.

Moreover, organizations have found that there isn't a unique security solution for supplying system security but it should be used of multilayered security strategy and the formation of a CSIRT is one of these layers.

Hence, in the first place, it seems that the formation of CSIRT teams in organizations In order to perform Incident Management processes (Incident Management) effectively can be efficient.
To start this process, we must identify all activities related to incident management and answer the question of "Who will perform the activities related to incident management? "This question is one of the question that is often asked by organizations that are looking to plan a strategy to incident manage in their organization.

It should be noted, incident management processes in CSIRT team examined independently and a model is also presented for it. But organizations in accordance with the Incident Management process, In Service -operations phase should examine the influence of establishment of a CSIRT initially and extract localized incident management process for their collections.

REFERENCES

[1] Askarzadeh, H., Rashti, S.M.R, computer security incidents response team (CSIRT / CERT), first edition, Tehran, rouyesh javanehhay farda , 1389.

[2] Mashhadi Abd Al Rahman, F., "provide a framework for an effective constitute aid groups and Computer Emergency Response (CSIRT) in enhancing the security of computer networks", Master Thesis PNU, 1390.

[3] SH. Von Solms, and R. Von Solms, "Information Security Governance: Due Care," Computers & Security, Vol. 25, (7), pp. (494-497), 2006.

[4] PW. Anderson, "Information Security Governance," Information Security Technical Report, Vol. 6, (3), pp. (60-70), 2001.

[5] Grossman, "FEMA Takes a New Enterprise Architecture Approach to Support DHS," Department of Homeland Security, 2009.

[6] A. Buecker, P. Ashley, M.Borret, M. Lu, S. Muppidi, N.Readshaw, "Understanding SOA Security," Red Book, IBM, 2007

[7] ISO/IEC 27001:2005, 1st Ed.: Information technology - Security techniques – Information security management systems – Requirements.

[8] F. S. Malik, "Information Security Maturity Model," International Journal of Computer Science and Security (IJCSS), Vol. 5, (3), 2011.

[9] ISM3 Consortium, "ISM3 - Information Security Management Maturity Model," 2007.

[10] European Network and Information Security Agency, "Good Practice Guide for Incident Management," 2010.

[11] Moura, J.Sauve, C.Bartolini, "Business-Driven IT Management-Upping the Ante of IT: Exploring the Linkage between IT and Businessto Improve Both IT and Business Results,"IEEE Communications Magazine, Vol. 46 (10), 2008.

[12] Office of Government Commerce, ITIL Core Books, UK, 2007.

[13] IT Governance Institute, Control Objectives for Information andrelated Technology (CobiT), 4.1th Edition, USA, 2007.

[14] International Organization for Standardization, "ISO/IEC 20000-1"&"ISO/IEC 20000-2", 2005.

[15] W. Gue, Y. Wang, “An Incident Management Model for SaaS Application in the IT Organization,” IEEE Computer Society, 2009.
[16] Cater-Steel, "Information Technology Governance and Service Mangement: frameworks and adaptions," IGI Global, 2009.
[17] V. Lloyd, C. Rudd, and C. Littlewood, "Planning to Implement Service Management," Earley: itSMF Ltd, 2003.
[18] Nabiollahi, B. Sahibuddin,, "Considering Service Strategy inITILV3 as a Framework for IT Governance, 2008.
[19] Hochstein, R. Zarnekow, W. Brenner, "ITIL as Common Practice Reference Model for IT Service Management: Formal Assessment andImplications for Practice", IEEEXplore, 2005.
[20] M. Brenner, M. Garschhammer, and H. Hegering,"Managing Development and Application of Digital Technologies", Berlin: Springer, 2006.
[21] Cartlidge , A. Hanna, C. Rudd, I. Macfarlane, J. Windebank, and S. Rance,,"An Introductory Overview of ITIL V3”,The UK chapter of the itSMF, 2007.
[22] www.b-pi.com
[23] www.brighthubpm.com
[24] Carnegie Mellon, Software Engineering Institute, “Handbook for Computer Security Incident Response Teams (CSIRTs)”, 2ndEdition, 2003.
[25] European Network and Information Security Agency, “a step-by-step Approach on How to Setup a CSIRT,” 2006.
[26] Carnegie Mellon, Software Engineering Institute, “Defining Incident Management Processes for CSIRTs: A Work in Progress”, 2004.
[27] National Institute of Standards and Technology, "Computer Security Incident Handling Guide," 2nd Edition, 2012.