Chapter 28
Cybersecurity Incident Response and Management

Regner Sabillon
Universitat Oberta de Catalunya, Spain

ABSTRACT

This chapter presents a systematic literature review on best practices regarding cybersecurity incident response handling and incident management. The study identifies incident handling models that are used worldwide when responding to any type of cybersecurity incident. The authors highlight the importance of understanding the current cyber threat landscape in any incident response team and their standard operations procedures. The chapter provides guidelines for building a cybersecurity incident team in terms of incident categorization, capabilities, tasks, incident cost calculation, and metrics.

INTRODUCTION

Following the devastating Internet effects of the "Morris Worm" in 1988, the Defense Advanced Research Projects Agency (DARPA) assigned the Software Engineering Institute of the Carnegie Mellon University with the mission to set up a security center for emergencies – this center was lately named the CERT Coordination Center (CERT/CC). The CERT Division (Computer Emergency Response Team) of the Software Engineering Institute (SEI) has been a pioneer in providing resources to create and implement Computer Security Incident Response Teams (CSIRT) and Incident Management resources against global cybersecurity threats and vulnerabilities. According to the National Institute of Standards and Technology-NIST (2012), an event is any observable occurrence in a system or network, an adverse event is a negative consequence and a computer security incident is a violation or imminent threat of violation of acceptable use policies, standard security practices or computer security policies.

A recent study from Hathaway et al. (2015) about Cyber Readiness Index (CRI) 2.0, the CRI 2.0 methodology evaluated the cyber readiness of 125 countries by assessing the national cybersecurity commitment and maturity. The analysis included more than seventy indicators across seven basic elements: national strategy, incident response, e-crime and law enforcement, information sharing, investment in research and development (R&D), diplomacy and trade, and defense and crisis response.

DOI: 10.4018/978-1-6684-3698-1.ch028

The Cybersecurity incident response capability can be organized and achieved as a national agency (National Computer Security Incident Response Team - CSIRT) or a military unit, or through the development of an organizational team like the Computer Emergency Response Team (CERT).

INCIDENT HANDLING MODELS

According to ISACA (2012), Incident Management is the capability to effectively manage unexpected disruptive events with the objective of minimizing impact and maintaining or restoring normal operations within defined time limits. Subsequently, Incident response is considered as a subset of incident management as the operational capability of incident management that identifies, prepares, responds to incidents to controls to control and limit damage; provides forensic and investigative capabilities; maintaining, recovering and restoring normal operations based on the service level agreements (SLAs).

According to Oriyano et al. (2020), an incident is defined as any violation or impending of the security policy. Existing corporate security policies clearly define what events are considered cyber incidents, contain procedures and guidelines for responding to cyber incidents and define clear course of action to deal with detection and response to security incidents.

Table 1 shows the most relevant incident handling and management models:

Table 1. Cybersecurity incident handling and management models

Name of the model	Phases
Donaldson et al. (2015): Incident Response Process	Identify, investigate, collect, report, contain, repair, remediate, validate, report conclusions and resume normal IT operations
CREST (2014): Cyber security incident management capability	Prepare, respond and follow up
NIST (2012): The Incident Response Life Cycle	Preparation; detection & analysis, containment; eradication & recovery and post-incident activity
ISACA (2012): Incident Management Life Cycle	Planning and preparation; detection, triage and investigation; containment, analysis, tracking and recovery; postincident assessment and incident closure
SANS (2011): Incident handling step-by-step	Preparation, identification, containment, eradication, recovery and lessons learned
ISO/IEC 27035 (2011): Information Security Incident Management	Plan and prepare; detection and reporting; assessment and decision; responses and lessons learnt
ENISA (2010): Incident handling process	Report, registration, triage, incident resolution, incident closure and post-analysis
Kennedy (2008): Modified small business approach for incident handling	Develop a security policy, protect computer equipment, keep data safe, use Internet safely, protect the network, secure line of business applications and training
CERT/CC (2003) Incident handling life-cycle process	Report, analyze, obtain contact information, provide technical assistance, coordinate information & response and provide resolution

While some incident handling models have similar phases, others combine certain elements in conjoined phases but in the end, any specific model must be able to mitigate and eradicate the cybersecurity incident in order to avoid additional cyber threats.