A Structured Approach to Guide the Development of Incident Management Capability for Security and Privacy

Luis Tello-Oquendo[1], Freddy Tapia[2], Walter Fuertes[2], Roberto Andrade[3], Nicolay Samaniego Erazo[1], Jenny Torres[3] and Alyssa Cadena[2]

[1]*Universidad Nacional de Chimborazo, Riobamba, Ecuador*

[2]*Universidad de las Fuerzas Armadas ESPE, Quito, Ecuador*

[3]*Escuela Politécnica Nacional, Quito, Ecuador*

Keywords: CSIRT, Cybersecurity, Incident Management, Information Security, Privacy.

Abstract: The growth and evolution of threats, vulnerabilities, and cyber-attacks increase security incidents and generate adverse impacts on organizations. Nowadays, organizations have been strengthened in aspects of information security and information through the implementation of various technological solutions. Nevertheless, defined processes for the proper handling and coordinated management of security incidents should be established. In this paper, we propose an incident management framework that is adaptable to educational organizations and allows them to improve their management processes in the face of computer incidents. We introduce a coordination network with three levels of decision-making that defines interfaces and communication channels with supporting policies and procedures for coordination across processes and process actors. It enables different organizations to maintain focus on different objectives, to work jointly on common objectives, and to share information that supports them all in case of security incidents. Our model enables the examination of incident management processes that cross organizational boundaries, both internally and externally. This can help CSIRTs improve their ability to collaborate with other business units and other organizations when responding to incidents.

1 INTRODUCTION

During the last years, an increasing number of information security incidents have been reported (ENISA, 2017; ENISA, 2018). Besides minor errors with severe consequences, typical incidents include both general and single-purpose attacks caused by malware. Furthermore, the variety of attackers is wide which yield the threat landscape quite complex. The fact that new vulnerabilities and information security incidents occur occasionally is inevitable. Thus, it is evident that organizations, and in particular educational organizations, should have plans and procedures so that incidents can be handled when they occur. Therefore, the implementation of information security policies and controls in any type of organization is a must (Anderson et al., 2013).

Incident management is an umbrella term that comprises all activities for the entire incident lifecycle. These activities include from planning, training and raising awareness, to detecting, responding, and learning from incidents. An incident management capability includes an incident management policy, a plan, and procedures; all of which should be tailored to the specific needs of each organization (Hove et al., 2014). The existence of an incident response capability in organizations can assist them in rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services (Cichonski et al., 2012).

A challenging task for many organizations is planning and preparing for a cybersecurity incident. An organization should take immediate action when it occurs with the aim of mitigating threats to the confidentiality, integrity, and availability of its information assets. As the amount of incidents and threats in the network constantly grows, the concerned scientific and academic communities have been progressively developing methods to respond and mitigate them. Besides the establishment of communication strategies and the effective deployment of resources, several approaches has been proposed in the literature. In (Yang et al., 2016), the authors focus on the predictive aspect and low level inspection operations to eliminate vulnerabilities. The use of data mining techniques to perform trend analysis and behavior patterns is addressed in (Macas et al., 2017; Ahmad et al., 2012). In (Tisdale, 2015), the authors use an ad-

Tello-Oquendo, L., Tapia, F., Fuertes, W., Andrade, R., Erazo, N., Torres, J. and Cadena, A.
A Structured Approach to Guide the Development of Incident Management Capability for Security and Privacy.
DOI: 10.5220/0007753503280336
In *Proceedings of the 21st International Conference on Enterprise Information Systems (ICEIS 2019)*, pages 328-336
ISBN: 978-989-758-372-8

equate knowledge management, governance, and organizational psychology to solve issues related to cybersecurity. The proper use of information security managers, through systems protection, information security architecture and event management (SIEM) is tackled in (Gabriel et al., 2009). Also, the optimization of an intrusion detection system (IDS), such as Snort, as a tool to generate a large number of alerts is addressed in (Harang and Guarino, 2012).

Incident response is one of the functions performed in incident handling, and incident handling is one of the services provided as part of incident management. Some of the primary objectives of cybersecurity incident management are the following:

- Avoid cybersecurity incidents before they occur.
- Minimize the impact of cybersecurity incidents to the confidentiality, availability, or the integrity of the institutions' services, information assets, and operations.
- Mitigate threats and vulnerabilities as cybersecurity incidents are occurring.
- Improve cybersecurity incident coordination and management within the investment industry.
- Reduce the direct and indirect costs caused by cybersecurity incidents.
- Report findings to executive management.

Based on the above-mentioned objectives, this paper is an initial attempt to produce an incident management framework that is adaptable to educational organizations and allows them to improve their management processes in the face of computer incidents. Specifically, we describe an overall plan for handling information security incidents at organizations and evaluate how various factors contribute to the efficiency and effectiveness of organizations' incident management. By identifying how these factors affect successful incident management, we hoped to find improvements to incident management practice for most organizations and academic communities.

Furthermore, we define the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The main goal is to provide a plan and a set of actions to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

The remainder of the paper is structured as follows: Section 2 analyzes the role of incident management within the scope of information security management. Section 3 presents the proposed framework for incident management. Section 4 presents the discussion. Finally, Section 5 draws the conclusions and presents future work lines.

2 INCIDENT MANAGEMENT ROLE WITHIN INFORMATION SECURITY MANAGEMENT

Giving an accurate definition of incident management is difficult; it means different things to different communities. For instance, in the Information Technology Infrastructure Library (ITIL), *incident management* refers to the handling of any service disruption or interruption (Van Bon et al., 2010); in the International Standard for Information Security Incident Management (ISO/IEC 27035), it is the processes for detecting, reporting, assessing, responding to, dealing with, and learning from cybersecurity incidents (ISO/IEC 27035-1:2011, 2011). The scope of our *incident management* definition is preventing and handling computer security incidents. This includes identifying and minimizing the impact of technical vulnerabilities in software or hardware that may expose computing infrastructures to attacks or compromise, thereby causing incidents. Part of the inherent difficulty in defining the term *incident management* is defining the term *incident*, which is often derived based on organizational requirements and specifications. We consider a computer security incident as any adverse event which compromises some aspect of computer or network security as defined in (Brownlee and Guttman, 1998).

Distinguishing the boundary between information security management and incident management is open to interpretation and can be confusing, especially if the incident management scope includes processes for protecting infrastructures and detecting events using network monitoring and IDS. The dividing line often depends on the structure of an organization's security or incident management capabilities.

In agreement with related works in the area of information security management, in our model we view incident management as an integral component of information security management. Information security management encompasses all of the tasks and actions necessary to secure and protect an organization's critical assets, and this is much broader in scope than incident management. It involves aligning and prioritizing security actions based on the organization's mission and objectives and assessing security risks to achieving such objectives. It also involves establishing, configuring, operating, and maintaining

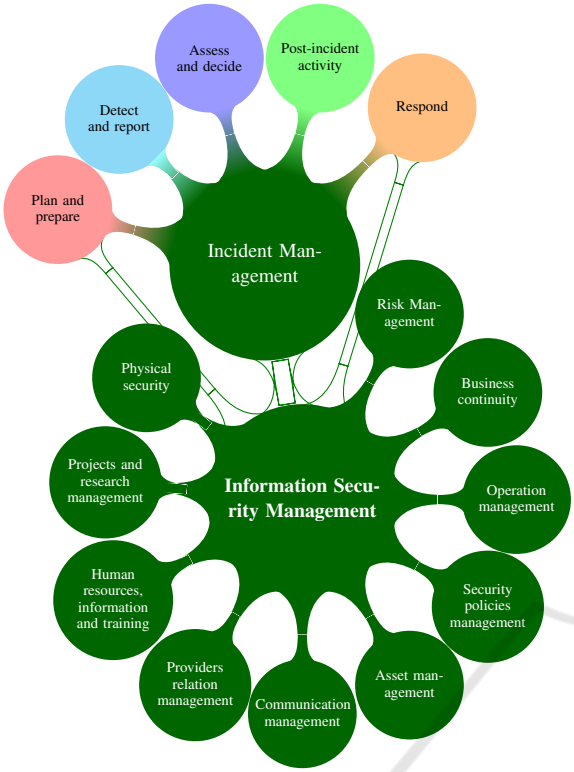

Figure 1: Overlap of information security management and incident management (NIST, 2013; ISO/IEC 27001:2013, 2013; Cichonski et al., 2012; ISO/IEC 27035-1:2011, 2011).

the organization's computing infrastructure in a secure manner and as a continuous process. Therefore, we consider that information security management includes risk management, business continuity, operation management, security policies management, assets management, communication management, providers relation management, human resources, information and training, projects and research management, physical security, and disaster recovery. Note that information security management comprises physical security to protect critical assets at the organization level and applies risk management approaches to help choosing the most effective course of action.

On the other hand, incident management may use several of these capabilities in the performance of its objectives, such as communication management, operation management, or security policies. Nevertheless, incident management is not responsible for establishing and maintaining these capabilities. Therefore, incident management is a component of information security management as depicted in Fig. 1; whereas information security management provides a framework within which the execution of incident management processes occurs.

If we examine the five high-level incident management processes (as detailed later in Section 3), we see that some of them intersect and overlap with information security management in some fashion. Fig. 1 illustrates how incident management processes fit into the scope of information security management. As can be seen, the *plan and prepare* processes are included in both incident management and information security management. In the former, the *plan and prepare* process addresses infrastructure changes in response to current computer security threats, whereas, in the latter, the *plan and prepare* process addresses a wider range of protection activities, including those necessary to configure and secure a computing infrastructure and maintain and monitor those configurations. The assess and decide, triage, and respond processes are totally within the scope of incident management, with regards to the treatment of computer security events and incidents.

Note that there are also several *plan and prepare* process actions that are beyond the scope of incident management, as described above. Additionally, Fig. 1 demonstrates the need for coordination and information sharing between business capabilities such as legal, human resources, and incident management. Furthermore, incident management touches many of the other functions, indicating the need for established channels of communication and collaboration.

3 PROPOSED MODEL FOR INCIDENT MANAGEMENT

Several standards and guidelines have been proposed to handle cybersecurity incidents; they have a number of similarities and have chosen to divide the incident management process into several phases. Most of them describe a preparation phase, where an incident management capability is built. All of the standards and guidelines have phases for detection, analysis, and incident responses, but the structure of these phases varies. All of them highlight lessons learned activities, even though not all describe a separate phase for this. Table 1 presents a brief comparison of the main guidelines and standards concerning incident management models in the literature.

In the following, we describe a structured approach based on five phases that aim at managing cybersecurity incidents. This proposed model resembles the structure offered by ISO/IEC (ISO/IEC 27035-1:2011, 2011) and NIST (Cichonski et al., 2012) that stand out as two of the primary standards and guidelines related to information security incident management. Both offer a structured approach to incident

Table 1: Comparison of Incident Management Models in International Standards and Guidelines (Ab Rahman and Choo, 2015).

	CERT/CC (West-Brown et al., 2003)	ITIL BIP 0107 (Van Bon et al., 2008)	ENISA (Maj et al., 2010)	ISO/IEC 27035 (ISO/IEC 27035-1:2011, 2011)	SANS (Kral, 2011)	NIST SP 80061 (Cichonski et al., 2012)
Relevant phases				Plan and prepare	Preparation	Preparation
	Reporting and detection	Incident detection and recording	Incident report registration	Detection and reporting	Identification	Detection and analysis
	Triage	Classification and initial support	Triage			
	Analysis	Investigation and diagnosis				
	Incident response	Resolution and recovery	Incident resolution	Responses	Containment, eradication, recovery	Containment, eradication, recovery
		Incident closure	Incident closure Post- Analysis	Lessons learned	Lessons learned	Post-incident activity
Mode	Reactive	Reactive	Reactive	Proactive	Proactive	Proactive

Figure 2: Structured approach based on five major sequence components of cybersecurity incident management.

management, including planning and preparing for incident response, what to do when incidents strike, and how to extract lessons learned afterward.

3.1 Structured Approach

Benefits from a structured approach to information security incident management include an overall improvement of information security, reduced impact of incidents, improved focus and better prioritization of security activities, and better and more updated information security risk assessment efforts (ISO/IEC 27035-1:2011, 2011; Cusick and Ma, 2010; Bustamante et al., 2017; Bustamante et al., 2016). The five major sequence components comprising this approach are: (1) plan and prepare, (2) detect and report, (3) assess and decide, (4) respond, and (5) post-incident activity. These phases are depicted in Fig. 2.

3.1.1 Plan and Prepare

In this phase, the organization should be in a state of readiness to minimize the impacts of security incidents and maintain the organization continuity (Taylor, 2013). The key activities in this phase include the following:

- Obtain support from senior management for the cybersecurity incident management plan.
- Establish a formal cybersecurity incident response capability to respond quickly and effectively when computer security defenses are breached.
- Establish a policy governing cybersecurity incident management that: describes which types of events should be considered incidents; establishes the organizational structure for incident response; defines roles and responsibilities; and lists reporting requirements.
- Develop incident response procedures.
- Establish policies and guidelines for internal and external cooperation and information sharing.
- Know the information assets that you are responsible for protecting.
- Implement controls to safeguard your organization's information assets. Possible controls include firewalls, patch management, and vulnerability assessments.
- Create an Incident Response Team (IRT) and conduct training for team members.
- Develop a communications plan and awareness training for the entire organization.
- Provide easy reporting mechanisms.
- Deploy endpoint security controls (e.g., anti-malware scanners) on information systems.
- Establish relationships with law enforcement agencies and other external Incident Response Teams.
- Perform evaluations, such as tabletop exercises, of the incident response capability.

3.1.2 Detect and Report

Preparation aims at minimizing incident risk; however, not all incidents can be prevented. It is, therefore, necessary to rapidly detect and report an incident occurrence. The key activities in this phase include the following:

- Monitor user reports of anomalous activities.
- Monitor alerts from internal security systems.
- Monitor information shared from peer organizations, vendors, and organizations who specialize in cybersecurity incidents.
- Monitor alerts from external information sources such as national incident response teams, law enforcement, etc.
- Look for signs of anomalous activities within systems or the network.
- Gather relevant information.
- Continue monitoring and detection.
- Escalate anomalous reports to the incident response team.

3.1.3 Assess and Decide

Incident analysis is then conducted to determine the report's validity (probably false alarm) and the potential impact(s) to the organization's core services and assets. Risk management (including risk assessment, mitigation, and evaluation) is the key to estimating the damage that such impacts can have on an organization. Furthermore, the results of risk assessment are needed to prioritize incident (if multiple incidents occur simultaneously). The key activities in this phase include the following:

- Assign a person who will be responsible for the event.
- Determine whether an event is actually a cybersecurity incident or a false alarm.
- If a cybersecurity incident has occurred, then escalation to the incident response team is required.
- Find out what information, system, or network is impacted.
- Find out what the impact is in terms of confidentiality, integrity, and availability.
- Notify the appropriate officials.
- Find out if your partners are being affected.

3.1.4 Respond

Once an incident has been detected and verified, an effective response reaction must be undertaken. Response should be generally a quick and effective reaction to an event to mitigate its harmful impacts as explained in (Baskerville et al., 2014). In this phase, the proactive degree is low which suggests that reactive activities are taking place. The key activities in this phase include the following:

- Assign internal resources and identify external resources in order to respond to the incident.
- Contain the problem, for example, by shutting down the system or disconnecting it from the network.
- Eradicate the malicious components of the incident, for example, by deleting malware or disabling a breached user account.
- Recover from the incident by restoring systems to normal operation and fixing the vulnerabilities to prevent similar incidents.
- If necessary, conduct a forensic analysis of the incident.

3.1.5 Post-incident Activity

Post-incident constitutes the final phase after an incident has been resolved. It is beneficial in improving security measures, and the cybersecurity incident handling process itself. It provides a chance to achieve closure concerning an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The degree of pro-activeness is switched to high as the relevant personnel must take the initiative to recognize and reflect new threats, and improve protection mechanisms. Information or results from this phase will be used as feedback to improve incident management. The key activities in this phase include the following:

- Identify the lessons learned from the cybersecurity incident.
- Identify and make improvements to the organization's security architecture.
- Review how effectively the incident response plan was executed during the cybersecurity incident.

3.2 The Role of CSIRTs Within Incident Management

Incident management is a process that involves several areas of an organization. In many cases, it includes participants from multiple divisions, who may have different organizational business drivers or missions (Fuertes et al., 2017). Balancing these different drivers effectively in the development and execution of an incident management plan can be challenging.

The term incident management also includes other services and functions that may be performed by CSIRTs, being these vulnerability handling, artifact handling, security awareness training, and the other services outlined in the CSIRT Services list as shown in Fig. 3. Including this expanded set of services is

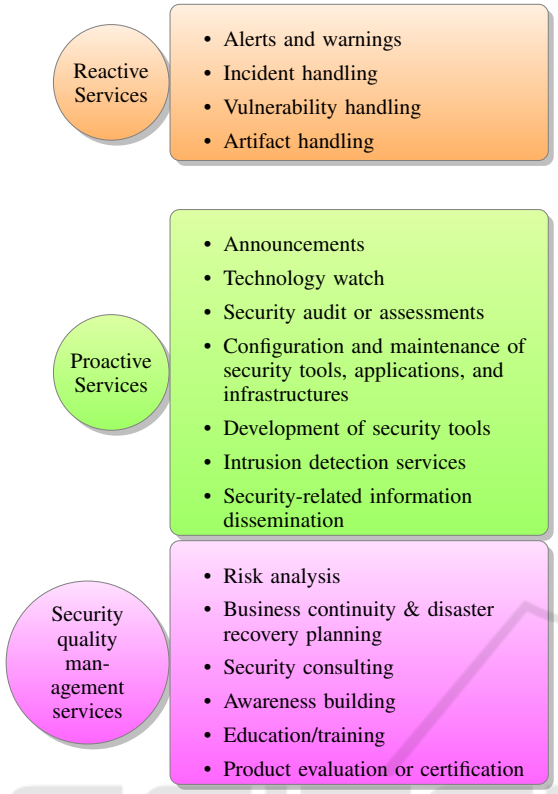

Figure 3: CSIRT services.

important since incident management is not just responding to an incident when it happens. It also includes proactive activities that help preventing incidents by providing guidance against potential risks and threats; for instance, identifying vulnerabilities in software that can be addressed before they are exploited. Training end users is also part of these proactive actions; it helps them to understand the importance of computer security in their daily operations and to define what constitutes abnormal or malicious behavior. By doing so, end users can identify and report this behavior.

Therefore, a CSIRT is one type of incident management capability that can take several roles. It can provide a set of comprehensive policies and procedures for analyzing, reporting, and responding to computer security incidents. Also, it can conform an ad hoc or crisis team with defined functions and responsibilities that is called together when an incident occurs. Furthermore, it can be an established or designated group that is given the responsibility for handling computer security events.

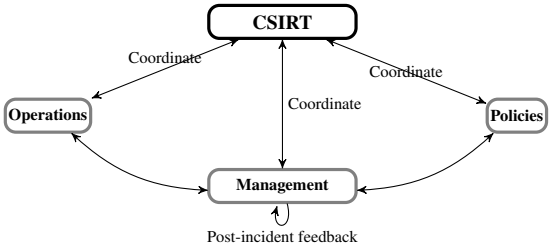

Figure 4: Scalable coordinated incident response model.

3.3 Coordination and Decision-making

Considering that the nature and quantity of simultaneous cyber events might yield large-scale cyber incidents that involve several CSIRTs, a crosscutting coordination network (Osorno et al., 2011; Daley et al., 2011) should be established for coordinated incident response. It has the following key characteristics:

- It enables different organizations to maintain focus on different objectives, to work jointly on common objectives, and to share information that supports them all.
- It is easily understood, tracked, and managed to reduce information overload at all levels.
- It enables rapid escalation and communication, both inside and outside an organization.

The underlying coordination network employs three levels of decision-making, two modes of communication, and the coordination activities, generally performed by a CSIRT, that tie them all together as illustrated in Fig. 4.

The three levels of decision-making, namely operations, management, and policy are defined by types of decisions, inputs and outputs, as well as the time frames in which those decisions usually are made. *Operations* include the immediate activities required to manage incidents; they are almost always concerned with whether a problem can be diagnosed and fixed immediately with resources at hand, or if it needs to be reported to other entities for their awareness or as a request for assistance or prioritization. *Management* includes those activities needed to prioritize and allocate resources to manage and respond to incidents, including the identification and reporting of critical incidents and the scope of coordination activities to address them. *Policy* is primarily concerned with the establishment and governance of effective business processes for managing incidents.

The two modes of communication, namely peer-to-peer and hierarchical are distinguished by whether they occur within a level or between levels. *Peer-to-peer* represents the communications within a

level (i.e., operator-to-operator, analyst-to-analyst, manager-to-manager, and so on). *Hierarchical* represents the communications between levels, that is the escalation of incident information and dissemination of directives or plans, as well as the flow of questions and answers between the layers.

4 DISCUSSION

The proposed model is a road-map that integrates the main processes or actions in the literature to build an overarching framework that outlines a methodology for planning, implementing, improving, and evaluating an incident management capability. It can be used by an organization to guide the development of their incident management capability.

Moreover, the proposed methodology identifies critical components for building consistent, reliable, and repeatable incident management processes. It includes a set of essential activities or criteria against which an organization can benchmark its current incident management processes. The results of such benchmarking can help an organization identify gaps and problem areas in its incident prevention and handling processes and plans.

As mentioned earlier, incident management is not just responding to an incident when it happens. It also includes proactive activities that help prevent incidents by providing guidance against potential risks and threats. Thus, incident management expands the scope of incident handling and incident response; it includes several CSIRTs' services or function including vulnerability handling, artifact handling, security awareness training, among others.

Given the persistent nature of many contemporary cybersecurity threats and related incidents that are simultaneously affecting multiple organizations, various sectors, or different types of organizations, coordination between CSIRTs is often required. Our model enables examination of incident management processes that cross organizational boundaries, both internally and externally. This can help CSIRTs improve their ability to collaborate with other business units and other organizations when responding to incidents.

Once implemented, the proposed model will provide a set of supporting materials that can be used by any organization. These materials include various components and guides that will help organizations to

- identify the issues and decisions that must be addressed in planning a new or expanding an existing incident management capability;
- identify the various components of such a capability and the various processes that should be in place to perform effective incident management;
- develop work-flows and tasks that can be followed to implement or improve the capability.

It is worth noting that the incident management processes introduced in our model are distributed in nature. It defines roles and responsibilities to ensure accountability; also, it defines interfaces and communication channels with supporting policies and procedures for coordination across processes and process actors. Furthermore, it can be integrated into other business and security management processes.

Currently, organizations, especially those of an educational nature, have a dynamic environment that entails new challenges such as the management of Internet of Things (IoT) devices, bring your own device (BYOD), geographical positioning information systems, use of social networks, surveillance systems, among others. This involves the handling of large amounts of data in real time, but above all, analyzing, understanding, and discovering hidden information that can affect the organization and the people who directly and indirectly interact with it.

A well-developed incident management capability is the foundation for implementing an architecture and infrastructure of solutions such as Big data and artificial intelligence applied to cybersecurity. Therefore, we consider as the next step the analysis of data analytics methodologies and architectures used in conjunction with decision support systems, which will allow organizations to take actions based on institutional knowledge. Also, proposing a Big data architecture and machine learning that can be used by different organizations on demand. For this, it is necessary to consider the governance of security in organizations using these new technological solutions, establish methods of communication between the interested parties, collaborative processes between the security groups of the organizations, procedures for the collection, aggregation and analysis of the data and the management of strategic indicators in cybersecurity considering the principles of personal privacy and information transparency.

5 CONCLUSIONS AND FUTURE WORK

We proposed an incident management framework based on a structured approach that include planning and preparing for incident response, what to do when incidents strike, and how to extract lessons learned

afterward. The aim of this framework is to give a thorough description of why and how organizations should plan for security incident management, conduct business impact analysis and explain various measures to improve information security in organizations. We also detailed the role of CSIRTs within the incident management. It can provide a set of comprehensive policies and procedures for analyzing, reporting, and responding to computer security incidents. Our proposed model defines roles and responsibilities to ensure accountability; also, it defines interfaces and communication channels with supporting policies and procedures for coordination across processes and process actors in a distributed manner. Furthermore, it can be integrated into different types of organizations and security management processes. As future work, we plan to analyze data analytics methodologies and architectures used in conjunction with decision support systems, which will allow organizations to take actions based on institutional knowledge. We aim at implementing an architecture and infrastructure of solutions such as Big data and artificial intelligence applied to cybersecurity.

ACKNOWLEDGMENTS

The authors would like to thank the financial support of the Ecuadorian Corporation for the Development of Research and the Academy (RED CEDIA) for the development of this work, under Project Grant GT-II-2018 (Cybersecurity).

REFERENCES

Ab Rahman, N. H. and Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, 49:45–69.

Ahmad, A., Hadgkiss, J., and Ruighaver, A. B. (2012). Incident response teams–challenges in supporting the organisational security function. *Computers & Security*, 31(5):643–652.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., and Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy*, pages 265–300. Springer.

Baskerville, R., Spagnoletti, P., and Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, 51(1):138 – 151.

Brownlee, N. and Guttman, E. (1998). Expectations for computer security incident response. Technical report.

Bustamante, F., Fuertes, W., Díaz, P., and Toulkeridis, T. (2016). A methodological proposal concerning to the management of information security in Industrial Control Systems. In *Ecuador Technical Chapters Meeting (ETCM), IEEE*, pages 1–6. IEEE.

Bustamante, F., Fuertes, W., Díaz, P., and Toulkeridis, T. (2017). Integration of IT frameworks for the management of information security within industrial control systems providing metrics and indicators. In *Electronics, Electrical Engineering and Computing (INTERCON), 2017 IEEE XXIV International Conference on*, pages 1–4. IEEE.

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, 800(61):1–147.

Cusick, J. J. and Ma, G. (2010). Creating an itil inspired incident management approach: Roots, response, and results. In *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP*, pages 142–148. IEEE.

Daley, R., Millar, T., and Osorno, M. (2011). Operationalizing the coordinated incident handling model. In *Technologies for homeland security (HST), 2011 IEEE international conference on*, pages 287–294. IEEE.

ENISA (2017). Annual Incident Reports 2016. Technical report, European network and information security agency (ENISA).

ENISA (2018). Annual Report Telecom Security Incidents 2017. Technical report, European network and information security agency (ENISA).

Fuertes, W., Reyes, F., Valladares, P., Tapia, F., Toulkeridis, T., and Pérez, E. (2017). An Integral Model to Provide Reactive and Proactive Services in an Academic CSIRT Based on Business Intelligence. *Systems*, 5(4):52.

Gabriel, R., Hoppe, T., Pastwa, A., and Sowa, S. (2009). Analyzing malware log data to support security information and event management: Some research results. In *2009 First International Conference on Advances in Databases, Knowledge, and Data Applications*, pages 108–113. IEEE.

Harang, R. and Guarino, P. (2012). Clustering of snort alerts to identify patterns and reduce analyst workload. In *MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012*, pages 1–6. IEEE.

Hove, C., Tarnes, M., Line, M. B., and Bernsmed, K. (2014). Information security incident management: identified practice in large organizations. In *IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on*, pages 27–46. IEEE.

ISO/IEC 27001:2013 (2013). Information technology – Security techniques – Information security management systems – Requirements . Standard, International Organization for Standardization, Geneva, CH.

ISO/IEC 27035-1:2011 (2011). Information technology – Security techniques – Information security incident management . Standard, International Organization for Standardization, Geneva, CH.

Kral, P. (2011). The incident handlers handbook.

Macas, M., Lagla, L., Fuertes, W., Guerrero, G., and Toulkeridis, T. (2017). Data mining model in the discovery

of trends and patterns of intruder attacks on the data network as a public-sector innovation. In *2017 Fourth International Conference on eDemocracy eGovernment (ICEDEG)*, pages 55–62.

Maj, M., Reijers, R., and Stikvoort, D. (2010). Good practice guide for incident management. *European network and information security agency (ENISA)*.

NIST (2013). Security and privacy controls for information systems and organizations. *NIST Special Publication*, 800(53):1–462.

Osorno, M., Laurel, M., Millar, T., Team, E. R., and Rager, D. (2011). Coordinated cybersecurity incident handling. *)ˆ(Eds.):'Book Coordinated Cybersecurity Incident Handling'(2011, edn.)*.

Taylor, L. P. (2013). Chapter 11 - developing an incident response plan. In Taylor, L. P., editor, *FISMA Compliance Handbook*, pages 95 – 115. Syngress, Boston.

Tisdale, S. M. (2015). Cybersecurity: Challenges from a systems, complexity, knowledge management and business intelligence perspective. *Issues in Information Systems*, 16(3).

Van Bon, J., De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., and Verheijen, T. (2008). *Foundations of IT Service Management Based on ITIL®*, volume 3. Van Haren.

Van Bon, J., De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., and Verheijen, T. (2010). *ITIL®*, volume 3. Van Haren.

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., and Ruefle, R. (2003). Handbook for computer security incident response teams (CSIRTS). Technical report, Carnegie-mellon univ pittsburgh pa software engineering inst.

Yang, J., Ryu, D., and Baik, J. (2016). Improving vulnerability prediction accuracy with secure coding standard violation measures. In *Big Data and Smart Computing (BigComp), 2016 International Conference on*, pages 115–122. IEEE.