Cybersecurity Management for Incident Response

Alin Zamfiroiu
The Bucharest University of Economic Studies, Bucharest, Romania
National Institute for Research and Development in Informatics, Bucharest, Romania
alin.zamfiroiu@ici.ro

Ramesh C Sharma
Dr B R Ambedkar University Delhi, New Delhi, India
rcsharma@aud.ac.in

Abstract: In information technology, security is the protection of information assets through the use of technology, processes and training. There will always be situations of attack on software systems but the software must continue to work properly under such potential risks. The security process assumes and is required to provide three important elements: integrity, authentication, and availability. Security is a set of processes and techniques implemented to protect private information in electronic or printed format against modification, destruction or unauthorized access. This paper discusses effective management of cybersecurity for incident response.
Keywords: Information Security, Cybersecurity, Threats, Detection, Incident Response

INTRODUCTION

Software security is an important dimension of engineering software so that it continues to function properly under malicious attacks. Meng et al. (2018) noted the difficulty in creating a secure system around existing computer architectures. One of the reasons is the increasing complexity of the software which may invite exploitative software vulnerabilities. The attacks have two important issues: (a) Variety of means, for example, worms, botnets, trojans etc. Not only the software but even the hardware vulnerabilities can also be exploited. (b) Range of attack, it can be from any place and from any layer of physical hardware to application software, for example Cross-site Request Forgery (Lin et al., 2009).

The five stages of security are presented in Figure 1: evaluation, prevention, detection, response and recovery.

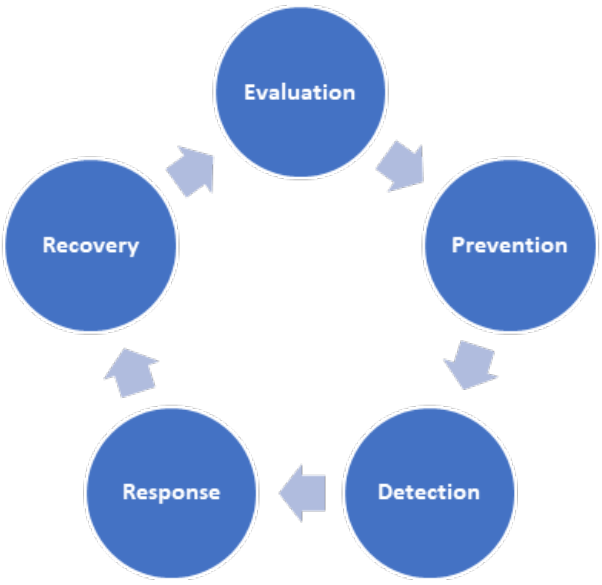

Fig 1.: *The stages of security assurance*

http://doi.org/10.54851/v4i1y202208

Security aims to identify and assess security risks with objectives:

- prevention of security breaches and incidents, in particular major accidents (Stajano, 2002);
- minimizing business interruptions caused by unwanted incidents;
- maintaining the integrity, functionality and availability of information to users;
- develops and maintains the necessary protection against theft, loss, damage or unauthorized alteration;
- developing and maintaining the necessary response capacity in emergency situations;
- the capacity required to continue operations in the event of major incidents;
- minimize the impact and restoration time in case of security incidents;
- efficient management of security risks;
- ensuring the continuity of the activity;
- compliance with the laws and regulations that are in force.

INCIDENT RESPONSE FUNDAMENTALS

A computer security incident is any real or suspected adverse event related to the security of your system or computer networks (Choi, 2020). One of the strong dimensions of security is resilience, which allows us to identify, detect, prevent and react to the technological or process failure with the purpose to avoid or minimize the damage originating from service failure (Nogueira et al., 2009).

A security incident can be defined as the result of a network or host activity that threatens the security of an existing computer system. Each organization will need to define what a computer security incident represents for their site and its structure.

Examples of incidents include the following activities:

- Attempts to gain unauthorized access to a system or to data from this system (Shulman & Waidner, 2014);
- Unwanted disruption or refusal of service (Hacks, Katsikeas, Ling et al., 2020);
- Unauthorized using of the system to process some data changes to system hardware, or software features without the knowledge of the owner of this system (Morikawa & Yamaoka, 2011);
- When a security incident is reported to an organization's customer site, the organization must handle the incident responsibly (Noel et al., 2009).

Signs of an incident can fall into one of two categories:

- Precursors;
- Indicators.

A precursor is considered to be a sign that an incident regarding the system may occur in the future.

An indicator is considered to be a sign that an incident has occurred or may occur on the system at this time.

Most possible attacks that can be realized do not have identifiable or detectable signs or precursors from a target perspective. If some precursors are detected in time, the organization may have the opportunity to organize and to prevent the incident by changing its security position to save an attack target (Paja, Dalpiaz, & Giorgini, 2015).

At the very least, the organization could monitor more closely the activity involving the target (Ferrillo, 2015).

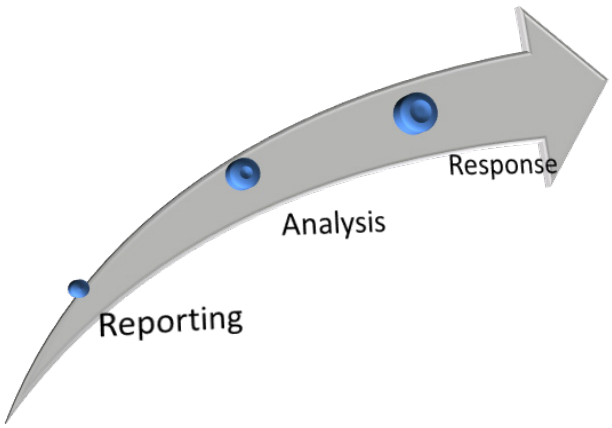

Fig 2.: *Handling Incidents*

Incident handling includes three functions:

- incident reporting;
- incident analysis;
- incident response.

The incident reporting feature allows a CERT to serve as a central point of contact for reporting local issues.

This allows all incident reports and activity to be collected at the location where the information can be reviewed and correlated within the parent organization or constituency.

This information can then be used to determine intruder activity trends and patterns and to recommend appropriate prevention strategies for the entire constituency.

The other part of the incident analysis involves a detailed analysis of the incident report or activity to determine the purpose, priority and threat of the incident, as well as research into possible response and mitigation strategies.

A CERT may send recommendations for recovery, retention, and prevention to constituents or systems and network administrators on sites that then perform the response steps themselves.

A CERT can also perform these steps on the affected systems.

The response may also involve the exchange of information and lessons learned with other response teams and other appropriate organizations and sites.

PRINCIPLES OF CYBERSECURITY MANAGEMENT

Cybersecurity is a management issue. Principles of the cybersecurity management are presented in Figure 3 and in (The Six Principles of Cyber Security, n.d.).

A. Security Beyond Firewall

- It is important to be achieved a scanning network trac on various OSI layers to assure the network security.
- Some tools are able to look and analyze the suspicious patterns of trac to identify and protect the system against some kind of actions.

B. Advanced Access Management

- An advanced management solution should be implemented and the systems should be accessed through it.
- In our days, a simple combination of username and a password is no secure enough.

C. Enhanced Application Security

- All used systems should be secured with an antivirus solution.
- Enhanced application security consists of two additional measures:
  - security driven release management – the applications should be updated for security reasons;
  - pattern behavior recognition in the application that permit continue authentication by using the user behavior.

D. Trusted Attack Simulation

- Is very important to have a team of ethical hackers that identify the vulnerabilities of the system.
- Trusted Attack Simulation, simulates attacks from outside and inside the system, and gives a report that identifies potential security holes in the system.

E. Data Encryption

- Any data can be stolen, both when it is in transit to the system, or directly from the servers and database storage, where the data is at rest.
- The data encryption principle addresses the objective to provide a mechanism for two entities or people to communicate between them without any other third party being able to understand their messages.

F. Compliance Business Framework

- Is very important for any company to develop its Compliance Business Framework (CBM) for security if it uses data from internal sources, a cloud, or any third-party provider, needs.
- These compliances are linked to other compliances policies such as ISO9001, ISO27001 or other.

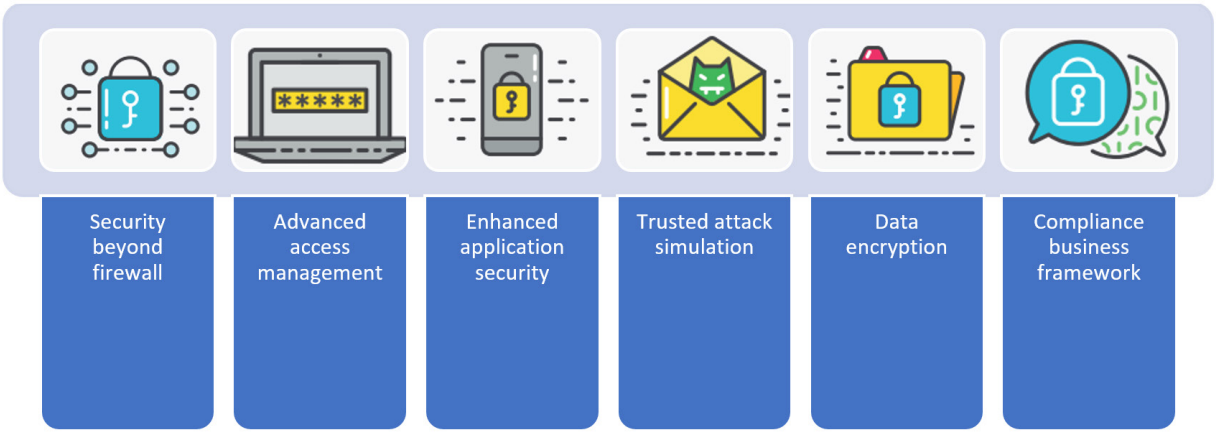

Fig 3.: Principles of cybersecurity management

ITEMS OF CYBERSECURITY MANAGEMENT

The management are required to steadily drive cybersecurity measures by giving directions on the ten important items. These ten items are presented below. For each one we have the definition, The scenario if nothing is done and some actions recommended:

A. Recognize a cybersecurity risk and develop company-wide measures

Definition: Recognize cybersecurity risk as one important element among a variety of management risks and develop a company-wide policy (security policy).

Scenario if nothing is done: Without cybersecurity policy developed and announced by management, each security measures implemented will be inconsistent with the corporate strategy.

Recommended actions: Develop a security policy taking cybersecurity risks into consideration. The security policy should be posted somewhere that is easily accessible to employees. By publicly announcing the security policy, the company will be able to show its security posture to stakeholders and society and increase trust from them.

B. Build a management system for cybersecurity risk

Definition: Establish a structure for cybersecurity risk management.

Scenario if nothing is done: Without a structure for cybersecurity risk management, it is impossible for an entire company to identify cybersecurity risks. There is a risk of inconsistency between the cybersecurity risk management policy and the overall risk management policy.

Recommended actions: Establish a cybersecurity management structure and define its scope of responsibility. Participate in a corporate risk management committee in the organization. The cybersecurity risk management structure should cover plan/design phase as well as later phases.

C. Secure resources (budget, workforce etc.) for cybersecurity measures

Definition: Secure the budget to implement measures for cybersecurity risks and provide training for cybersecurity personnel.

Scenario if nothing is done: It would be difficult to implement cybersecurity measures; it is impossible to retain talented human resources within an organization.

Recommended actions: Secure the budget necessary for necessary cybersecurity measures. Secure a budget for training of employees and personnel (Social Engineering). Consider using security training provided by external organizations.

D. Identify cybersecurity risks and develop plans to address them.

Definition: Develop a strategic plan for cybersecurity risks from the threat of cyber-attacks.

Scenario if nothing is done: Such measures will only increase tasks for the employees if the organization doesn't have proper risk management measures. Any unacceptable remaining risk might cause unexpected loss.

Recommended actions: Identify cybersecurity risks related to the information that should be protected; Implementation of risk reduction measures; Implementation of risk transfer measures; Consider cybersecurity measures from planning stage of a software product.

E. Establish systems to effectively address cybersecurity risks

Definition: The system should implement the protection measures in order to address cybersecurity risks.

Scenario if nothing is done: Damage may spread when a cyber-attack occurs. It is impossible to grasp the overview of the cyberattack when this one occurs.

Recommended actions: Implement multi-layer defense; Segregate network segments as necessary by switches or firewalls; Perform a vulnerability diagnosis to detect system vulnerabilities and fix them; Train employees to report if they receive a suspicious email.

F. Implement a PDCA cycle for cybersecurity measures

Definition: PDCA – Plan, Do, Check, Act. The measures that should be implemented have to respect this cycle. Disclose the status of measures to enhance the trust of stakeholders.

Scenario if nothing is done: If this cycle is not respected there is risk that a plan might not be surely executed. Failure in these efforts might lead to the inability to cope with changes in the cybersecurity environment.

Recommended actions: Develop a PDCA cycle in order to respond continuously to cybersecurity risks. Modify the policy as needed when a new cybersecurity risk is identified. Detect and resolve any issues regarding the current system and cybersecurity measures.

G. Develop a cybersecurity incident response team and relevant procedures

Definition: It is important to be established a CSIRT in the organization to identify the scope of impact and damages of a cybersecurity attack.

Scenario if nothing is done: There will be communication difficulties with internal and external stakeholders. There is risk of damage spreading to customers and business partners and consequently the possibility of being liable for their damage. There will possibly be legal penalty.

Recommended actions: Conserve evidence such as various logs and devices infected with malware after being victimized by a cyber-attack. Execute drills in preparation for cyber-attacks including developing measures to prevent similar incidents. Prepare a list of emergency contacts. Report to management the status of damage and impact to other companies due to the incidents.

H. Develop a recovery team and relevant procedures in preparation for damage due to cyber incidents

Definition: Create a recovery procedure manual and develop a structure for recovery.

Scenario if nothing is done: Without practical procedures, personnel may not be able to act appropriately in unforeseen situations.

Recommended actions: Give employees directions to do recovery tasks in cooperation with relevant organizations for prompt recovery in case of a cyber-attack. Align the recovery goal with an organizational plan.

I. Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies

Definition: A complete cycle of cybersecurity measures should cover more companies or business partners.

Scenario if nothing is done: If there are vulnerable points in some companies from the group, the company might be attacked via those weak partners, and possibly, the company could cause collateral damage to other companies.

Recommended actions: A contract should be made after clearly understanding measures deployed in the partner. Reports on the status of cybersecurity measures (including audits) from the all partners should be shared to all partners.

J. Gather, utilize, and provide cyber-threat information through information sharing activities

Definition: In order for the whole society to have capability against latest cyber-

attacks, participate in information sharing activities on cyber-attacks. Additionally, develop environments to effectively utilize the information obtained.

Scenario if nothing is done: If information on a specific cyber-attack is not shared among companies, each company needs to fight against the same cyber-attack individually and it will increase cybersecurity cost in each company.

Recommended actions: It is needed to protect the whole society, not company by company, from cyber-attacks through mutual information shared among organizations. The employees should report any information on malware and unauthorized access to the organization management team based on the regulations.

CONCLUSIONS

The challenges to the field of incident prevention are increasing continuously because of constant evolving of attacks as they are getting more sophisticated.

The software engineers respond to such incidences in most cases once they are discovered. Meng et al. (2018) proposed developing Security-first Architecture using Active Security Processors. Such Active Security Processors have unidirectionally access to all resources of computation processors and can detect malevolent activities in the system. In the recent times, certain security incidents, for example, PRISM (Gellman & Poitras, 2013), WannaCry (Ehrenfeld, 2017), Meltdown (Lipp et al. 2018) and Spectre (Kocher et al., 2018) have brought the security weakness to the limelight. Not only the software, but also the hardware is unsafe (Liu et al., 2015). The growth in the field of ubiquitous computing (Weiser, 1993), Wireless Sensor Networks (Estrin, 1999), Internet of Things (Ashton, 2009), Wearables (Mann, 1997) and Cyber-Physical Systems (Rajkumar et al., 2010) have produced new kind of challenges. In this paper we have proposed certain measures for effective cybersecurity management, like, recognize a cybersecurity risk and develop company-wide measures; build a management system for cybersecurity risk; secure resources (budget, workforce etc.) for cybersecurity measures; identify cybersecurity risks and develop plans to address them; establish systems to effectively address cybersecurity risks; implement a PDCA cycle for cybersecurity measures; develop a cybersecurity incident response team and relevant procedures; develop a recovery team and relevant procedures in preparation for damage due to cyber incidents; understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies; and gather, utilize, and provide cyber-threat information through information sharing activities.

REFERENCE LIST

Ashton, K. (2009). That 'Internet of Things' Thing. Radio Frequency IDentification Journal; 22:97–114.

Buchanan, B. (1999). Data Encryption Principles. In: *Handbook of Data Communications and Networks*. Springer, Boston, MA. Available at: <https://doi.org/10.1007/978-1-4757-0905-6_15>.

Choi, Y. H., Liu, P., Shang, Z. et al. (2020). Using deep learning to solve computer security challenges: a survey. *Cybersecur 3*, 15. Available at: <https://doi.org/10.1186/s42400-020-00055-5>.

Cybersecurity Management Guidelines, ver 2. (Minister of Economy, Trade and Industry). Information-technology Promotion Agency, Japan (IPA).

Ehrenfeld, J. M. (2017). Wannacry, cybersecurity and health information technology: A time to act, *Journal of Medical Systems 41*(7):101.

Estrin, D., Govindan, R., Heidemann, J. S. & Kumar, S. (1999). Next century challenges: Scalable coordination in sensor networks. In: MobiCom'99. New York: ACM. p. 263–70.

Ferrillo, P. A. (2015). *Navigating Cybersecurity Storm*. Available at: <http://cybersecuritysummit.com/wp-content/uploads/2015/12/navigatingcybersecuritystorm-paulferrillo.pdf>.

Gellman, B., & Poitras, L. (2013). US intelligence mining data from nine U.S. internet companies in broad secret program. *The Washington Post*. Available at: <https://www.sanders.senate.gov/newsroom/must-read/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program>.

Hacks, S., Katsikeas, S., Ling, E. et al. (2020). powerLang: a probabilistic attack simulation language for the power domain. *Energy Informatics* 3, 30. Available at: <https://doi.org/10.1186/s42162-020-00134-4>.

<https://cert.societegenerale.com/resources/files/IRM-1-Worm-Infection.pdf>

<https://aisn.net/5-cybersecurity-incident-response-steps/>

<https://fireh7nter.com/2020/08/04/incident-response-methodology-and-case-study/>

<https://digitalguardian.com/blog/what-security-incident-management-cybersecurity-incident-management-process>

<https://www.computerweekly.com/tip/10-security-incident-management-best-practices>

<https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf>

<https://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542>

Kocher, P., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M. & Yarom, Y. (2018). Spectre attacks: Exploiting speculative execution. *ArXiv e-prints*. Available at: <https://spectreattack.com/spectre.pdf>.

Lin, X., Zavarsky, P., Ruhl, R. & Lindskog, D. (2009). Threat modeling for CSRF attacks In: International Conference on Computational Science and Engineering (pp. 486–491). IEEE, Vancouver.

Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., Kocher P, Genkin, D., Yarom, Y. & Hamburg, M. (2018). *Meltdown. ArXiv e-prints*. Available at: <https://meltdownattack.com/meltdown.pdf>.

Liu, F., Yarom, Y., Ge, Q., Heiser, G. & Lee, R.B. (2015). Last-level cache side-channel attacks are practical In: *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 605–622). IEEE, San Jose.

Mann, S. (1997). Wearable computing: A first step toward personal imaging. *Computer 30(2)* (pp.25–32).

Meng, D., Hou, R., Shi, G. et al. (2018). Security-first architecture: deploying physically isolated active security processors for safeguarding the future of computing. *Cybersecurity 1, 2.* Available at: <https://doi.org/10.1186/s42400-018-0001-z>.

Morikawa, I. & Yamaoka Y. (2011). Threat tree templates to ease difficulties in threat modeling, *14th International Conference on Network-Based Information Systems, 2011* (pp. 673–678). IEEE, New York. Available at: <https://doi.org/10.1109/NBiS.2011.113>.

Noel, S., Elder, M., Jajodia, S., Kalapa, P., O'Hare, S. & Prole, K. (2009) Advances in topological vulnerability analysis In: Conference For Homeland Security, 2009. CATCH '09. Cybersecurity Applications Technology, 124–129. IEEE, New York. Available at: <https://doi.org/10.1109/CATCH.2009.19>.

Nogueira, M., dos Santos, A. L. & Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks, *IEEE Commun Surv Tutor. 11*(1): 66–77.

Paja, E., Dalpiaz, F., Giorgini, P. (2015). Modelling and reasoning about security requirements in socio-technical systems. Data Knowl Eng 98:123–143.

Rajkumar, R.R., Lee, I., Sha, L. & Stankovic J. (2010). Cyber-physical systems: the next computing revolution. 47*th Design Automation Conference*. ACM: 2010.

Shulman, H. & Waidner, M. (2014). DNSSEC for cyber forensics. EURASIP Journal on Information Security 2014, 16. Available at: <https://doi.org/10.1186/s13635-014-0016-2>.

Syed, R. (2020). Cybersecurity Vulnerability Management: A Conceptual Ontology and Cyber Intelligence Alert System, *Information & Management*, 103334.

Stajano F. (2002). Security for ubiquitous computing. Hoboken: Wiley.

Neos IT. (n.d.). The Six Principles of Cyber Security. Available at: <https://blog.neosit.com/en/the-six-principles-of-cyber-security>.

Weiser, M. (1993). Some computer science issues in ubiquitous computing. C*ommunications of the ACM 36(7)*:75–84.