Cybersecurity: Practice

Chapter · March 2019

DOI: 10.1007/978-3-319-69891-5_81-1

CITATIONS
0

READS
53

1 author:

George Grispos
University of Nebraska at Omaha
30 PUBLICATIONS **368** CITATIONS

SEE PROFILE

C

Cybersecurity: Practice

George Grispos
School of Interdisciplinary Informatics,
University of Nebraska Omaha,
Omaha, NE, USA

Keywords
Cybersecurity · Best practices · Standards · Policies · Guidelines

Definition

Cybersecurity involves the application and management of techniques with the aim of protecting the confidentiality, integrity, and availability of information and information assets in cyberspace.

Introduction

The widespread use of electronic information processing coupled with the emergence of business conducted through the Internet has fueled the need for organizations to protect proprietary and customer information from malicious cyber actors and nations (Grispos et al. 2017). As a result, many organizations have recognized the importance of implementing effective cybersecurity practices. According to the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), cybersecurity encompasses the preservation of confidentiality, integrity, and availability of information in cyberspace (International Organization for Standardization/International Electrotechnical Commission 2012). Confidentiality refers to "the protection of sensitive information from unauthorized disclosure" (Peltier 2013). Integrity is defined as "the accuracy, completeness, and validity of information in accordance with business values and expectations" (Peltier 2013). Availability relates to "information being available when required by the business process now and in the future" (Peltier 2013). Collectively, *confidentiality*, *integrity*, and *availability* are referred to as the CIA triad. An organization's cybersecurity objectives should be to protect the confidentiality, integrity, and availability of information and information assets within its distinct cyberspace. Various approaches can be taken to achieve this objective including through the implementation of security controls; enforcing security polices, standards, and guidelines; using risk management approaches; as well as, education and training initiatives. These approaches have existed and matured over several decades and have been classified in terms of generational waves.

Cybersecurity Waves

As part of a wider analysis into cybersecurity practices within organizations, Von Solms (2000,

L. R. Shapiro, M-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-69891-5_81-1

2006) separated the evolution of cybersecurity countermeasures within organizations into four generational "waves". The first generation of cybersecurity countermeasures existed up until the early 1980s and can be characterized as the "Technical Wave". In this generation, cybersecurity countermeasures focused on mainframes and data centers, where solutions focused on enhancing the cybersecurity of the operating system through access control lists, user IDs, and the use of passwords. In addition, physical security barriers were also the norm. The second generation of countermeasures (the "Management Wave"), lasted from the early 1980s to the mid-1990s and emerged with management within organizations realizing that security was no longer just a technical issue. Hence, organizations needed to develop cybersecurity policies and procedures and integrate managers and executives in the security decision-making process. The third generation of countermeasures (the "Institutional Wave") started in the mid-1990s and continued into the early 2000s. This wave is characterized by the demand for organizations to implement cybersecurity standards and best practices. As a result, many organizations looked to implement standards and best practices such as the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 standard. The fourth-generation wave (Von Solms 2006) (the "Information Security Governance Wave") developed at the turn of the millennium and emerged as a result of new legal and regulatory requirements dictating that organizations implement cybersecurity policies and processes to protect information and information systems. Therefore, this wave defines that an organization's security governance is included and part of its overall corporate governance posture.

Cybersecurity Programs

In an effort to address their cybersecurity objectives, many organizations have chosen to implement *cybersecurity programs (Grispos* et al. 2013*)*. The primary objective of a cybersecurity program is to protect the CIA triad while also ensuring that any legal and regulatory requirements are also fulfilled. Several organizations and government agencies, such as the National Institute of Standards and Technology (NIST), the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), and the Internet Engineering Task Force (IETF), have published frameworks, processes, and best practice guidelines describing how organizations can reduce cybersecurity risk and enhance their security posture.

The NIST Cybersecurity Framework

In February 2013, the President of the United States issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity. In particular, the Executive Order called for the development of a risk-based Cybersecurity Framework including industry standards and best practices to help organizations manage and mitigate cybersecurity risks. NIST answered this call to arms by publishing in 2014 a document called the "Framework for Improving Critical Infrastructure Cybersecurity," which has since been updated in 2018 (National Institute of Standards and Technology 2018). To achieve these objectives, NIST have published a series of documents, called Special Publications (SPs), that can be used either collectively or individually to secure information assets. These documents include:

- SP 800–12 provides an overview of cybersecurity security and emphasizes the importance of the cybersecurity controls and the different ways to implement them.
- SP 800–14 describes common security principles that are used and that should be incorporated within a cybersecurity policy. These guidelines can be used to enhance existing policies and develop new policies.
- SP 800–37 provides a risk-based approach called the "Risk Management Framework." The publication provides guidelines on applying the Framework to information systems with the aim of identifying what security controls are needed, how they can

be implemented, and how security control effectiveness can be assessed.
- SP 800–53 specifically describes 194 security controls that could be applied to an information system in order to enhance the security and privacy of both the system and the information that can reside within the system itself.

It must be noted that while NIST has developed and published the Framework and SPs with the aim of securing critical infrastructure and federal government information systems, any organization is free to use this approach to establish a minimum security-control baseline within their specific environments (Ross 2007).

ISO/IEC 27000 Family of Standards

The ISO/IEC 27000 family of standards are an alternative set of practices that can be applied to mitigate cybersecurity attacks. The last major revision to these standards was published in 2013. While there are nearly 50 standards in the 27000 family, two main standards called ISO/IEC 27001 and ISO/IEC 27002 are considered the baseline for cybersecurity management. The ISO/IEC 27001 standard specifies how an organization can develop and implement an Information Security Management System (ISMS). An ISMS is defined as "the policies, procedures, guidelines, associated resources, and activities, collectively managed by an organization, in the pursuit of protecting its information assets" (International Organization for Standardization/International Electrotechnical Commission 2014). Similarly, Eloff and Eloff define an ISMS as "used for establishing and maintaining a secure information environment" (Eloff and Eloff 2003). Regardless, once an organization has met the requirements specified in ISO/IEC 27001, it can become certified following the successful completion of an audit to determine it complies with the standard. The ISO/IEC 27001 standard recommends that organizations use an improvement process such as Plan-Do-Check-Act (PDCA) or Six Sigma's Define, Measure, Analyze, Improve, and Control as a method for designing, implementing, and reviewing an ISMS within their respective organization.

Within the above methods, organizations are required to identify and assess cybersecurity risks and then select appropriate security controls. ISO/IEC 27002 is a standard that provides security control recommendations, which can be used during the initiation, implementation, and maintenance of secure systems. SO/IEC 27002 consists of fourteen security domains, which cover cybersecurity control information including security policies, asset management, human resource security, business continuity management, and operations security (International Organization for Standardization/International Electrotechnical Commission 2013). The idea behind ISO/IEC 27002 is that the security controls can be applied to various organizations, irrespective of type, size, risks, or the threats faced by the organization. Hence, the range of security controls covered in the standard can also provide an organization with some flexibility to adopt only the controls that they require within their distinct environment.

IETF Request for Comments (RFC) 2196

RFC 2196 is a cybersecurity standard, formally called "Site Security," published by the Internet Engineering Task Force (IETF). The standard that was published in 1997 is intended to guide organizations during the development of cybersecurity policies and procedures to protect systems connected on the Internet. While the document might appear outdated, much of the information and practical guidance is still very much relevant to organization trying to secure their information and information assets. A range of cybersecurity subjects are covered in RFC 2196 including Firewall implementation, network security, security incident handling, policy development, and risk management.

Other Cybersecurity Practices

Depending on its type, an organization may decide to implement cybersecurity practices that have been specifically developed for its particular domain. For example, the Payment Card Industry Data Security Standard (PCI-DSS) was developed

by a number of major credit card companies. The purpose of PCI-DSS is to provide consistent security controls for organizations around the world that manage, handle, and storage payment card information. At the time of writing, the current version of PCI-DSS (Version 3.2.1) was released in May 2018. Changes are usually made to the standard every 3 years. PCI-DSS specifies twelve requirements, which are organized into six control objectives (PCI Security Standards Council 2018):

1. **Build and Maintain a Secure Network and Systems**
   Requirement 1: Install and maintain a firewall configuration to protect cardholder information.
   Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
2. **Protect Cardholder Data**
   Requirement 3: Protect stored cardholder data.
   Requirement 4: Encrypt transmission of cardholder data across open, public networks.
3. **Maintain a Vulnerability Management Program**
   Requirement 5: Protect all systems against malware and regularly update antivirus software or programs.
   Requirement 6: Develop and maintain secure systems and applications.
4. **Implement Strong Access Control Measures**
   Requirement 7: Restrict access to cardholder data by business need to know.
   Requirement 8: Identify and authenticate access to system components.
   Requirement 9: Restrict physical access to cardholder data.
5. **Regularly Monitor and Test Networks**
   Requirement 10: Track and monitor all access to network resources and cardholder data.
   Requirement 11: Regularly test security systems and processes.
6. **Maintain an Information Security Policy**
   Requirement 12: Maintain a policy that addresses information security for all personnel.

While PCI-DSS is not legally binding within the European Union, there are some States in the United States of America where specific laws directly refer to PCI-DSS. For example, the State of Washington has incorporated the PCI-DSS standard into state law, which stipulates that compliant organizations are shielded from liability, in the event of a data breach or a security incident (The House of Representatives of the State of Washington 2010).

Another example of cybersecurity practices developed for a specific domain is the requirements described in the "Security Rule" within the Health Insurance Portability and Accountability Act (HIPAA) of 1996. More specifically, the Security Rule establishes cybersecurity standards for healthcare organizations that are legally required to protect electronic Personal Health Information (ePHI). This includes implementing appropriate administrative, physical, and technical security controls that will ensure that confidentiality, integrity, and availability of ePHI is upheld. While HIPAA provides explicit security requirements that must be implemented by healthcare organizations, an organization can select and implement security controls from various sources, including NIST Special Publications and ISO 27002.

Cybersecurity Programs in Practice

While some organizations could be legally required to implement cybersecurity practices, there are other benefits to creating, deploying, and maintaining cybersecurity programs. Siponen and Willison argue that organizations who implement cybersecurity programs can "demonstrate their commitment to secure business practices; apply for security certification, accreditation, or a security-maturity classification attesting to their compliance to a set of rules and practices" (Siponen and Willison 2009). Effectively, implementing cybersecurity programs provides an organization with a baseline for improving its overall cybersecurity management strategy.

Several researchers (Siponen 2006; Siponen and Willison 2009; Wiander 2007) have examined

how organizations implement cybersecurity programs and evaluated how these programs impact an organization's wider security posture. Wiander (2007) evaluated how four organizations implemented ISO/IEC 17799 security standard. The results from this analysis showed that implementing cybersecurity programs within these organizations increased the overall understanding of cybersecurity by employees within the organizations (Wiander 2007). However, Wiander also observed that many individuals within these organizations found it difficult to implement the security standard, with the readability of the standard being one of the main problems cited during the study. Siponen (2006) made similar observations and added that many cybersecurity standards are not universally validated because they are based on personal experiences. Hence, Siponen (2006) argues that cybersecurity standards should not be treated as a "gold standard" but rather as a library of material for organizations to enhance their security posture. These concerns were further validated in a later study (Siponen and Willison 2009) when four cybersecurity standards were evaluated in several organizations. Siponen and Willison (2009) argued that when these standards are developed, they do not pay enough attention to the differences between organizations and their differing cybersecurity requirement. For example, while a larger organization could place equal emphasis on all aspects of information security, a smaller organization might lack the demand for a dedicated security incident management team and place more emphasis on antivirus solutions and firewalls. Hence, there could be cases where some organizations are not in compliance with a particular standard because they lack the resources to segregate security functions (Siponen and Willison 2009).

Conclusions

Addressing cybersecurity effectively is an extremely difficult and complex task. This is because there is no single solution to all of an organization's security challenges. While the threat from malicious actors and nations continues to increase, organizations are under continuous pressure to identify and implement cybersecurity controls to protect company and customer information assets. One solution could involve an organization designing and implementing a cybersecurity program based on cybersecurity best practices proposed by organizations such as NIST, ISO/IEC, and IETF. However, financial constraints often limit the number and type of security controls that can be implemented within an organization. Hence, the best approach to implementing cybersecurity practices is one where an organization takes into consideration its legal and regulatory obligations while balancing the cost of security controls.

Cross-References

- ▶ Cybersecurity: Cybercrime and Prevention Strategies
- ▶ Cybersecurity: Policy

References

Eloff, J. H., & Eloff, M. (2003). *Information security management: A new paradigm.* Paper presented at the Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology.

Grispos, G., Glisson, W. B., & Storer, T. (2013). *Cloud security challenges: Investigating policies, standards, and guidelines in a fortune 500 organization*. Paper presented at the 21st European Conference on Information Systems, Utrecht.

Grispos, G., Jesús, G-G., Liliana, P., & Bashar N. (2017). Are you ready? Towards the engineering of forensic-ready systems. In *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, pp. 328–333. IEEE.

International Organization for Standardization/International Electrotechnical Commission (2012). *Information technology – Security techniques – Guidelines for cybersecurity*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

International Organization for Standardization/International Electrotechnical Commission (2013). *Information technology – Security techniques – Code of practice for information security controls*.

International Organization for Standardization/International Electrotechnical Commission (2014). *ISO/IEC 27000 – Information security management systems – Overview and vocabulary.*

National Institute of Standards and Technology (2018). *Framework for improving critical infrastructure cybersecurity.*

PCI Security Standards Council (2018). *Payment Card Industry (PCI) Data Security Standard (DSS), version 3.2.1*.

Peltier, T. R. (2013). *Information security fundamentals*. Boca Raton: CRC Press.

Ross, R. (2007). Managing enterprise security risk with NIST standards. *IEEE Computer, 40*(8), 88–91.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM, 49*(8), 97–100.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270.

The House of Representatives of the State of Washington (2010). *Financial information security breaches – Credit and debit cards, chapter 151, laws of 2010 – House Bill 1149*.

Von Solms, B. (2000). Information security – The third wave? *Computers & Security, 19*(7), 615–615.

Von Solms, B. (2006). Information security – The fourth wave. *Computers & Security, 25*(3), 165–168.

Wiander, T. (2007). *Implementing the ISO/IEC 17799 standard in practice-findings from small and medium sized software organisations.* Paper presented at the 5th International Conference on Standardization and Innovation in Information Technology, 2007. SIIT 2007.

Further Reading

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy.* Springer. Basingstoke, United Kingdom.

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). *Enterprise cybersecurity – How to build a successful cyberdefense program against advanced threats*. New York: Apress.