Review of Business and Technology Research, Vol. 13, No. 1, 2016, ISSN 1941-9414

DEVELOPING A MODERN SECURITY POLICY

Michael Anunswith, Young B. Choi

College of Arts & Sciences
Regent University
1000 Regent University Drive
Virginia Beach, Virginia 23464

U.S.A.

e-mail: michanu@mail.regent.edu | ychoi@regent.edu

Abstract

In this paper we will address the development of a modern security policy. Current security policy development strategies are introduced first and we will move on to what is new and upcoming. The strategies will range from past, present, and the future.

***Keywords**:* Security Policy, Information Security Policy, CFAA, DMCA, HIPAA, Enterprise Security Policy, Issue-Specific Security Policy, System-Specific Security Policy, Modern Security Policy Model, TM Forum Security Management Model, ZOOM Policy Model

1. Introduction

The success of any Information Security program lies in policy development. In 1989, the National Institute of Standards and Technology addressed this point in "Special Publication SP 500-169, Executive Guide to the Protection of Information Resources" (p.1):

The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated systems. Your primary responsibility is to set the information resource security policy for the organization with the objectives of reduced risk, compliance with laws and regulations and assurance of operational continuity, information integrity, and confidentiality.

A policy is the essential foundation of an effective Information Security Program as stated by Charles Cresson Wood in his book "Information Security Policies Made Easy" (p.1):

The centrality of information security policies to virtually everything that happens in the information security field is increasingly evident. These policies will stipulate the type of transmission services that should be permitted, how to authenticate the identities of users, and how to log security-relevant events. An effective

information security training and awareness effort cannot be initiated without writing information security policies because policies provide the essential content that can be utilized in training and awareness.

2. Information Security Policy

Information is an important business asset and is valuable to an organization. Therefore, it needs to be protected to ensure its confidentiality, integrity and availability. The first step in information security is to set up policies and procedures on how to protect information. Our text defines an Information Security Policy as a written instruction, provided by management, to inform employees and others in the workplace of the proper behavior regarding the use of information and information assets. (p.630) Security policies are the foundation of information security in an organization and a well written and well implemented policy will contain sufficient information on what must be done as to protect information and people in the organization. Security policies also establish computer usage guidelines for staff in the course of their job duties. System administrators and business owners have to acknowledge the fact that security threats exist and how to prevent and respond to them. Identifying and implementing suitable controls requires careful planning and participation of all employees in the organization and are also vital for the success of information security management. Depending on the size, financial resources, and the degree of threat, an organization needs to implement a security policy that has the right balance between overreacting and the vulnerability of exposing a system to potential threats. The objective of a well written and implemented security policy is improved information availability, integrity and confidentiality, from both inside and outside the organization.

3. Laws and Regulations

Information security professionals work within an enterprise to protect it from all non-physical threats to the integrity and availability of its data and systems. Performing this function draws security professionals into simultaneous, ongoing relationships between the organization and the organization's employees and other entities: its customers, suppliers, competitors, and government officials and regulators. This section will be a discussion of important laws and regulations as they pertain to organizations.

3.1 CFAA-Computer Fraud and Abuse Act

The U.S. Code § 1030 Computer Fraud and Abuse Act was originally created solely as a computer crime statute, but in its present form, it imposes both civil and criminal liability for a wide variety of acts that compromise the security of public and private sector computer systems. It defines and formalizes laws to counter threats from computer-related acts and offenses. It specifically states that however intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); information from any department or agency of the United States; or information from any protected computer. Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period. (18 U.S. Code §1030, 2015)

3.2 DMCA -The Digital Millennium Copyright Act

The Digital Millennium Copyright Act, 17 U.S.C. §1201-05 (the "DMCA"), provides that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title [the Copyright Law]," and goes on to prohibit the "manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to [a copyrighted work]; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to [a copyrighted work]; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to [a copyrighted work]." (17 U.S. Code §12.1, 2015)

3.3 The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996. According to the Centers for Medicare and Medicaid Services (CMS) website, The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the

Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. To date, the implementation of HIPAA standards has increased the use of electronic data interchange. (Administrative Simplification Overview, 2016)

4. Types of Security Policies

In this section I will go over various security policies, both past and present. Policy management is one mechanism to achieve automation; it has the benefit of adding structure to how process is automated. According to techgadget, 'Policy-based management is an administrative approach that is used to simplify the management of a given endeavor by establishing policies to deal with situations that are likely to occur. Policies are operating rules that can be referred to as a way to maintain order, security, consistency, or otherwise further a goal or mission.' (Policy-based Management, 2011)

Something to think about when implementing a security policy is distribution. While this may seem straightforward, getting the policy into the hands of each employee may require a substantial investment by the organization. One option is by hand out but in today's world the better option is electronic distribution. Though this requires an organization to provide a mechanism to prove distribution, such as an auditing log tracking when users access the document. To be certain that employees understand the policy, the document should be written at a reasonable reading level, with minimal technical terms and management terminology. The next step is to use some form of assessment to gauge how well the employees understood the policy's underlying issues. One option is a quiz, requiring the employee to pass by earning a minimum score of 70 and which require additional training and awareness efforts before the policy can be enforced. This brings us to policy compliance in which the employee must agree to the policy. One way to accomplish this is by incorporating a digital signature when the employee has read and comprehended the policy. Lastly, policy enforcement is used in an impartial way to make sure it is governed in a uniform fashion. As in law enforcement, policy enforcement must be able to withstand external scrutiny.

4.1 **Enterprise Information Security Policy**

In our text, enterprise information security policy is defined as what sets the strategic direction, scope, and tone for all of an organization's security efforts. It assigns responsibilities for the various areas of information security, including maintenance of information security policies and practices and responsibilities of end users. In

particular, the EISP guides the development, implementation, and management requirements of the information security program, which must be met by information security management, IT development, IT operations, and other specific security functions. (p.122) The high level security policy is based on and directly supports the vision, mission, and direction of the organization and sets a strategic direction, scope, and tone for all security effort consisting of anywhere between 2 to 10 pages.

4.2 Issue-Specific Security Policy

A sound issue-specific security policy provides detailed, targeted guidance to instruct all members of the organization in the use of a resource, such as a process or a technology employed by the organization. It should begin with an introduction of the organizations fundamental resource use philosophy and assure members of the organization that its purpose is not to establish a foundation for administrative enforcement or legal prosecution but to provide a common understanding of the purposes for which an employee can and cannot use the resource. An ISSP should provide ways to help an organization to protect itself and its employees from inefficiency. An effective ISSP is a binding agreement between the organization and its members and shows that the organization has made a good faith effort to ensure that its technology will not be used in an inappropriate manner. (p.124, 128)

4.3 System-Specific Security Policy

System-specific security policies often function more like standards or procedures to be used when configuring or maintaining systems that could include a statement of managerial intents, guidance to network engineers on selecting, configuring, and operating firewalls, and an access control list that defines levels of access for each authorized user. This policy type is more focused technically that the issue-specific security policy in that it outlines how to protect the system and technology. (McMillan & Abernathy) There is also a system-specific security policies configuration that combines management guidance system-specific security policy and the technical specifications system-specific security policy into a single document. This document may be a little confusing to users; it is highly practical to have the guidance from both perspectives in a single place.

5. Modern Security Policy Models

There are a number of possible routes available when creating policies, ranging from an off the shelf purchase, to carefully crafting every clause and sentence. The most cost effective way is often to procure a set of pre-written policies, and then tailor them as necessary to meet specific organizational needs. Why re-invent the

wheel and proceed down a more complex route than necessary? When adopting this course, or indeed, when simply redeveloping existing policies, a number of less direct factors should also be taken on board - how will the policies sit with ISO17799 for instance. Modern Security policies are often based on ISO 17799. ISO 17799 is the most widely recognized security standard. It is based upon the original version of BS7799, which was first published in 1995, an edition which itself was based on an earlier document called the 'Information Security Code of Practice'. The first version of ISO 17799 was published in December of 2000. ISO17799 is very comprehensive in its coverage of security issues. It contains a substantial number of control requirements, some of which are extremely complex and detailed. (ISO 17799 Description and Review) Compliance with this internationally recognized standard is growing in importance. Because of this, and because of the standards relevance as a common currency for information security measurement, many organizations are basing their security policies upon the standard itself. Having a security policy document in place itself is not enough; the contents must be implemented to be effective but this is often easier said than done! Information security policies are the bottom line; they set the boundaries of acceptability across the organization. However, it is certainly the case that some areas are more security sensitive than others. In these, for example, more stringent security measures may be appropriate. (Information Security Policies and Standards)

A newer trend in the workplace is companies letting their employees bring their own devices. According to Steve Durbin, managing director of the Information Security Forum (ISF), "As the trend of employees bringing mobile devices, applications and cloud-based storage and access in the workplace continues to grow, businesses of all sizes are seeing information security risks being exploited at a greater rate than ever before," he says. "These risks stem from both internal and external threats including mismanagement of the device itself, external manipulation of software vulnerabilities and the deployment of poorly tested, unreliable business applications." He notes that if you determine the BYO risks are too high for your organization today, you should at least make sure to stay abreast of developments. And realistically, Durbin says, expect that your users will find a way to use their own devices for work even if you have a policy against BYOx. (Olavsrad, 2014)

5.1 An Abstract Model for Security Management:

The TM Forum Security Management Model, illustrated in Figure 1, is an abstract model consisting of process flows and operational states. As an abstract model, it is a logical amalgam of multiple similar models and not intended as an exact representation of any specific actual system implementation. It

is intended primarily as a tool to promote understanding, facilitate communication and collaboration, and guide coherent evolution across the complete TM Forum Frameworx. (TM Forum, 2011, p.9)

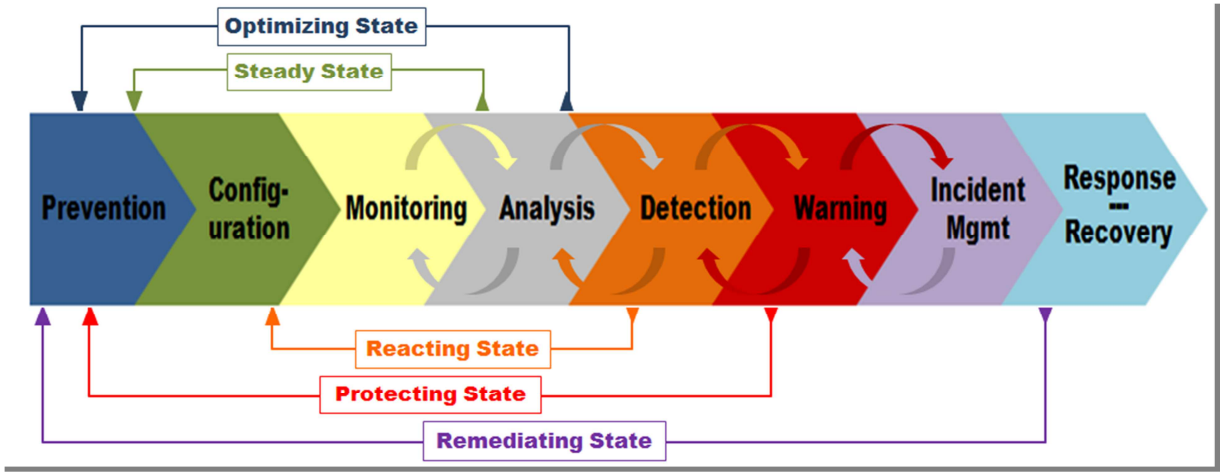

Figure 1: TM Forum Security Management Model [TM Forum]

From this figure we can see the different states of the security management model. The steady state is the operational flow; policy-based analysis of data collected via monitoring discovers no anomalies or inefficiencies. The Optimizing State arises when policy-based analysis of data collected via monitoring discovers one or more internal anomalies or deficiencies that analysis identifies as opportunities to enhance the baseline Prevention posture. The Reacting State arises when policy based analysis of data collected via monitoring identifies a potential vulnerability, violation, or intrusion – anything that can be remediated via a Configuration change, within the bounds of active policy. Detection triggers real-time updates to Configuration (e.g., log level adjustments, port blocking, traffic filtering) to isolate anomalies, expand the evidence base, and activate additional defensive measures. The Protecting State arises when analysis of data collected via monitoring and flagged by detection as a probable vulnerability, violation, or intrusion satisfies the policy-based criteria for formal Warning. Such Warning triggers notifications being sent (alerting) to appropriate entities (humans and software). And lastly, the Remediating State arises when Incident Management leads to Response and Recovery actions that result in updates to the baseline Prevention posture. (pp. 16-21)

5.2 ZOOM Policy Model and Architecture Snapshot

FOCALE stands for Foundation – Observe – Compare – Act – Learn – Reason. Network administration is inherently difficult. In contrast to other types of administration, network administration typically applies to a heterogeneous environment, where each node can implement the same function using different programming models with different side effects. Many times, this entails manually managing diverse technologies and devices whose functionality needs to be coordinated to provide a set of services to multiple users. One of the ways of dealing with the many complexities of dynamic systems is to use autonomic. The primary purpose of autonomic systems is to manage complexity. The heart of an autonomic system is its ability to manage its operation by taking an appropriate set of actions based on the conditions it senses in the environment**Error! Reference source not found.**. (TM Forum, 2015, p.16) Sensors retrieve data, which is then analyzed to determine if any correction to the managed resource(s) being monitored is needed (e.g., to correct non-optimal, failed or error states). If so, then those corrections are planned, and appropriate actions are executed using effectors that translate commands back to a form that the managed resource(s) can understand. If the autonomic network can perform manual, time-consuming tasks (such as configuration management) on behalf of the network administrator, then that will free the system and the administrator to work together to perform higher-level cognitive functions, such as planning and network optimization.

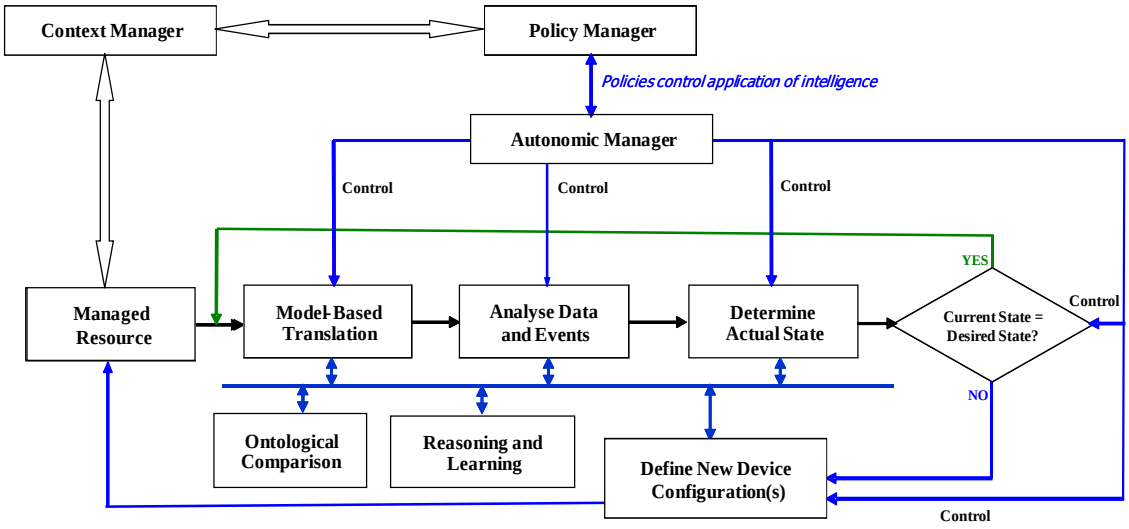

Figure 2. A Simplified View of the FOCALE Autonomic Architecture (p.16) [TM Forum]

6. Conclusion

In this paper we have discussed what a security policy is and what it entails. Some of the topics discussed go as follows: laws and restrictions that government what needs to be included in the implementation of a security policy, the various types of security policies to include enterprise information security policies, issue specific security policies, and system specific security policies, how to distribute a policy, ensure its comprehension, and how to impartially enforce said policy, and we discussed a few newer security policies that are now be implemented. Policies are operating rules that can be referred to as a way to maintain order, security, consistency, or otherwise further a goal or mission.' It is important to get your policy distributed to everyone in your organization and have a way for the reading of it to be traceable.

References

National Institute of Standards and Technology. URL: http://www.nist.gov/

Wood, Charles Cresson. *Information Security Policies Made Easy*, 12th ed. Information Shield, Inc., 2012.

18 U.S. Code §1030 – Fraud and related activity in connection with computers, https://www.law.cornell.edu/uscode/text/18/1030.

HIPAA and ACA, https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html.

Policy-based management, http://whatis.techtarget.com/definition/policy-based-management.

TMforum. *TM Forum Security Management Model.* Release 1.0. Oct 2011.

TMforum. *ZOOM Policy Model and Architecture Snapshot.* Release 14.5.1. February 2015.

Whitman, M. E., & Mattord, H. J. (2004). *Management of information security*. Boston, MA: Thomson Course Technology.

Whitman, Michael E., and Herbert J. Mattord. *Principles of Information Security*. Boston, MA: Course Technology, 2012.

Council, E. (2011). *Network defense: Security Policy and Threats*. Clifton Park, NY: Course Technology, Cengage Learning.

McMillan, T., & Abernathy, R. (2013). *CISSP cert guide*. Pearson IT Certification.

The Information Security Policies / Computer Security Policies Directory

http://www.information-security-policies-and-standards.com/.

5 Information Security Trends That Will Dominate 2015,

http://www.cio.com/article/2857673/security/5-information-security-trends-that-will-dominate-2015.html.

Executive Guide to the Protection of Information Resources, NIST Special Publication 500-169,

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-169.pdf.