Chapter 97
Promoting Cybersecurity Compliance

Mark A. Harris
Augusta University, USA

Ronald Martin
Augusta University, USA

ABSTRACT

In a global online economy, organizations are tasked with protecting their cybersecurity assets. Penalties from failing to protect assets, such as customer data, can severely harm an organization and even lead to bankruptcy. Cybersecurity governance programs need to be aware of the laws and regulations affecting their organizations and use applicable standards or frameworks to develop appropriate cybersecurity polices and controls. Compliance programs then need to monitor policy compliance on a continuing basis. This chapter discusses the laws, regulations, and standards that are used to create cybersecurity polices and the typical tools used to measure compliance. In addition, theoretical cybersecurity compliance research is reviewed to highlight supplementary techniques to improve compliance.

INTRODUCTION

In 2014, Walgreen's Inc. was held liable for $1.4 million due to a pharmacist revealing confidential patient information (HHS, 2018) in violation of the United States (U.S.) Health Insurance Portability and Accountability Act of 1996 (HIPAA). The decision set a precedent by which companies could be held liable for an employee's actions regarding HIPAA compliance (Evans, 2014). Inaction in securing patient health information can also violate HIPAA. In 2017, CardioNet, Inc. reached a $2.5 million settlement for leaving a laptop with patient information unsecured that was consequently stolen (Day, 2017). These are examples from just one of many laws and regulations affecting organizations today. In a violation of the Sarbanes-Oxley Act of 2002, Morgan Stanley paid a $1 million penalty in 2016 for inaction that allowed 730,000 customer account's information to be stolen. The U.S. Securities and Exchange Commission (SEC) claims the company "failed to adopt written policies and procedures rea-

DOI: 10.4018/978-1-7998-8954-0.ch097

sonably designed to protect customer data" (SEC, 2016). In another Sarbanes-Oxley violation involving the loss of customer data, investment advisor R. T. Jones Capital Equities Management paid a $75,000 fine for also failing to adopt written policies and procedures to protect customer data (SEC, 2016). In a violation of the Children's Online Privacy Protection Rule (COPPA), the company VTech was penalized $650,000 for failing to encrypt their Web site's customer data in transit, failing to notify parents of data collected from children, and failing to verify those creating parent accounts were actually adults.

The potential loss from violating laws and regulations requires organizations to establish policies and other governing documents outlining the expectations for employees' behavior regarding adherence to all appropriate laws, regulations, and industry standards. The process of ensuring an enterprise establishes and deploys appropriate controls is generally referred to as cybersecurity governance. The National Institute of Standards and Technology (NIST) defines governance as "the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk" (Bowen, 2006). The part of the governance definition discussed in this chapter is the adherence to policies and internal controls, often referred to as compliance.

ISACA (n.d.), formerly the Information Systems Audit and Control Association, defines compliance as "adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies." The enterprise demonstrates compliance with applicable cybersecurity requirements through the creation, deployment and enforcement of cybersecurity policies. Policies are documents that record a high-level principle or course of action indicating the intention and direction management has determined (ISACA, n.d.-a). To help with implementing broad-level policies, organizations often develop accompanying standards, guidelines, and procedures (Nieles et al., 2017). NIST's SP 800-12 states that standards and guidelines specify technologies and methodologies and that procedures detail steps to accomplish tasks. Policy standards, guidelines, and procedures are specific to the organization, but are often informed by externally recognized standards and frameworks.

The content of the policies will be driven by a variety of factors. For instance, certain industries have specific requirements defined by congressional action via legislation and commensurate regulations. HIPAA in the medical field and Sarbanes-Oxley in the financial industry are examples of industry specific legislation requiring cybersecurity related activities. Other influences on policy creation include a desire by an organization to be seen as adherent to externally recognized cybersecurity standards, such as the ISO 27000 series.

Once an organization has cybersecurity policies in place, users are required to abide by them. Users typically are the organization's employees and contracted workers. Users are often informed about the organization's cybersecurity polices through a security education, training, and awareness program. Such programs may have face-to-face trainings, web-based trainings, security awareness posters, and more that take place on a periodic schedule. Once polices are created and users are aware of them, organizations need to ensure compliance. There are many tools available for measuring compliance with cybersecurity polices and some can be automated. For example, firewalls can be configured to block certain sites to maintain compliance. Software scanners can be scheduled to scan the network and equipment for vulnerabilities and configuration issues. Penetration testing can be used by an authorized team to actually exploit weaknesses. Beyond tools, organizations use internal and external auditing to help ensure compliance. Some laws and regulations require periodic auditing, such as HIPAA.