Chapter 2
Auditor Evaluation and Reporting on Cybersecurity Risks

Jeffrey S. Zanzig
Jacksonville State University, USA

Guillermo A. Francia III
https://orcid.org/0000-0001-8088-2653
University of West Florida, USA

ABSTRACT

Tremendous improvements in information networking capabilities have brought with them increased security risks resulting from the deterioration of the ability of a physical layer of computer security to protect an organization's information system. As a result, audit committees have had to deal with new security issues as well as the need to understand the cyber perpetrator and ensure the proper training of employees to consider cybersecurity risks. Standard setters including the Institute of Internal Auditors and the American Institute of Certified Public Accountants have issued guidance about lines of defense and reporting on an entity's cybersecurity risk management program and controls, respectively. Each of these topics is considered along with how cybersecurity guidance from COBIT, the National Institute of Standards and Technology, and the Center for Internet Security can be mapped into five cyber infrastructure domains to provide an approach to evaluate a system of cybersecurity.

INTRODUCTION

Just a few decades ago information systems consisted primarily of mainframe computers with what were commonly referred to as "dumb terminals" that granted access into a mainframe computer which performed an organization's information processing. The risk of intruders accessing such systems was significantly less and physical security measures such as locked doors and security guards served as an effective approach in protecting information systems from outsiders. Substantial information processing

DOI: 10.4018/978-1-6684-3698-1.ch002

capabilities were then added with the widespread use of the Internet, company networks, and the distribution of computing power to the end user. Unfortunately, it also resulted in an immense increase in the danger of outsiders hacking into company information systems gaining access to sensitive information and causing various types of malicious behavior.

A recent cybersecurity attack at the Marriott hotel chain illustrates what can happen when cybersecurity incidents occur and are not thoroughly resolved. In 2015, Marriott Hotels acquired another hotel, known as Starwood Hotels and Resorts Worldwide, as part of a $13.6 billion deal which made Marriott the No. 1 hotel chain in the world. Four days after the announcement of this 2015 merger, Starwood stated that credit card information had been stolen in some of its hotel restaurants and gift shops as a result of malware that attackers installed on point-of-sale systems in 2014. In December 2018, The Wall Street Journal reported the theft of personal information for up to 500 million customers as a result of a hack of Marriott's customer database for its Starwood properties. Although Marriott claimed that the 2018 discovery was unrelated to the prior incident, security experts believe that a more thorough investigation of the initial intrusion would have identified a second intruder who was able to stay in the Marriott reservation system for the more than three years following the initial security breach (McMillan, 2018).

The objectives of this research are to provide an overview of some of the considerations that are involved in an assessment of an organization's system of cybersecurity including: lines of defense, audits and reporting, and standards and frameworks for evaluation. This article begins by considering challenges facing today's audit committees, the need to understand the common profile of the cyber perpetrator, and the necessity of employee training to overcome complacency in dealing with cybersecurity risks. This is followed by guidance from both the Institute of Internal Auditors (IIA) and the American Institute of Certified Public Accountants (AICPA). A thought-provoking discussion based on IIA literature considers what the IIA refers to as "three lines of defense" to address risks in today's cyber environment. Guidance from the AICPA describes reporting on an entity's cybersecurity risk management program and controls. In the audit of security systems to address cybersecurity risks, it is also essential to make use of standards and frameworks to facilitate a proper evaluation. This is also addressed by considering how guidance from COBIT, the National Institute of Standards and Technology, and the Center for Internet Security can be mapped into five cyber infrastructure domains.

BACKGROUND

A primary focus of an audit committee is to provide an independent oversight function to ensure that the processing and storage of information is performed in a secure and reliable manner to meet the needs of information users. Although the birth of the Internet and extensive networking capabilities has substantially increased the ability of organizations to process and disseminate information, it has also opened the door to allow greater access to information systems by unauthorized and many times malicious intruders. It is certainly a difficult task to address these security issues due to the constantly changing availability of technology that is both within and outside of an organization's control. This section discusses challenges faced by audit committees as a result of cybersecurity issues. It also considers common profiles of the cyber perpetrator and how noncompliance with information security policy by well-meaning organizational personnel can allow unauthorized access into an organization's information system.