CHAPTER 5

CORPORATE AND IT GOVERNANCE

WHAT IS CORPORATE GOVERNANCE

"A company's corporate governance sets the stage for how it is run, as well as what the roles and duties of those who work in the corporation may be."

—April Klazema, founder and owner of Klazema Communications

CREDIT AND DEBIT CARD THEFT

Why Managers Must Get Involved in IT Governance

On September 8, 2014, Home Depot revealed that its payment data system had been breached by hackers. In the weeks that followed the announcement, the company disclosed that hackers had stolen information connected to 56 million credit and debit cards and that these thefts had gone undetected for over five months. Home Depot's antivirus software had been infected with a **malware** (malicious software installed without a computer user's knowledge) known as Mozart, which was used to steal the card data by spying on the payment data system as the transactions were taking place. To date, investigators have been unable to determine exactly who planted the virus and how. What is known is that Mozart is a version of BlackPOS, a malware program created by a Russian teenager in 2012, and it has been used in attacks on other major retailers, including Target, Neiman Marcus, and Michaels.

Initially, the biggest question was, "How were hackers able to break into these companies' data systems?" These retailers had all complied with the Payment Card Industry Data Security Standard (PCI DSS)—the IT security measures mandated by credit companies to ensure that retailers adequately protect credit card data. In fact, since PCI standards were established in 2004, retailers have spent billions of dollars building systems that comply with them. However, some analysts have begun to question whether PCI compliance means anything in a world of rapidly evolving IT security threats. It turns out that to be PCI compliant, retailers only need to encrypt stored data—not data in motion. That is, PCI standards do not require retailers to encrypt active transaction data, including data passed to the merchant at point-of-sale (POS) terminals, such as cash registers. BlackPOS exploits this weakness and since its release has targeted retailer after retailer, evolving with time, so that although Home Depot knew of the vulnerability, it could not detect the new variant, Mozart.

In fact, at the time of the attack, Home Depot was taking steps to safeguard data in its in-store payment system. The retailer had hired Voltage Security in January 2014, not long after the massive data thefts from Target's point-of-sale systems were made public, to encrypt its data at point of sale. Unfortunately, at the time of the attack, the project was incomplete—the encryption software was installed and tested in some but not all of Home Depot's stores. By September 13, however, five days after the breach was revealed, Home Depot had installed the encryption software at all locations in the United States.

Clearly, PCI standards need to keep up with the times—as do retailers. However, technology is not the only solution. Some analysts have charged that human error contributed to the damage caused by the theft of data involving 40 million credit and debit cards from Target's systems. Six months before the incident, Target had installed a $1.6 million malware detection tool developed

by the security firm FireEye. Target had a team in Bangalore who monitored the system and alerted the security team in Minneapolis of breaches. Breaches were purportedly detected and reported on November 30 and December 2, but Target did not immediately act on those internal alarms. The company waited until December 19 to publicly confirm the breach.

Consumers and banks have since filed over 90 lawsuits against Target. However, retailers, credit card companies, and banks typically work together once a data breach occurs. For example, credit card companies and banks alerted Home Depot to the fraudulent use of credit cards that had been used at its stores. Yet, some industry experts are now calling for credit card companies, banks, and retailers to cooperate more closely so that they can prevent emerging threats, rather than just stop them as—or after—they occur.

LEARNING OBJECTIVES

As you read this chapter, ask yourself:

- What is IT governance and what are the key elements of an IT effective governance process?
- How can an effective IT governance program improve the likelihood of organizational success?

This chapter defines the goals of IT governance and clarifies the importance of good governance in terms of achieving organizational objectives and managing risk.

WHAT IS IT GOVERNANCE?

Corporate governance is the set of processes, customs, rules, procedures, policies, and traditions that determine how to direct and control management activities. An organization's board of directors, CEO, senior executives, and shareholders are all involved in corporate governance. Corporate governance addresses issues such as the following:

- Preparation of the firm's financial statements
- Monitoring the choice of accounting principles and policies