CASE 5.1 OPENING CASE

BlackPOS Malware Steals Target's Customer Data

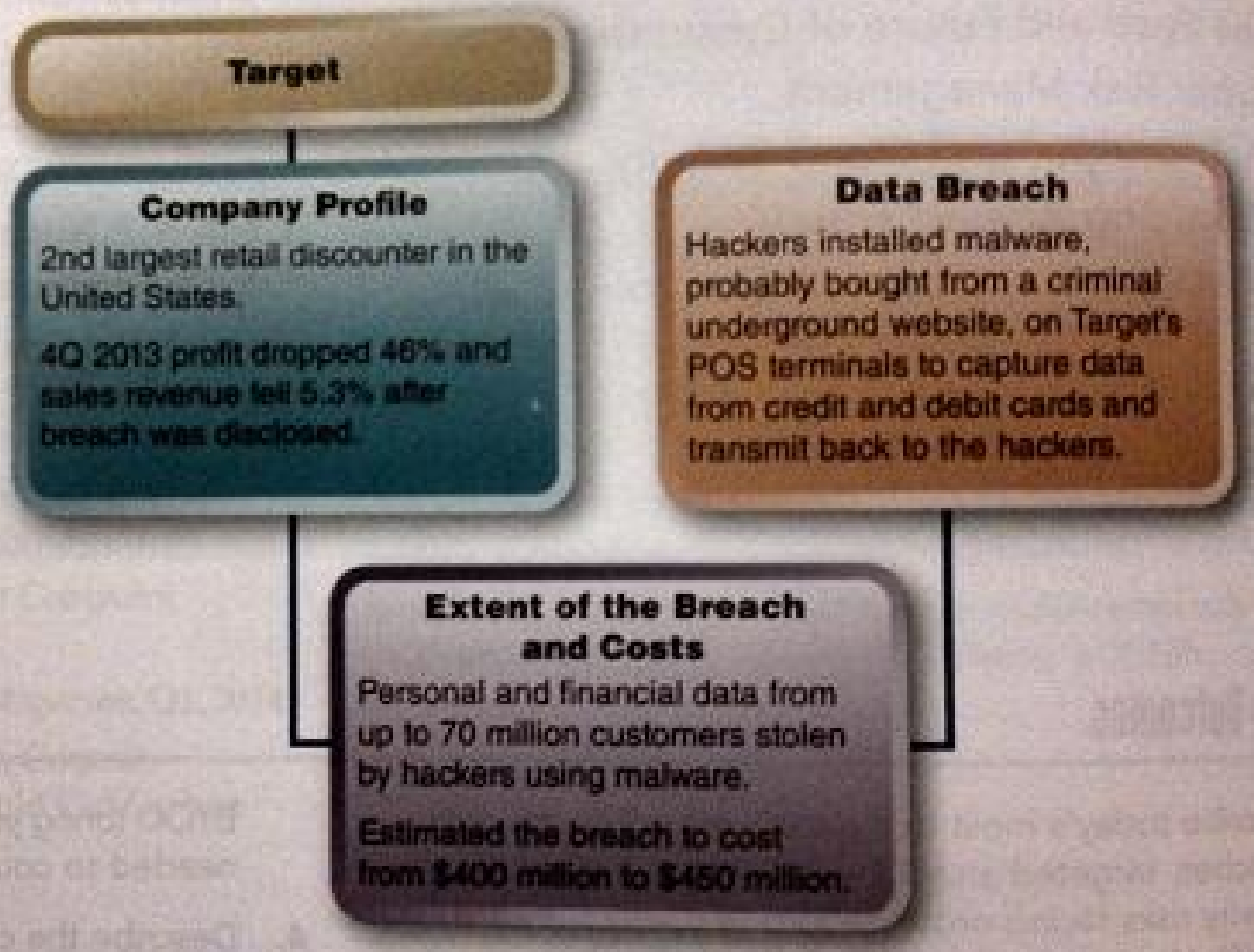

Figure 5.1 Target data breach overview.

Target is a major discount retailer in the United States (Figure 5.1). Target's management admitted that 40 million credit and debit card accounts were exposed between November 27 and December 15, 2013. During that peak holiday shopping

Estimated the breach to cost from $400 million to $450 million.

Target is a major discount retailer in the United States (Figure 5.1). Target's management admitted that 40 million credit and debit card accounts were exposed between November 27 and December 15, 2013. During that peak holiday shopping season, hackers captured credit card data from the stores' point-of-sale (POS) payment terminals (Figure 5.2).

Target disclosed the breach on December 19, 2013; then on January 10, 2014, the retailer also reported that hackers stole 40 million credit card numbers along with the personal information of another 70 million customers. The incident scared shoppers away, affecting the company's profits throughout 2014.

Several experts believe that POS malware bought from the criminal underground was responsible. **Malware**, short for *malicious software*, are computer programs whose code causes disruption, destruction, or other devious action. Malware named **BlackPOS** is sold on the black market for $1,800 or more. The malware is advertised on Internet underground forums under the generic name *Dump Memory Grabber by Ree*. BlackPOS is malware designed to be installed on POS devices in

Figure 5.2 POS payment terminal. Malware-infected POS terminals caused Target's data breach.

© Alexis Sluiter/Shutterstock

order to record data from credit and debit cards swiped through the infected device. Specifically, the malware identifies the process associated with the credit card reader and steals payment card Track 1 and Track 2 data from its memory. These are the data stored on the magnetic strip of payment cards that were used to clone or create counterfeit cards.

More feature-rich versions of BlackPOS selling for roughly $2,300 provide encryption support for stolen data. The BlackPOS creator is not confirmed, but experts tracking the malware suggest that the hacker may be based in Russia or Ukraine. The U.S. Secret Service estimated that the type of malware that led to Target's breach has affected over 1,000 U.S. businesses.

In February 2014 Target reported that its 2013 fourth-quarter (4Q) profit dropped 46 percent and sales revenue fell 5.3 percent. A few months later, in May 2014, Target estimated that technological changes to harden its IT security would cost more than $100 million in addition to $61 million incurred in breach-related expenses in Q4 2013. These costs and damages harmed the company's profitability.

Gregg Steinhafel, chairman, president, and CEO of Target, tried to reassure customers and investors, saying, "As we plan for the new fiscal year, we will continue to work tirelessly to win back the confidence of our guests. . . . We are encouraged that sales trends have improved in recent weeks" (D'Innocenzio, 2014).

Six months after the breach, it still was not clear when Target would fully recover. A security analyst at the tech firm Gartner estimated the costs of the breach to range from $400 million to $450 million. That includes the bills associated with fines from credit card companies and services for its customers like free credit card report monitoring. Target also faced at least 70 lawsuits related to privacy invasion and negligence, alleging Target did not take proper steps to protect consumer data.

According to financial services firm Cowen Group's note to investors, criminals were able to hack into Target's database due to a lack of security, which might have been a result of underinvestment by senior management.

Target's cybersecurity staff had also warned management to review the security of its payment card system at least two months before the breach. At the time of the warning, Target was updating the payment terminals, which makes them more vulnerable to attack, in preparation for the holiday season. Data security was not a top priority. Months before the attack, the federal government and private research firms were also warning companies about the emergence of new types of malware

worldwide in 2013. The consequences of lax cybersecurity include damaged reputations, financial penalties, federal and state government fines, lost market share, falling share prices, and consumer backlash.

The main cause of a data breach is hacking, but the reason hacking is so successful is *negligence*—management not doing enough to defend against cyber-threats. Even high-tech companies and market leaders, as shown in Table 5.1, appear to be detached from the value of the confidential data they store and the threat that highly motivated hackers will try to steal them. As you will read in this section, robust data security is not the responsibility of IT alone, but the ongoing duty of everyone in an organization.

Hacks of high-tech companies like LinkedIn, Google, Amazon, eBay, and Sony, and top security agencies like the CIA and FBI are proof that no one is safe. Cyberwarriors are too well funded and motivated. Countering cyber-threats demands diligence, determination, and investment. IT at Work 5.1 illustrates the self-destructing and encryption features of a secure smartphone in order to protect conversations, transmissions, and stored data effectively.

IT at Work 5.1

Black—the Self-Destructing Smartphone