Business Horizons (2016) 59, 257—266

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

BUSINESS LAW & ETHICS CORNER

Why you should care about the Target data breach

Nathan Manworren [a,*], Joshua Letwat [b], Olivia Daily [c]

[a] Candidate for B.A. in Economic Consulting, Kelley School of Business, Indiana University (expected 2017)
[b] Candidate for B.A. in Accounting and Finance, Kelley School of Business, Indiana University (expected 2017)
[c] Candidate for B.A. in History and Finance, Kelley School of Business, Indiana University (expected 2017)

KEYWORDS
Cyberattack;
Cybersecurity;
Target;
Best practices;
Internet;
Malware;
Data;
Data breach;
Security;
Lawsuit;
Privacy

Abstract Data breaches are becoming more frequent and more damaging to the bottom line of many businesses. The Target data breach marked the beginning of increased scrutiny of cybersecurity practices. In the past, data breaches were seen as a cost of doing business, but Target's negligence and the scale of the data loss forced businesses and the courts to reevaluate current practices and regulatory frameworks. Businesses must make strategic use of their chief information officers, adopt cybersecurity best practices, and effectively train their employees to respond to growing security threats. They must also shape the cybersecurity narrative to influence regulatory responses to these threats.

1. The breach that changed everything

Shortly before Thanksgiving 2013, someone installed malicious software (*malware*) on Target's security and payments system. The malware was designed to steal information on every credit card used at the company's 1,797 U.S. stores. At a moment when shoppers were focused on spending for the upcoming Christmas season, malware began capturing their credit card numbers and storing that captured information on servers commandeered by the hackers. In theory, Target was prepared for the hack: six months earlier, the company had begun installing a $1.6 million malware detection tool designed to inform them of a data breach. Yet in late 2013, Target failed to respond quickly to the attack—a failure that marked the beginning of a series of challenges for Target.

Since those fateful days in late 2013, customers and banks have filed more than 90 lawsuits against Target for negligence and compensatory damages. The costs of responding to the breach have continued to mount. In numbers, Target's profit for the 2013 holiday shopping period fell 46% from the same quarter the year before; in sentiment, Target lost the trust of its customers, investors, and lenders.

* Corresponding author
E-mail addresses: nmanworr@indiana.edu (N. Manworren), jletwat@iu.edu (J. Letwat), odaily@indiana.edu (O. Daily)

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.01.002

Target is just one of many companies to be affected by data security breaches. The Target case is unique, however, in that its employees evidently worked *against* its security systems. Because of this, the Target breach will likely stand as the data loss that changed everything. This article explores the Target breach, first by examining the technology involved and then by considering the roles that Target employees and others played in jeopardizing the security of its data. The article then considers the complexity of state and federal laws as they relate to data loss and suggests that creation of a national standard is the only hope for reducing the complexity of the current regulatory system. Finally, the article considers what businesses must do to protect themselves and their customers in the changing landscape of data breach regulation.

2. Target's failure

Target was at the forefront of technology in 2013, investing in state-of-the-art security. The company was warned when the hackers attacked in 2013, but it ignored multiple alerts that something was wrong and continued selling to consumers. As a result, millions of people continued to swipe their credit cards and their information continued to be sent to hackers. The resulting loss of critical consumer data put millions of people at risk for identity theft (Riley, Elgin, Lawrence, & Matlack, 2014).

2.1. How the attack happened

The hackers were able to gain access to Target's system by stealing credentials provided by the company to Fazio Mechanical Services, a contractor that ran Target's climate systems. Target failed to segment its network to ensure that Fazio—and other third parties—did not have access to its payment systems (Riley et al., 2014). As a result, the hackers were able to exploit a connection designed to let Fazio exchange contract and project management information with Target and then used this connection to upload malware onto Target's systems, including its individual point-of-sale systems (Hosenball, 2014).

2.1.1. Point-of-sales systems

A point-of-sale (or POS) system is a type of technology used to collect a consumer's payment information. The POS system calculates the amount owed by the customer and collects the payment. The interaction between the consumer and the POS system is an extremely familiar and innocuous process that occurs countless times a day. However, there is much more to a POS system then what is visible to consumers.

POS systems are comprised of both software and hardware. The hardware includes equipment such as a cash register, credit card reader or terminal, pin pad, and monitor. The software communicates the customer's information using a central payment-processing server connected to a number of POS application terminals. When a credit card is used at the POS terminal, the terminal connects to the central payment-processing server in the merchant's corporate environment, which then provides payment authorization (Hizver & Chiueh, 2012). When people swipe their credit cards at a POS terminal, the data encoded on the card's magnetic stripe—such as the card number, cardholder name, and card expiration date—is sent with the transaction request to the payment software application and then to the company's payment processing provider (Constantin, 2014).

The malware used by the hackers was programmed to steal Target's customer data at the point of sale. So-called 'RAM scrappers' would copy customers' card information while it was still in the memory storage of Target's POS system. While payment information is encrypted when it is sent off to confirm a sale, it remains readable within the system (Constantin, 2014). Target's IT infrastructure should have identified and destroyed this malware, but it failed to do so (Smith, 2014).

2.1.2. Target's security

Target was aware of the threats posed by hackers and had deployed numerous security measures to protect its computing architecture. It had "multiple layers of protection, including five firewalls, malware detection software, intrusion detection and prevention capabilities, and data loss prevention tools" (Committee on the Judiciary, 2014). Target also performed internal and external validation and benchmarking assessments, and its security systems complied with data security standards in the credit card industry. It was even widely reported that Target used "the same security system. . .employed by the CIA, the Pentagon, and other spy agencies around the world" (Smith, 2014).

Target's sophisticated security system could and should have addressed the malware uploaded by the hackers. The system even had a function that would automatically delete malware as soon as it was detected, but Target's security team had turned off that function—just as many other businesses using the same system had done—because it often halted email and Internet traffic by incorrectly flagging data as malware (Finkle & Heavey, 2014; Smith, 2014).