INTRODUCTION

As part of its oversight responsibilities, the board of directors is expected to ensure that management has identified and developed processes to mitigate risks facing the organization, including risks arising from data theft and the loss of proprietary or customer information. Unfortunately, general observation suggests that companies are not doing a sufficient job of securing this data. Data theft has grown considerably over the last decade. According to the Identity Theft Resource Center, the number of data breaches tripled from 2007 to 2016. The main contributor to this increase was theft by third-party hacking, skimming, and phishing schemes (see Exhibit 1).1

The cost of data theft is significant. According to the Ponemon Institute, the average direct organizational cost of a data breach in the United States is $7 million. This includes the cost to identify and contain the breach, notify customers, and loss of business.2 Class-action lawsuits add to this figure, with settlements ranging from approximately $1 million for moderate-scale data breaches to over $100 million for large-scale breaches.3 One study finds that the average stock declines 5 percent following the disclosure of a breach and performs negatively over the subsequent 90-day period.4 Clearly, cybersecurity is an important risk facing companies and their shareholders.

INCIDENTS OF DATA THEFT

Given the cost and likelihood of a successful cyberattack, it is important to ask whether boards and management have sufficient understanding and are appropriately prepared to prevent, monitor, and mitigate digital data theft (see Exhibit 2 for survey data). To shed light on this question, we reviewed prominent incidents of data theft over the last five years to understand the types of cyberattacks that occur and how companies respond to them.

Customer Data. Payment and accounting system breaches are an important source of cyber risk. One of the largest attacks on a payment network occurred at Target in December 2013 when over 40 million accounts were compromised in a system-wide breach over a three-week period during the holiday shopping season. This attack was followed by several high-profile payment-system breaches at the Home Depot, Michaels Stores, Neiman Marcus, Supervalu, and Staples, as well as franchised owners of UPS Stores, PF Chang’s, and Hard Rock Café. The frequency of credit card breaches has been significantly reduced through chip-card requirements introduced by the major payment networks in 2016; however, they remain an important point of vulnerability.5

Another type of data theft involves penetrating corporate networks or employee devices that store the personal information of clients and employees. This information is then sold in anonymous “dark” markets on the web. Recent examples of personal data theft include Morgan Stanley, Scottrade, and Standard Charter, where hackers or internal employees download the personal information of wealth-management clients, including names, account numbers, and investments. Similarly, health insurance networks such as Anthem, Primera, and CareFirst BlueCross have been targeted by cybercriminals who steal the names, birthdays, addresses, social security numbers and health information of customers. One of the largest breaches of personal data occurred in September 2017 when the credit-reporting firm Equifax reported that personal information on 143 million customers was exposed.

A more unusual example of personal data theft occurred in September 2014 when hackers accessed the Apple iCloud data storage accounts of targeted celebrities, such as actresses Jennifer Lawrence and Kirsten Dunst and model Kate Upton, and stole their personal photos and videos, some of which were released publicly. The individual responsible for hacking these accounts was sentenced to 18 months in prison.6 To improve security, Apple introduced technology to provide automatic email notification when an iCloud account is accessed from a new device or browser.7

Corporate Systems and Data. Customer data is not the sole target of cybercriminals. In 2014, the North Korean government attacked Sony Picture’s IT infrastructure in an attempt to intimidate the company into not releasing a comedy film titled The Interview, which featured a fictional plot to assassinate
North Korea’s real leader. Hackers inserted a malware program, which wiped out half of the company’s computers and servers with a sophisticated algorithm that made data recovery nearly impossible. Sony withheld release of the movie from most theaters but later made it available on demand and in select locations. Similarly, in 2017, rumors circulated that hackers had infiltrated Disney Studios and stole a copy of a forthcoming sequel to the movie Pirates of the Caribbean. Reports alleged that the hackers demanded “an enormous amount of money” in Bitcoin in order not to release the firm. Disney, in cooperation with the FBI, eventually determined that the hack had not been successful.

Company products also are subject to cyber threats when hackers access and assume control over products. The variety of products vulnerable to such attacks is remarkably broad. For example, in 2015 Fiat Chrysler recalled 1.4 million Jeep vehicles after it was determined that a cybersecurity flaw allowed hackers to remotely assume control of the car through wireless communication systems. The company had been aware of the security flaw but issued the recall when it discovered that hackers could remotely control the car’s brakes, transmission, and other electronics. In 2016, a short-selling research firm released a report that cardiac implants produced by medical device company St. Jude Medical were vulnerable to cyberattack. A third party confirmed that in proprietary testing it was successful in gaining control over the company’s Merlin@home implantable cardiac devices that wirelessly monitor patient heartbeat and was able to remotely turn off the devices or, alternatively, deliver an extreme shock that would lead to cardiac arrest. The company subsequently updated product software to reduce the risk of remote access.

Companies are also vulnerable to the theft of proprietary technology or methods of production. In 2016, US Steel was attacked by hackers allegedly linked to the Chinese government who stole methods for producing lightweight steel. That same year, Monsanto discovered that an employee had been working with a foreign government to steal information on the company’s advanced seed technology. The employee loaded “highly sophisticated and unauthorized software” on his computer that allowed a foreign government to monitor his activity remotely and transmit proprietary data.

More mundane but potentially more lucrative cybercrimes involve the theft of corporate information shared between companies and their advisors. For example, in 2016, prominent law firms Cravath Swaine and Weil Gotshal were among a number of law firms hacked by cybercriminals who stole nonpublic information on corporate clients, which could potentially be used for insider trading. Similarly, the servers of accounting firm Deloitte were hacked and files for a small number of clients were accessed. In 2017, the Securities and Exchange Commission revealed that Edgar, the database that stores the corporate filings of all publicly traded companies listed in the U.S., had been accessed, although the agency did not detail what information was stolen.

Finally, companies and their supply chains have been compromised by ransomware attacks in which cybercriminals disrupt computing systems or demand payment under threat of disrupting systems. Two major attacks occurred in 2017. The first involved a ransomware program called WannaCry which infected computers running Microsoft Windows operating system. The program automatically encrypted computer data and demanded payment in Bitcoin for its release. Over 200,000 computers in 150 countries were affected. FedEx and Nissan reported being materially impacted. A second malware attack in July 2017 took down the computing systems of major multinational corporations—such as Merck, Mondelez, and Maersk—and disrupted business operations over multiple days. Maersk announced that widespread computer outages prevented the company’s shipping subsidiary from booking new shipments and providing quotes at selected terminals. Mondelez estimated that the attack reduced second-quarter revenue growth by 3 percentage points.

CORPORATE RESPONSE TO CYBERATTACKS

What actions do corporations take in response to cyberattacks such as these? Many announce steps to improve data security. When customers are affected, they make assurances about their commitment to data protection and offer free credit or identity-theft monitoring. Almost invariably, the company is sued and enters into a settlement (see Exhibit 3).

Beyond this, however, surprisingly little happens in terms of holding individuals accountable or structural changes that improve cybersecurity expertise at the senior-executive and board levels. For example, among a sample of approximately 50 cybersecurity breaches over the last five years, we find that the CEO is fired or steps down in only a handful of cases. Exceptions include massive data breaches such as those at Target, Equifax, and the website Ashley Madison, in which hackers stole and published the names of 32 million (potentially unfaithful) clients. Executive pay is almost never reduced. The CEO of Target received no bonus and forfeited $5 million in pension benefits after 40 million credit card accounts were stolen; however, the CEO of the Home Depot suffered no decrease in compensation after more than 50
We found only one instance of a company making changes to an executive compensation plan to incorporate cybersecurity risk. JPMorgan added cybersecurity as part of the annual performance plans of both its CEO and COO.

Whether governance changes such as these are sufficient to compensate shareholders for the costs incurred in a cyberattack is unclear. Verizon Communications reduced the amount that it offered to pay for Yahoo!’s internet properties by $350 million after Yahoo! disclosed that hackers had stolen the birthdays, email addresses, and passwords of over 1 billion users (later increased to 3 billion users). A spokesperson for Yahoo! described the reduced purchase price as “a fair and favorable outcome.”

To decrease the risk of a cyber threat, some experts recommend the following:

- Elevate cybersecurity within the company’s risk framework. The board should ensure that management and employees take cybersecurity seriously. They should periodically review the company’s potential exposure and cybersecurity policies.
- Develop an action plan to respond to a breach in customer data. The plan should outline employee and board responsibilities, who should be contacted and when, how the company will communicate to the public, and how the breach will be assessed.
- Implement additional safeguards to protect corporate data. Management and the board should review who has access to critical corporate data and trade secrets, and develop policies around how this information is documented, stored, accessed and shared within the company. The board should have its own cybersecurity policies to protect director communications, documents, and conversations.

**WHY THIS MATTERS**

1. In recent years, cyberattacks on corporate data have increased in frequency and cost. At the same time, experience has shown that a wide variety of data—not just customer but also corporate data—are the target of such attacks. What steps can the board and management teams take to prepare for and respond to cyber threats? What practical steps can they take to mitigate or prevent them?

2. Observation suggests that companies make very few governance changes in response to major cyberattacks. Senior executives are rarely terminated. Their pay packages are rarely reduced or restructured to reward data protection. Cyber expertise is not a central qualification or requirement of most board members. Why? Do boards not appreciate the scope and severity of cyber threats? Or do they believe that they have sufficient policies in place to deal with them?
3. Cyberattacks represent a major risk to organizations: the cost of a breach is high, the variety of attacks broad, and the technological issues sophisticated. What data, metrics, and information should board members review to satisfy themselves that management has taken proper steps to minimize cyber risks? What qualifications should a board member have in order to constructively contribute to boardroom discussions on cybersecurity? How difficult is it to find board candidates with these skills?

---

5. According to data from Visa, chip-enabled merchants experienced a 26 percent drop in counterfeit fraud year-over-year in January 2016, following the first rollout of new credit and debit card chip technology. See Andrew Meola, “Visa Is Significantly Reducing Fraud,” Business Insider (June 9, 2016).
17. At the time of the data breach, the company was in the middle of a CEO transition. Neither the outgoing CEO nor his successor saw a reduction in bonus or performance awards as a result of the breach. Key performance indicators (KPIs) for the annual bonus plan were sales, operating profit, and inventory turns; KPIs for long-term equity awards were three-year return on invested capital and operating profit. Neither payment was decreased because of the data breach.
Critical Update Needed

EXHIBIT 1 — DATA BREACHES BY CATEGORY

Data breach is defined as an incident in which an individual name plus social security number, driver’s license number, medical record, or financial record (including credit or debit card numbers) is potentially at risk because of exposure.

Source: Identity Theft Resource Center (ITRC).
EXHIBIT 2 — SURVEY DATA: BOARD OF DIRECTORS ON CYBERSECURITY

HOW CONFIDENT ARE YOU THAT YOUR COMPANIES ARE PROPERLY SECURED AGAINST CYBERATTACKS?

- Very confident
- Confident
- Less than confident

HOW OFTEN ARE CYBERSECURITY MATTERS DISCUSSED DURING BOARD MEETINGS?

- Every meeting: 35%
- Most meetings: 46%
- Only after internal or industry incident: 18%
- Never: 1%

## EXHIBIT 3 — COST TO SETTLE CLASS ACTION LAWSUITS FOR DATA THEFT (SELECTED)

<table>
<thead>
<tr>
<th>Defendant</th>
<th>Approval</th>
<th>Data Type</th>
<th>Relief to Class</th>
<th>Service Awards, Fees, &amp; Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Depot</td>
<td>2016</td>
<td>Card data</td>
<td>Up to $1.1 million for class claims; up to $65 million of 18 months of credit monitoring services; security practice changes</td>
<td>$1,000 for each representative plaintiff; $166,925 in costs; $7,536 million in fees</td>
</tr>
<tr>
<td>Target</td>
<td>2016</td>
<td>Card data</td>
<td>Up to $20.25 million for class claims; $10,108 million for MasterCard, reportedly up to $67 million for Visa's claims against Target</td>
<td>$29,000 for 5 representative plaintiffs; $2.189 million in costs; $17.8 million in fees</td>
</tr>
<tr>
<td>Sony</td>
<td>2016</td>
<td>Login and personal information</td>
<td>Up to $2 million for preventative losses; up to $2.5 million for claims for identity theft losses; up to two years of credit monitoring services.</td>
<td>$8,000 for each named plaintiff; $1,000 for each plaintiff who initially filed a motion; $2,588 million in fees</td>
</tr>
<tr>
<td>St. Joseph Health System</td>
<td>2016</td>
<td>Health information</td>
<td>$7.5 million in cash payment; up to $5 million for class claims; one year of credit monitoring services offered during remediation; security practice changes</td>
<td>$80,000 in incentive payments for class representatives; $7.45 million in fees and costs</td>
</tr>
<tr>
<td>Target</td>
<td>2015</td>
<td>Card data</td>
<td>Up to $1.8 million for claims; security practice changes</td>
<td>$1,000 for three deposited plaintiffs; $500 for other plaintiffs; $6,75 million in fees</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>2015</td>
<td>Login information</td>
<td>Up to $1.25 million for claims; security practices changes</td>
<td>$5,000 for named plaintiff; $2,669 in costs; $12,500 in fees</td>
</tr>
<tr>
<td>Adobe</td>
<td>2015</td>
<td>Login and card data</td>
<td>Security practice changes and audit</td>
<td>$5,000 to each individual plaintiff; $1.38 million in fees</td>
</tr>
<tr>
<td>Sony/Gaming Networks</td>
<td>2015</td>
<td>Card data and personal information</td>
<td>Up to $1 million for identity theft losses; benefit options including free games and themes or month subscription, unused wallet credits, virtual currency; some small cash payments</td>
<td>$2.75 million in fees</td>
</tr>
<tr>
<td>AvMed</td>
<td>2014</td>
<td>Personal information</td>
<td>Up to $3 million; security practice changes</td>
<td>$5,000 for each representative plaintiff; $750,000 in fees</td>
</tr>
<tr>
<td>Winn-Dixie</td>
<td>2013</td>
<td>Personal information</td>
<td>Up to $225,000 for class claims; up to one year of credit monitoring services; security practice changes</td>
<td>$3,500 for representative plaintiff; $200,000 in fees</td>
</tr>
<tr>
<td>CDF Systems</td>
<td>2013</td>
<td>Health information</td>
<td>Up to $586,000 for claims for expenses; up to $2 million for class claims for identity theft; two years of credit monitoring services; security practices changes</td>
<td>$5,000 for representative plaintiff; $14,954 in costs; $565,936 in fees</td>
</tr>
<tr>
<td>Michaels Stores</td>
<td>2013</td>
<td>Card data</td>
<td>Up to $806,000 for class claims; up to two years of credit monitoring services; security practice changes</td>
<td>$2.500 for each representative plaintiff; $55,565 in costs; $1.2 million in fees</td>
</tr>
</tbody>
</table>