paloalto NETWORKS | NYSE

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

Georgia Tech Institute for Information Security & Privacy | Internet Security Alliance

NAVIGATING THE DIGITAL AGE:
The Definitive Cybersecurity Guide for Directors and Officers

Published by

CAXTON
Business & Legal inc.

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers

Publisher: Tim Dempsey

Editor: Matt Rosenquist

Design and Composition: Graphic World, Inc.

Printing and Binding: Transcontinental Printing

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers
is published by:
Caxton Business & Legal, Inc.
27 North Wacker Drive, Suite 601
Chicago, IL 60606
Phone: +1 312 361 0821
Email: tjd@caxtoninc.com

First published: 2015
ISBN: 978-0-9964982-0-3

Cover illustration by Tim Heraldo

DISCLAIMER

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers (the Guide) contains summary information about legal and regulatory aspects of cybersecurity governance and is current as of the date of its initial publication (October 2015). Although the Guide may be revised and updated at some time in the future, the publishers and authors do not have a duty to update the information contained in the Guide, and will not be liable for any failure to update such information. The publishers and authors make no representation as to the completeness or accuracy of any information contained in the Guide.

This guide is written as a general guide only. It should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided. Every effort has been made to ensure that the information in this guide is correct at the time of publication. The views expressed in this guide are those of the authors. The publishers and authors do not accept responsibility for any errors or omissions contained herein. It is your responsibility to verify any information contained in the Guide before relying upon it.

Introduction

New York Stock Exchange – Tom Farley, President

No issue today has created more concern within corporate C-suites and boardrooms than cybersecurity risk. With the ability to shatter a company's reputation with their customers and draw criticism from shareholders, lawsuits from affected parties, and attention from the media, the threat of cyber risk is ubiquitous and insidious. No company, region, or industry is immune, which makes the responsibility to oversee, manage, and mitigate cyber risk a top-down priority in every organization.

The New York Stock Exchange has long advocated that exemplary governance and risk oversight is fundamental to the health of individual companies, as well as to the sound operation of our capital markets. In other words, we too take the threat very seriously. Today, managing cybersecurity risk has expanded far beyond the realm of IT; it has become a business continuity necessity to ensure shareholder value remains intact and that privacy and corporate intellectual property is protected. Accordingly, those responsibilities are weighing heavily on corporate executives and directors, making it vital for them to better understand and prepare for the evolving cybersecurity landscape.

Cyber risk ultimately poses a threat to confidence, a foundational aspect of U.S. corporate issuers and markets. We are taking a leadership role on many fronts, such as reducing market fragmentation and complexity, as well as increasing efficiency through the highest levels of intelligence, analytics, and technology. Confidence in the integrity and security of our assets is concurrent with our success—as it is for every other company operating in the public markets today.

Moreover, because the public markets have become increasingly reliant on interdependent technology systems, the threat looms even larger. As we witnessed during the 2008 financial crisis, rarely does any failure happen in a vacuum; therefore, the threat of systemic disruption has taken on an even higher level of prominence and concern among regulators and policymakers worldwide.

It is important that companies remain vigilant, taking steps to proactively and intelligently address cybersecurity

risk within their organizations. Beyond the technological solutions developed to defend and combat breaches, we can accomplish even more through better training, awareness, and insight on human behavior. Confidence, after all, is not a measure of technological systems, but of the people who are entrusted to manage them.

With insights from the preeminent authorities on cybersecurity today, this groundbreaking, practical guide to cybersecurity has been developed to reflect a body of knowledge that is unsurpassed on this topic. At the heart of effective risk management must be a thorough understanding of the risks as well as pragmatic solutions. Thank you for your continued partnership with the New York Stock Exchange, and we look forward to continuing to support your requirements in this dynamic landscape.

Foreword

Visa Inc. – Charles W. Scharf, CEO

For years, cybersecurity was an issue that consumers, executive management, and boards of directors took for granted. They were able to do so because the technologists did not. The technologists worked every day to protect their systems from attack, and they were quite effective for many years. We sit here today in a very different position. The threats are bigger than ever before and growing in frequency and severity every day. Cybersecurity is now something everyone needs to think about, whether it's in your personal or professional life. What worked in the past is not enough to protect us in the present and future.

So what has changed?

First of all, the technology platforms of today are bigger targets than ever given the breadth and criticality of items they control. Second, the amount and value of the data that we all produce and store has grown exponentially. The data is a gold mine for criminals. Third, the interconnectedness of the world just makes it easier for more people—regardless of geography—to be able to steal or disrupt. And fourth, the perpetrators are more sophisticated, better organized, better funded, and harder to bring to justice than ever before.

So the problem is different, and what we all do about it is different.

This is not simply an IT issue. It is a business problem of the highest level. Protecting our data and our systems is core to business today. And that means that having an outstanding cybersecurity program also can't detract from our objectives around innovation, speed, and performance.

Security has been a top priority at Visa for decades. It is foundational to delivering our brand promise. To be the *best* way to pay and be paid, we must be the *most secure* way to pay and be paid. We cannot ask people to use our products unless they believe that we are just that. Thus we must guard carefully both the security of our own network and company and the security of the broader payments ecosystem.

There are several elements that we have found to be critical to ensuring an effective security program at Visa.

- Be open and honest about the effectiveness of your security program and regularly share an honest assessment of your security posture with the executive team and board.

  We use a data-driven approach that scores our program across five categories: risk intelligence, malware prevention, vulnerability management, identity and access management, and detection and response. Scores move up and down not only as our defenses improve or new vulnerabilities are discovered but also as threats change. The capabilities of the adversaries are growing, and you need a dynamic approach to measurement.

- Invest in security before investing elsewhere. A well-controlled environment gives you the license to do other things. Great and innovative products and services will only help you win if you have a well-protected business.
- Don't leave the details to others. Active, hands-on engagement by the executive team and the board is required. The risk is existential. Nothing is more important. Your involvement will produce better results as well as make sure the whole organization understands just how important the issue is.
- Never think you've done enough. The bad guys are smart and getting smarter. They aren't resting, and they have more resources than ever. Assume they will attack.

Defending against cyberthreats is not something that we can solve for our company in a vacuum. At Visa, we must protect not only our own network but the whole payments ecosystem. This came to life for us in late 2013 when some of the largest U.S. retailers and financial institutions in the U.S. reported data breaches. Tens of millions of consumer accounts had been compromised—a pivotal moment for our industry.

The losses experienced by our clients, combined with the impact on consumer confidence, galvanized our industry to take actions that, we believe, will have a meaningful and lasting effect on how the world manages sensitive consumer data—not just payments.

We are taking action as an ecosystem, to collaborate and share information across industries and with law enforcement and governments and to develop new technologies that will allow us to prevent attacks and respond to threats in the future.

- Protect payments at physical retailers. Fraudsters have targeted the point-of-sale environment at leading U.S. retailers, capturing consumer account information and forcing the reissuance of millions of payment cards. As an industry we are rapidly introducing EMV (Europay, MasterCard, and Visa) chip payment technology in the United States. Chip-enabled payment cards and terminals work in concert to generate dynamic data with each transaction, rendering the transaction data useless to fraudsters.
- Protect online payments. Consumer purchases online and with mobile devices are growing at a significant rate. In order to prevent cyberattacks and fraudulent use of consumer accounts online, Visa and the global payments industry adopted a new payment standard for online payments. The new standard replaces the 16-digit account number with a digital token that is used to process online payments without exposing consumer account information.
- Collaborate and share information. Sharing threat intelligence is a necessity rather than a "nice to have," allowing merchants, financial institutions, and payment networks like Visa to rapidly detect and respond to cyberattacks. Public and private partnerships are also critical to creating the most robust

community of threat intelligence, so we also work closely with law enforcement and governments. At the heart of Visa's security strategy is the concept of "cyber fusion," which is centered on the principle of shared intelligence—a framework to collect, analyze, and leverage cyberthreat intelligence, internally and externally, to build a better defense for the whole ecosystem.

Championing security is one of Visa's six strategic goals. This is an area where there are no grades—it is pass or fail, and pass is the only option. Cybersecurity needs to be part of the fabric of every company and every industry, integrated into every business process and every employee action. And it begins and ends at the top. It is job number one.

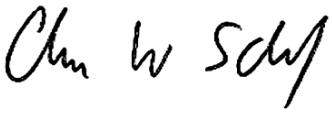

TABLE OF CONTENTS

V. Design best practices

VI. Cybersecurity beyond your network

VII. Incident response

8

The risks to boards of directors and board member obligations

Orrick, Herrington & Sutcliffe LLP – Antony Kim, Partner; Aravind Swaminathan, Partner; and Daniel Dunne, Partner

As cyberattacks and data breaches continue to accelerate in number and frequency, boards of directors are focusing increasingly on the oversight and management of corporate cybersecurity risks. Directors are not the only ones. An array of federal and state enforcement agencies and regulators, most notably the Department of Justice (DOJ), Department of Homeland Security (DHS), Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), and state Attorneys General, among others, identify board involvement in enterprise-wide cybersecurity risk management as a crucial factor in companies' ability to appropriately establish priorities, facilitate adequate resource allocation, and effectively respond to cyberthreats and incidents. As SEC Commissioner Luis A. Aguilar recently noted, "Boards that choose to ignore, or minimize, the importance of cybersecurity responsibility do so at their own peril."[1] Indeed, even apart from the regulators, aggressive plaintiffs' lawyers, and activist shareholders are similarly demanding that boards be held accountable for cybersecurity. Shareholder derivative actions and activist investor campaigns to oust directors are becoming the norm in high-profile security breaches.

Directors have clearly gotten the message. A survey by the NYSE Governance Services (in partnership with a leading cybersecurity firm) found that cybersecurity is discussed at 80% of all board meetings. However, the same survey revealed that only 34% of boards are confident about their respective companies' ability to defend themselves against a cyberattack. More troubling, a June 2015 study by the National Association of Corporate Directors found that only 11% of respondents believed their boards possessed a high level of understanding of the risks associated with cybersecurity.[2] This is a difficult position to be in: aware of the magnitude of the risks at hand but struggling

to understand and find solutions to address and mitigate them.

In this chapter, we explore the legal obligations of boards of directors, the risks that boards face in the current cybersecurity landscape, and strategies that boards may consider in mitigating that risk to strengthen the corporation and their standing as dutiful directors.

I. Obligations of Board Members

The term "cybersecurity" generally refers to the technical, physical, administrative, and organizational safeguards that a corporation implements to protect, among other things, "personal information,"[3] trade secrets and other intellectual property, the network and associated assets, or as applicable, "critical infrastructure."[4] This definition alone should leave no doubt that a board of directors' role in protecting the corporation's "crown jewels" is essential to maximizing the interests of the corporation's shareholders.

Generally, directors owe their corporation fiduciary duties of good faith, care, and loyalty, as well as a duty to avoid corporate waste.[3] The specific contours of these duties are controlled by the laws of the state in which the company is incorporated, but the basic principles apply broadly across most jurisdictions (with Delaware corporations law often leading the way). More specifically, directors are obligated to discharge their duties in good faith, with the care an ordinarily prudent person would exercise in the conduct of his or her own business under similar circumstances, and in a manner that the director reasonably believes to be in the best interests of the corporation. To encourage individuals to serve as directors and to free corporate decision making from judicial second-guessing, courts apply the "business judgment rule." In short, courts presume that directors have acted in good faith and with reasonable care after obtaining all material information, unless proved otherwise; a powerful presumption that is difficult for plaintiffs to overcome, and has led to dismissal of many legal challenges to board action or inaction. To maximize their personal protection, directors must ensure that, if the unthinkable happens and their corporation falls victim to a cybersecurity disaster, they have already taken the steps necessary to preserve this critical defense to personal liability.

In the realm of cybersecurity, the board of directors has "risk oversight" responsibility: the board does not itself *manage* cybersecurity risks; instead, the board oversees the corporate systems that ensure that management is doing so effectively. Generally, directors will be protected by the business judgment rule and will not be liable for a failure of oversight unless there is a "sustained or systemic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists." This is known as the *Caremark* test,[5] and there are two recognized ways to fall short: first, the directors intentionally and entirely fail to put *any* reporting and control system in place; or second, if there is a reporting and control system, the directors refuse to monitor it or fail to act on warnings they receive from the system.

The risk that directors will face personal liability is especially high where the board has not engaged in *any* oversight of their corporations' cybersecurity risk. This is a rare case, but other risks are more prevalent. For example, a director may fail to exercise due care if he or she makes a decision to discontinue funding an IT security project without getting any briefing about current cyberthreats the corporation is facing, or worse, after being advised that termination of the project may expose the company to serious threats. If an entirely uninformed or reckless decision to de-fund renders the corporation vulnerable to known or anticipated risks that lead to a breach, the members of the board of directors could be individually liable for breaching their *Caremark* duties.

II. The Personal Liability Risk to Directors

Boards of directors face increasing litigation risk in connection with their responsibilities

for cybersecurity oversight, particularly in the form of shareholder derivative litigation, where shareholders sue for breaches of directors' fiduciary duties to the corporation. The rise in shareholder derivative suits coincides with a 2013 Supreme Court decision limiting the viability of class actions that fail to allege a nonspeculative theory of consumer injury resulting from identity theft.[6] Because of a lack of success in consumer class actions, plaintiffs' lawyers have been pivoting to shareholder derivative litigation as another opportunity to profit from massive data breaches.

In the last five years, plaintiffs' lawyers have initiated shareholder derivative litigation against the directors of four corporations that suffered prominent data breaches: Target Corporation, Wyndham Worldwide Corporation, TJX Companies, Inc., and Heartland Payment Systems, Inc. Target, Heartland, and TJX each were the victims of significant cyberattacks that resulted in the theft of approximately 110, 130, and 45 million credit cards, respectively. The Wyndham matter, on the other hand, involved the theft of only approximately 600,000 customer records; however, unlike the other three companies, it was Wyndham's *third* data breach in approximately 24 months that got the company and its directors in hot water. The signs point to Home Depot, Inc., being next in line. A Home Depot shareholder recently brought suit in Delaware seeking to inspect certain corporate books and records. A "books and records demand" is a common predicate for a shareholder derivative action, and this particular shareholder has already indicated that the purpose of her request is to determine whether Home Depot's management breached fiduciary duties by failing to adequately secure payment information on its data systems, allegedly leading to the exposure of up to 56 million customers' payment card information.

Although there is some variation in the derivative claims brought to date, most have focused on two allegations: that the directors breached their fiduciary duties by making a decision that was ill-advised or negligent, or by failing to act in the face of a reasonably known cybersecurity threat. Recent cases have included allegations that directors:

- failed to implement and monitor an effective cybersecurity program;
- failed to protect company assets and business by recklessly disregarding cyberattack risks and ignoring red flags;
- failed to implement and maintain internal controls to protect customers' or employees' personal or financial information;
- failed to take reasonable steps to timely notify individuals that the company's information security system had been breached;
- caused or allowed the company to disseminate materially false and misleading statements to shareholders (in some instances, in company filings).

Board members may not be protected from liability by the exculpation clauses in their corporate charters. Although virtually all corporate charters exculpate board members from personal liability to the fullest extent of the law, Delaware law, for example, prohibits exculpation for breaches of the duty of loyalty, or breaches of the duty of good faith involving "intentional misconduct" or "knowing violations of law." As a result, because the Delaware Supreme Court has characterized a *Caremark* violation as a breach of the duty of loyalty,[7] exculpation of directors for *Caremark* breaches may be prohibited. In addition, with the myriad of federal and state laws that touch on privacy and security, directors may also lose their immunity based on "knowing violations of law." Given the nature of shareholder allegations in derivative litigation, these are important considerations, and importantly, vary depending on the state of incorporation.

Directors should also be mindful of standard securities fraud claims that can be brought against companies in the wake of a data breach. Securities laws generally prohibit public companies from making material

statements of fact that are false or misleading. As companies are being asked more and more questions about data collection and protection practices, directors (and officers) should be careful about statements that are made regarding the company's cybersecurity posture and should focus on tailoring cybersecurity-related risk disclosures in SEC filings to address the specific threats that the company faces.

Cybersecurity disclosures are of keen interest to the SEC, among others. Very recently, the SEC warned companies to use care in making disclosures about data security and breaches and has launched inquiries to examine companies' practices in these areas. The SEC also has begun to demand that directors (and boards) take a more active role in cybersecurity risk oversight.

Litigation is not the only risk that directors face. Activist shareholders—who are also customers/clients of corporations—and proxy advisors are challenging the re-election of directors when they perceive that the board did not do enough to protect the corporation from a cyberattack. The most prominent example took place in connection with Target's data breach. In May 2014, just weeks after Target released its CEO, Institutional Shareholder Services (ISS), a leading proxy advisory firm, urged Target shareholders to seek ouster of seven of Target's ten directors for "not doing enough to ensure Target's systems were fortified against security threats" and for "failure to provide sufficient risk oversight" over cybersecurity.

Thoughtful, well-planned director involvement in cybersecurity oversight, as explained below, is a critical part of a comprehensive program, including indemnification and insurance, to protect directors against personal liability for breaches. Moreover, it can also assist in creating a compelling narrative that is important in brand and reputation management (as well as litigation defense) that the corporation acted responsibly and reasonably (or even more so) in the face of cybersecurity threats.

III. Protecting Boards of Directors

From a litigation perspective, boards of directors can best protect themselves from shareholder derivative claims accusing them of breaching their fiduciary duties by diligently overseeing the company's cybersecurity program and thereby laying the foundation for invoking the business judgment rule. Business judgment rule protection is strengthened by ensuring that board members receive periodic briefings on cybersecurity risk and have access to cyber experts whose expertise and experience the board members can rely on in making decisions about what to do (or not to do) to address cybersecurity risks. Most importantly, directors cannot recklessly ignore the information they receive, but must ensure that management is acting reasonably in response to reported information the board receives about risks and vulnerabilities.

Operationally, a board can exercise its oversight in a number of ways, including by (a) devoting board meeting time to presentations from management responsible for cybersecurity and discussions on the subject, to help the board become better acquainted with the company's cybersecurity posture and risk landscape; (b) directing management to implement a cybersecurity plan that incentivizes management to comply and holds it accountable for violations or noncompliance; (c) monitoring the effectiveness of such plan through internal and/or external controls; and (d) allocating adequate resources to address and remediate identified risks. Boards should invest effort in these actions, on a repeated and consistent basis, and make sure that these actions are clearly documented in board and committee packets, minutes, and reports.

(a) **Awareness.** Boards should consider appointing a chief information security officer (CISO), or similar officer, and meet regularly with that individual and other experts to understand the company's risk landscape, threat actors, and strategies to address

that risk. Appointing a CISO has an additional benefit. Reports suggest that companies that have a dedicated CISO detected more security incidents and reported lower average financial losses per incident.[8]

Boards should also task a committee or subcommittee with responsibility for cybersecurity oversight, and devote time to getting updates and reports on cybersecurity from the CISO on a periodic basis. As with audit committees and accountants, boards can improve oversight by recruiting a board member with aptitude for the technical issues that cybersecurity presents, and placing that individual on the committee/subcommittee tasked with responsibility for cybersecurity oversight. Cybersecurity presentations, however, need not be overly technical. Management should use established analytical risk frameworks, such as the National Institute for Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity," (usually referred to as the "NIST Cybersecurity Framework") to assess and measure the corporation's current cybersecurity posture. These kinds of frameworks are critical tools that have an important role in bridging the communication and expertise gaps between directors and information security professionals and can also help translate cybersecurity program maturity into metrics and relative relationship models that directors are accustomed to using to make informed decisions about risk. It is principally through their use that directors can become sufficiently informed to exercise good business judgment.

(b) **Plan implementation and enforcement.** Boards should require that management implement an enterprise-wide cybersecurity risk management plan and align management's incentives to meet those goals. Although the details of any cybersecurity risk management plan should differ from company to company, the CISO and management should prepare a plan that includes proactive cybersecurity assessments of the company's network and systems, builds employee awareness of cybersecurity risk and requires periodic training, manages engagements with third parties that are granted access to the company's network and information, builds an incident response plan, and conducts simulations or "tabletop" exercises to practice and refine that plan. The board should further consider incentivizing the CISO and management for company compliance with cybersecurity policies and procedures (e.g., bonus allocations for meeting certain benchmarks) and create mechanisms for holding them responsible for noncompliance.

(c) **Monitor compliance.** With an enterprise-wide cybersecurity risk management plan firmly in place, boards of directors should direct that management create internal and external controls to ensure compliance and adherence to that plan. Similar to internal financial controls, boards should direct management to test and certify compliance with cybersecurity policies and procedures. For example, assuming that management establishes a policy that software patches be installed within 30 days of release, management would conduct a patch audit, confirm that all patches have been implemented, and have the CISO certify the results. Alternatively, boards can also retain independent cybersecurity firms that could be engaged by the board to conduct an audit, or validate compliance with cybersecurity policies and procedures, just as they would validate financial results in a financial audit.

(d) **Adequate resource allocation.** With information in hand about what the

company's cybersecurity risks are, and an analysis of its current posture, boards should allocate adequate resources to address those risks so that management is appropriately armed and funded to protect the company.

As criminals continue to escalate the cyber-war, boards of directors will increasingly find themselves on the frontlines of regulatory, class plaintiff, and shareholder scrutiny. Directors are well-advised to proactively fulfill their risk oversight functions by driving senior management toward a well-developed and resilient cybersecurity program. In so doing, board members will not only better protect themselves against claims that they failed to discharge their fiduciary duties, but will strengthen their respective organizations' ability to detect, respond, and recover from cybersecurity crises.

Endnotes

1. SEC Commissioner Luis A. Aguilar, Remarks at the N.Y. Stock Exchange, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014).
2. Press Release, Nat'l Assoc. of Corp. Dir., Only 11% of Corporate Directors Say Boards Have High Level of Cyber-Risk Understanding (June 22, 2015) https://www.nacdonline.org/AboutUs/PressRelease.cfm?ItemNumber=15879.
3. Personal information is defined under a variety of federal and state laws, as well as industry guidelines, but is generally understood to refer to data that may be used to identify a person. For example, state breach notification laws in the U.S. define personal information, in general, as including first name (or first initial) and last name, in combination with any of the following: (a) social security number; (b) driver's license number or other government-issued identification; (c) financial or credit/debit account number plus any security code necessary to access the account; or (d) health or medical information.
4. Critical infrastructure refers to systems, assets, or services that are so critical that a cyberattack could cause serious harm to our way of life. Presidential Policy Directive 21 (PPD-21) identifies the following 16 critical infrastructure sectors: chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear, transportation, waste, and wastewater. *See* Critical Infrastructure Sectors, Department of Homeland Security, *available at* http://www.dhs.gov/critical-infrastructure-sector.
5. For Delaware corporations, directors' compliance with their oversight function is analyzed under the test set out in *In re Caremark Int'l, Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).
6. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013). Consistent with *Clapper*, most data breach consumer class actions have been dismissed for lack of "standing": the requirement that a plaintiff has suffered a cognizable injury as a result of the defendant's conduct. That has proven challenging for plaintiffs because consumers are generally indemnified by banks against fraudulent charges on stolen credit cards, and many courts have rejected generalized claims of injury in the form of emotional distress or exposure to heighted risk of ID theft or fraud.
7. *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).
8. Ponemon Inst., 2015 Cost of Data Breach Study: Global Analysis (May 2015), http://www-03.ibm.com/security/data-breach/.