Cyber-Risk Oversight

Executive Summary

DIRECTOR'S HANDBOOK SERIES
2014 EDITION

PUBLISHED BY NACD IN
COLLABORATION WITH AIG AND ISA

AIG

INTERNET SECURITY ALLIANCE

NACD®
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Cyber-Risk Oversight

DIRECTOR'S HANDBOOK SERIES
2014 EDITION

Prepared By Larry Clinton
President & CEO, Internet Security Alliance

NACD®
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Acknowledgements

We wish to thank the following individuals for their contributions to this handbook (in alphabetical order by organization); Mark Camillo, Tracie Grella, Mike Snow, and Gil Vega, AIG; Tom Quinn, Bank of NY Mellon; Joe Buonomo and Bob Gardner, DCR; Ed Batts, Jim Halpert, and Nate McKitterick, DLA Piper; Arnold Bell and Larry Trittschuh, GE; Melissa Hathaway, Hathaway Global Strategies; Tanner Doucet and Josh Magri, Internet Security Alliance; Charlie Croom, Lockheed-Martin; J.R. Williamson, Northrup Grumman; Jeff Brown, Raytheon; Gary McAlum, USAA; Marcus Sachs, Verizon; and Richard Knowlton, Vodafone.

National Association of Corporate Directors

MANAGING DIRECTOR **Peter R. Gleason**
CHIEF KNOWLEDGE OFFICER **Alexandra R. Lajoux**
RESEARCH DIRECTOR **Robyn Bew**
SENIOR MANAGER, RESEARCH **Katherine Iannelli**
RESEARCH ANALYST **Adam Lee**
RESEARCH ANALYST **Matt Abedi**
RESEARCH ANALYST **Ted Sikora**
NACD DIRECTORSHIP EDITOR-IN-CHIEF **Judy Warner**
ART DIRECTOR **Patricia W. Smith**
GRAPHIC DESIGNER **Alex Nguyen**
PUBLICATIONS EDITOR **Carolyn Fischer**
NACD DIRECTORSHIP ASSISTANT EDITOR **Jesse Rhodes**

Table of Contents

Introduction

In the past 20 years, the nature of corporate asset value has changed significantly, shifting away from the physical and toward the virtual. One recent study found that 80 percent of the total value of the Fortune 500 now consists of intellectual property (IP) and other intangibles.[1] Along with the rapidly expanding "digitization" of corporate assets, there has been a corresponding digitization of corporate risk. Accordingly, policymakers, regulators, shareholders, and the public are more attuned to corporate cybersecurity risks than ever before. Organizations are at risk from the loss of IP and trading algorithms, destroyed or altered data, declining public confidence, harm to reputation, disruption to critical infrastructure, and new legal and regulatory sanctions. Each of these risks can adversely affect competitive positioning, stock price, and shareholder value.

Leading companies view cyber risks in the same way they do other critical risks—in terms of a risk-reward trade off. This is especially challenging in the cyber arena for two reasons. First, the complexity of cyber threats has grown dramatically. Corporations now face increasingly sophisticated events that outstrip traditional defenses. As the complexity of these attacks increases, so does the risk they pose to corporations. As noted above, the potential effects of a data breach are expanding well beyond information loss to include significant damage in other areas. Second, competitive pressures to deploy increasingly cost-effective business technologies often affect resource investment calculations. These two competing pressures on corporate staff and business leaders mean that conscientious and comprehensive oversight at the board level is essential.

NACD, in conjunction with AIG and the Internet Security Alliance, has identified five steps all corporate boards should consider as they seek to enhance their oversight of cyber risks. This handbook is organized according to these five key principles:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Some estimates predict that between $9 and $21 trillion of global economic value creation could be at risk if companies and governments are unable to successfully combat cyber threats.

A rapidly evolving cyber-threat landscape

As recently as a few years ago, cyberattacks were largely the province of hackers and a few highly sophisticated individuals. While problematic, many corporations could chalk up these events as simply a frustrating cost of doing business.

Today, corporations are subject to attackers who are part of ultra-sophisticated teams that deploy increasingly targeted malware against systems and individuals in multi-staged, stealthy attacks. These attacks, sometimes referred to as advanced persistent threats (APTs), were first deployed against government entities and defense contractors. More recently, they have migrated throughout the economy, meaning that virtually any company is at risk.

One of the defining characteristics of these attacks is that they can penetrate virtually all of a company's perimeter defense systems, such as firewalls or intrusion detection systems: intruders look at multiple avenues to exploit all layers of security vulnerabilities until they achieve their goal. In other words, if a sophisticated attacker targets a company's systems, they will almost certainly breach them.

In addition, company subcontractors and employees—whether disgruntled or merely poorly trained—present at least as big an exposure for companies as attacks from the outside. This highlights the need for a strong and adaptable security program, equally balanced between external and internal cyber threats. Put simply, companies can't deal with advanced threats if they are unable to stop low-end attacks.[2]

Government agencies have focused primarily on defending the nation's critical infrastructure (including power and water supplies, communication and transportation networks, and the like) from cyberattack. While such attacks are technically possible and could have very serious consequences, 95 percent of incidents are economically motivated, according to some estimates.[3] Cyberattackers routinely attempt to steal all manner of corporate data, including personal information, credit data, business plans, trade secrets, and intellectual property. It is difficult to gauge the total damage from cyberattacks, but estimates generally put it at hundreds of billions of dollars annually.[5] Projections of future losses are even more chilling: according to a 2013 study, between $9 trillion and $21 trillion of global economic value creation in the next five to seven years could be at risk if organizations and governments are unable to adopt successful strategies to combat cyber threats.[6]

Moreover, although many smaller and medium-size companies have historically believed that they were too insignificant to be a target, that perception is wrong. In fact, the majority of cyberattacks are levied against smaller organizations[7] that have fewer security resources. In addition to being targets in their own right, smaller firms are often an attack pathway into larger organizations via customer, supplier, or joint venture relationships, making vendor and partner management a critical function for all interconnected entities.

There is general consensus in the cybersecurity field that attackers are well ahead of the corporations that have to defend themselves. Cyberattacks are relatively inexpensive yet highly profitable, and the required resources and skills are easy to acquire. It is no wonder that many observers believe cyber defense tends to lag a generation behind the attacker. It is difficult to demonstrate return on investment (ROI) for preventing attacks, and successful law enforcement response is virtually nonexistent. According to some estimates, less than 1 percent of cyberattackers are successfully prosecuted.[8]

This does not mean that defense is impossible, but it does mean that corporate boards need to ensure that management is fully engaged in developing defense and response plans as sophisticated as the attack methods, or otherwise put their company's core assets at considerable risk.

Balancing cybersecurity with profitability

Similar to other critical risks, cybersecurity cannot be considered in a vacuum. Members of management and the board must strike the appropriate balance between protecting the security of the organization and mitigating downside losses, while continuing to ensure profitability and growth in a competitive environment.

Many technical innovations and business practices that en-

Greater Connectivity, Higher Risk

Due to the immense amount of interconnection among corporate systems, it is no longer adequate that organizations secure only "their" network. Vendors, suppliers, partners, customers, or any entity connected with the company electronically can become a potential point of vulnerability.

In 2014, a major oil company's systems were breached when a sophisticated attacker who was unable to penetrate the network instead inserted malware into the online menu of a Chinese restaurant popular with employees. Once inside the company's system, the intruders were able to attack its core business.[4]

Other high-profile breaches have been not the result of outside intruders but rather employees or contractors who were given access to the company's network. In 2013, contractor Edward Snowden compromised one of the supposedly most secure organizations in the world—the U.S. National Security Agency—from the inside. A couple of years earlier, Pvt. Bradley (now Chelsea) Manning stole a massive amount of supposedly secure information from the U.S. military and handed it over to WikiLeaks for broadcast—again from the inside. In this case, poor human resource management was the culprit.

hance profitability can also undermine security. For example, many technologies, such as mobile technology, cloud computing, and "smart" devices, can yield significant cost savings and business efficiencies, but can also create major security concerns if implemented haphazardly. Properly deployed, they could increase security, but only at a cost.

Similarly, trends such as bring your own device (BYOD), 24/7 access to data, and the use of long, international supply chains may be so cost-effective that they are required in order for a business to remain competitive. These practices, however, can also dramatically weaken the security of the organization.

It is possible for organizations to defend themselves while staying competitive and maintaining profitability. Successful cybersecurity methods, however, cannot simply be "bolted on" at the end of business processes. Cybersecurity needs to be woven into corporate processes—and when done successfully, it can help build competitive advantage. One recent study found that four basic security controls were effective in preventing 85 percent of cyber intrusions:

- Restricting user installation of applications (called "whitelisting").
- Ensuring that the operating system is patched with current updates.
- Ensuring that software applications have current updates.
- Restricting administrative privileges.[9]

The study showed that not only were these core security practices effective, but they also improved business efficiency and created an immediate positive return on investment, even before considering the positive economic impact of reducing cyber breaches.[10]

As one report noted: "Recognize that effective cyber threat risk management can give your company more confidence to take certain 'rewarded' risks (e.g., adopting proper cloud computing methods) to pursue new value."[11]

The five principles for effective oversight of cyber risk detailed in this handbook are presented in a relatively generalized form, in order to encourage discussion and reflection by corporate boards of directors. Naturally, boards will adapt these recommendations based on their company's unique characteristics, including size, life-cycle stage, business plans, industry sector, geographic footprint, culture, and so on.

Why Would They Attack Us?

Some organizations feel that because they are relatively small or don't hold substantial amounts of sensitive consumer data, such as credit card numbers or medical information, that they are unlikely to be the victims of a cyberattack. In fact, cyber criminals target companies of all sizes and from every industry, seeking anything that might be of value, including:

- Business plans, including merger or acquisition strategies, bids, etc.;
- Trading algorithms;
- Contracts with customers, suppliers, distributors, joint venture partners, etc.;
- Employee log-in credentials;
- Information about company facilities, including plant and equipment designs, maps, and future plans;
- Product designs;
- Information about key business processes;
- Source code;
- Lists of employees, customers, contractors, and suppliers; and
- Client data.

Source: Internet Security Alliance.

About the Contributors

NACD's mission is to advance exemplary board leadership—for directors, by directors. We deliver the knowledge and insights that board members need to confidently navigate complex business challenges and enhance shareowner value. We amplify the collective voice of directors in setting a substantive policy agenda.

NACD was founded in 1977 as the only national membership organization created for and by directors. Today, more than 14,000 directors and key executives from public, private, and nonprofit companies rely on us for board development, resources, education, and connections.

American International Group Inc. (AIG) is a leading international insurance organization serving customers in more than 130 countries. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIG_LatestNews | LinkedIn: http://www.linkedin.com/company/aig.

The Internet Security Alliance (ISA) is a multi-sector trade association that sees cybersecurity not as an IT issue, but as an enterprise-wide risk management issue. ISA's mission is to combine technology with economics and public policy to create a sustainable system of cybersecurity. ISA is focused on three main goals, thought leadership, public advocacy and creating standards and practices that effectively promote cybersecurity. In 2008 ISA published its cybersecurity social contract which argued that traditional government regulation would be ineffective and counter-productive against the growing cyber threat. Instead, ISA proposed that government work with industry to identify effective standards and practices and motivate voluntary adoption of these standards and practices by deploying market incentives. In 2011, the ISA "social contract" was embraced by the House GOP task force on cybersecurity and in 2013 the ISA approach was adopted in President Obama's executive order on cybersecurity.