Managing Cyber Risk:

A Handbook for UK Boards of Directors

FOREWORDS BY

Peter Gleason**

President and CEO,
National Association of Corporate Directors

AND

Larry Clinton

President and CEO, Internet Security Alliance

Based on the National Association of Corporate Directors Cyber Risk Oversight Director's Handbook

Managing Cyber Risk:

A Handbook for UK Boards of Directors

INTERNET SECURITY ALLIANCE

PREPARED BY

Larry Clinton

President and CEO, Internet Security Alliance

AND

Stacey Barrack

Senior Director of Policy, Internet Security Alliance

Why a Cyber-Risk Oversight Handbook for Corporate Boards?

Cyber-attacks are the fastest growing, and perhaps most dangerous, threat facing organisations today. Boards are increasingly focused on addressing these threats. However, due to the ever-changing nature of the threat, boards are seeking a coherent approach to deal with the issue at board level. In response, the Internet Security Alliance (ISA) and the National Association of Corporate Directors (NACD) created the first Cyber-Risk Oversight Handbook for Corporate Boards in 2014. The Handbook proved an immediate success in helping Boards address cyber risk on a global scale. Indeed, PricewaterhouseCoopers, in their 2016 Global Information Security Survey, referenced the Handbook by name and reported that:

> **"Guidelines from the National Association for Corporate Directors (NACD) advise that Boards should view cyber risks from an enterprise-wide standpoint and understand the potential legal impacts. They should discuss cybersecurity risks and preparedness with management, and consider cyber-threats in the context of the organisation's overall tolerance for risk."**
>
> **"Boards appear to be listening to this guidance. This year we saw a double-digit uptick in Board participation in most aspects of information security. Respondents said this deepening Board involvement has helped improve cybersecurity practices in numerous ways. It may be no coincidence that, as more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending."**
>
> **"Other notable outcomes cited by survey respondents include identification of key risks, fostering an organizational culture of security and better alignment of cybersecurity with overall risk management and business goals. More than anything, board participation has opened the lines of communication between executives and directors treating cybersecurity as an economic issue."**[1]

[1] PricewaterhouseCoopers (PwC), *Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016* (PwC, 2015), Web.

Table of Contents

RETURN TO TABLE OF CONTENTS

Acknowledgements

The following professionals are acknowledged for their contributions to the development of this Handbook through participation in project meetings, workshops, tele-conferences, and content creation.

The Handbook was revised from the 2017 U.S.-version based on their collective inputs, following a consensus process, and does not necessarily reflect the views of the companies and organisations listed.

Internet Security Alliance Board of Directors

*Workshop Breakout Session Chair

INTERNET SECURITY ALLIANCE **Larry Clinton**
INTERNET SECURITY ALLIANCE **Stacey Barrack**
RAYTHEON **Jeff Brown, Chairman***
USAA **Gary McAlum, First Vice Chairman**
NORTHROP GRUMMAN CORPORATION **JR Williamson, Second Vice Chairman**
AIG **Tracie Grella***
VODAFONE **Richard Spearman***
BNY MELLON **Robert Ife***
ERNST & YOUNG **Andrew Cotton***
CENTER FOR AUDIT QUALITY **Catherine Ide**
BUNGE **Bob Zandoli**
CENTENE **Lou DeSorbo**
SECURE SYSTEMS INNOVATION CORPORATION **John Frazzini**
LEIDOS **Stephen Hull**
GENERAL ELECTRIC **Nasrin Rezai**
LOCKHEED MARTIN CORPORATION **Jim Connelly**
RSA **Niloofar Howe**
STARBUCKS **Dave Estlick**
UTILIDATA **Ed Hammersla**
SYNCHRONY FINANCIAL **Larry Trittschuh**
DIRECT COMPUTER RESOURCES **Joe Buonomo**
CARNEGIE MELLON UNIVERSITY **Tim McNulty**
NATIONAL ASSOCIATION OF MANUFACTURERS **Brian Raymond**
THOMSON REUTERS **Tim McKnight**

Contributors

AIG **Camilla Kampmann**
AIG **Garin Pace***
AIG **Chloe Green**
AIG **Susanne Pauer**
AIG **Mark Camillo**
AIG **Richard Hebblethwaite**
VODAFONE **Stephen Hermanson**
VODAFONE **Robert MacDougall**
BNY MELLON **George Stephens**
DUNN & BRADSTREET **Anastassia Lauterbach**
DLA PIPER **Jan Pohle**
DLA PIPER **Jim Halpert**
DLA PIPER **Jan Spittka**
DLA PIPER **Andrew Dyson**
DLA PIPER **Alex Tamlyn**
DLA PIPER **Ben Johnson**
DLA PIPER **Christian Schoop**
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS **Peter Gleason**
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS **Erin Essenmacher**
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS **Robyn Bew**
HATHAWAY GLOBAL STRATEGIES **Melissa Hathaway**
RICHARD KNOWLTON ASSOCIATES **Richard Knowlton**
GEC RISK ADVISORY **Andrea Bonime-Blanc**
ALIXPARTNERS **Lorenzo Grillo**
AXELOS **Nick Wilding**
AXIO **Scott Kannry**
BLUEVOYANT **Dave Johnston**
BMW GROUP **Mick Albayati**
BNY MELLON **John Johnston**
BREWIN DOLPHIN **Susan Beckett**
BREWIN DOLPHIN **Paul Kilpatrick**
CREDIT SUISSE **Jason J. Mallinder**
CYBER SECURITY COUNCIL OF GERMANY **Hans-Wilhelm Dunn**
ESCAPE HUNT **Laura de Poitiers**
FIDELITY INTERNATIONAL **Pete Gillespie**
FRESHFIELDS BRUCKHAUS DERINGER LLP **Rhodri Thomas**
GCHQ **Robert Hannigan**
FIS GLOBAL **Kara Hill**

Thanks and acknowledgments are given for the support and participation of all the organisations that supplied experts to this initiative. Without the contributions of these individuals and their collective expertise, particularly those that chaired the various workshop breakout sessions and participated actively, this final deliverable would not have been possible.

Special acknowledgment and appreciation is given to AIG for being the project anchor company, and sponsoring the workshop activities through contribution of venues, logistical support, and marketing insight. Their leadership and dedication in helping shape the initiative, lead its proceedings, build consensus for the final deliverable, and help with distribution were instrumental in reaching a successful outcome.

Special thanks also go out to Freshfields Bruckhaus Deringer LLP and DLA Piper for their legal expertise.

Special thanks also go out to Vodafone for their help in translating the spelling and content to UK standards.

Foreword for ISA global adaptations for Cyber-Risk Oversight Handbook

PETER GLEASON, PRESIDENT AND CEO, NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Digital connectivity continues to transform the way we live and work. Nearly 4 billion people around the world connected to the internet in 2017.[2] Cross-border data transfers grew by 45 times between 2005 and 2016, and are on pace to increase at an even greater rate in the future.[3] In the business sphere, data flows now have a bigger impact on GDP growth around the world than traditional trade in goods[4], and new technologies are creating unprecedented opportunities for companies both large and small.

Yet as advances in technology continue to proliferate and spread, so do global leaders' concerns about cyber-threats and their associated costs. In study after study, senior executives, government leaders, and law enforcement officials express uncertainty about whether their organizations are equipped to manage and respond to cyber-risks, and are asking questions about how the digital revolution will affect data security and privacy. In the National Association of Corporate Directors' (NACD's) most recent survey of public-company board members, 58% of respondents believe it is somewhat or very difficult for their board to effectively oversee cyber-risks[5].

Cybersecurity has become a permanent fixture on the agendas of companies around the world, and board members need to be prepared to provide appropriate and effective oversight of cyber-risks. Placing cybersecurity in a business context, as an enterprise-wide strategy issue, is essential.

NACD is the U.S.'s oldest and largest non-profit education association serving the non-executive director (NED) community. We were proud to work with the Internet Security Alliance (ISA) on the development of the original NACD Director's Handbook on Cyber-Risk Oversight in 2014, and the updated edition in 2017. The publication broke new ground by identifying a set of five core principles for cyber-risk oversight by NEDs that have stood the test of time, even as the cyber-threat environment has continued to evolve.

NACD congratulates the ISA, AIG, eCoda and the German Federal Office for Information Security on taking forward the principles outlined in the Handbook, and putting them into a practical context for board members of UK companies.

Peter Gleason
President and CEO, NACD

[2] Steve Morgan, "Top 5 cybersecurity facts, figures and statistics for 2018," CSO, Jan. 23, 2018.
[3] James Manyika et. al., *Digital globalization: the new era of global flows*, McKinsey Global Institute, 2016.
[4] Ibid.
[5] *NACD 2017-2018 Public Company Governance Survey*, p. 23.

RETURN TO TABLE OF CONTENTS

Cybersecurity: we are all in this together

LARRY CLINTON, PRESIDENT AND CEO, INTERNET SECURITY ALLIANCE

Over the past few years, the public, including members of Boards of Directors, have become increasingly aware of the cyber risk.

However, at the same time, Board members have been bombarded with all manners of advisors, consultants and so-called specialists providing confusing, inconsistent and even conflicting suggestions for how to manage cyber risk.

The Cyber-Risk Handbooks are an attempt to provide Board members with a simple and coherent framework to understand cyber risk, as well as a series of straight-forward questions for Boards to ask management to assure that their organization is properly addressing its unique cyber-risk posture.

Independent research on previous editions of the Cyber-Risk Oversight Handbook – focused on the same core principles – has shown that use of these principles results in better cybersecurity budgeting, better cyber-risk management, increased alignment of cybersecurity with business goals, and helps create a culture of security.[6]

This Handbook has been put together by nearly a hundred cybersecurity experts from multiple governments and industry sectors, working together on a voluntary basis. No one is being paid to contribute to this effort and there is no charge for the Handbook.

The contributors to this Handbook are not providing their contributions for financial gain. They are working together because cyber criminals are targeting all of us. Government, industry, and private citizens are all on the same side in this fight. We must all work together.

It's our expectation that there will be subsequent editions, so we welcome your feedback as we all work together to protect our data in a sustainably secure cyber system.

Larry Clinton
President and CEO, ISA

[6] PricewaterhouseCoopers (PwC), Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016 (PwC, 2015), Web.

Introduction

In the past 25 years, the nature of corporate assets has changed significantly, moving from physical to virtual. Close to 90 percent of the total value of the Fortune 500 now consists of intellectual property (IP) and other intangible assets.[7] Along with the rapidly expanding "digitisation" of corporate assets, there has been a corresponding digitisation of corporate risk. Accordingly, policy makers, regulators, shareholders, and the public are more aware of corporate cybersecurity risks than ever before. Organisations are at risk from the loss of IP and trading plans, destroyed or altered data, declining public confidence, disruption to critical infrastructure, and evolving regulatory sanctions. Each of these risks can adversely affect competitive positions, 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 domain for two reasons. First, the complexity of cyber-threats has grown dramatically. Corporations now face increasingly sophisticated events that outstrip traditional defences. As the complexity of these attacks increases, so does the risk they pose to corporations. The potential effects of a data breach are expanding well beyond information loss or disruption. Cyber-attacks can have a severe impact on an organisation's reputation and brand, which may be affected more by tangential factors like timing or publicity than the actual loss of data. Companies and directors may also incur legal risk resulting from cyber-attacks. At the same time, the motivation to deploy new and emerging technologies in order to lower costs, improve customer service, and drive innovation is stronger than ever. These competing pressures on corporate staff and business leaders mean that conscientious and comprehensive oversight at the Board level is essential. As a result, managing and mitigating the impact of cyber risk requires strategic thinking that goes beyond the IT department.

NACD, in conjunction with AIG and the Internet Security Alliance, has identified five steps boards should consider as they seek to enhance their oversight of cyber risks. This handbook is organised 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 risk 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 board meeting agendas.
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 discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

While some language in the handbook refers to unlisted companies, these principles are applicable to, and important for, all directors, including members of private-company and non-profit Boards. Every organisation has valuable data and related assets that are under constant threat from cyber-criminals or other adversaries.

A rapidly evolving cyber-threat landscape

As recently as a few years ago, cyber-attacks 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 APTs (for advanced persistent threats), were first deployed against government entities and defence contractors. More recently, they have migrated throughout the economy, meaning that virtually any organisation is at risk.

One of the defining characteristics of these attacks is that they can penetrate virtually all of a company's perimeter defence systems, such as firewalls or intrusion-detection systems. Intruders look at multiple avenues to exploit vulnerabilities all layers of security until they achieve their goals. The reality is that if a sophisticated attacker targets a company's systems, they will almost certainly breach them.

In addition, contract workers 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

[7] Ocean Tomo, "*Annual Study of Intangible Asset Market Value from Ocean Tomo, LLC*" (press release), Mar. 5, 2015.

external and internal cyber-threats. Organizations cannot deal with advanced threats if they are unable to stop low-end attacks.[8]

Greater connectivity, greater risk

Due to the immense number of interconnects among data systems, it is no longer adequate that organisations secure only "their" network. Vendors, suppliers, partners, customers, or any entity connected with the company electronically can become a potential point of vulnerability. For example, 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.[9]

The growing interconnected nature of traditional information systems and non-traditional systems such as security cameras, copiers, video-gaming platforms and cars (the so-called Internet of Things, or IoT) has resulted in an exponential increase in the number of potential points of entry for cyber-attackers; and thus, the need for organisations to expand their thinking about cyber-risk. A "distributed denial of service" attack in 2016 that severely restricted access to over 1,000 corporate websites, including those of Twitter, PayPal, and Netflix, was coordinated by hackers using hundreds of thousands of end-user devices, including home digital video recorders and webcams.[10]

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 cyber-attack. While such attacks are technically possible and could have very serious consequences, the vast majority of incidents are economically motivated.[11] Cyber-attackers routinely attempt to steal all manner of data, including personal information from customers and employees, financial data, business plans, trade secrets, and intellectual property. Increasingly, cyber-attackers are employing tactics that encrypt an organisation's data, effectively holding it hostage until they receive a payment – so-called "ransomware." Estimating the damage of cyber-attacks is difficult, but some estimates put it at $400-500 billion or more annually,

Cyber Threats by the Numbers

- 48 percent of cyber-breaches result from criminal or malicious attacks.[i] 80 percent of black hat hackers are affiliated with organised crime.[ii]
- Top methods of access by cybercriminals include using stolen access credentials and malware.[iii] Attacks on mobile devices and cyber-extortion attacks are both on the rise.[iv]
- The median number of days an organisation is compromised before discovering a cyber-breach is 146.[v] 53 percent of cyber-attacks are first identified by law enforcement or third parties, compared with 47 percent that are discovered internally.[vi]
- 48 percent of IT security professionals do not inspect the cloud for malware, despite the fact that 49 percent of all business applications are now stored in the cloud. Of those cloud-based applications, less than half are known, sanctioned, or approved by IT.[vii]
- 38 percent of IT organisations do not have a defined process for reviewing their cyber-breach response plans, and nearly a third have not reviewed or updated their plans since they were initially developed.[viii]

[i] Ponemon Institute and IBM, *2016 Cost of Data Breach Study: Global Analysis*, p. 2.

[ii] Limor Kessem, "2016 Cybercrime Reloaded: Our Predictions for the Year Ahead," Jan. 15, 2016.

[iii] Verizon, *2016 Data Breach Investigations Report*, p. 8-9.

[iv] Kessem, "2016 Cybercrime Reloaded."

[v] FireEye Inc, *Mandiant M-Trends 2016*, p. 4.

[vi] *Mandiant M-Trends*, p. 7, 2016 *Data Breach Investigation Report*, p. 11.

[vii] Jeff Goldman, "*48 Percent of Companies Don't Inspect the Cloud for Malware*," eSecurity Planet (blog), Oct. 12, 2016.

[viii] Thor Olavsrud, "Companies complacent about data breach preparedness," CIO, Oct. 28, 2016.

[8] Verizon RISK Team, et al., *2013 Data Breach Investigations Report*, March 2013.

[9] Nicole Perlroth, "Hackers Lurking in Vents and Soda Machines," the *New York Times*, Apr. 7, 2014.

[10] Samuel Burke, "Massive cyberattack turned ordinary devices into weapons," CNNMoney.com, Oct. 22, 2016.

[11] Verizon, *2016 Data Breach Investigations Report*, p. 7.

with a significant portion of costs going undetected.[12] Cybercrime costs quintupled between 2013 and 2015, and could top $2 trillion per year by 2019.[13]

Moreover, although many smaller and medium-sized companies have historically believed that they were too insignificant to be targets, that perception is wrong. In fact, the majority of small and medium-sized businesses have been victims of cyber-attacks; a figure that is closer to 75 percent in the United Kingdom.[14,15] Alarmingly, 60 percent of small companies that suffer a cyber-attack are out of business within six months.[16] In addition to being targets in their own right, smaller firms are often an attack pathway into larger organisations 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 cyber-attackers are well ahead of the corporations that must defend against them. Cyber-attacks are relatively inexpensive yet highly profitable, and the resources and skills necessary to launch an attack are quite easy to acquire. It is no surprise that many observers believe cyber-risk defence tends to lag a generation behind the attackers. It is difficult to demonstrate return on investment (ROI) for cyber-attack prevention, and successful law enforcement response to such attacks is virtually non-existent. According to some estimates, less than 1 percent of cyber-attackers are successfully prosecuted.[17]

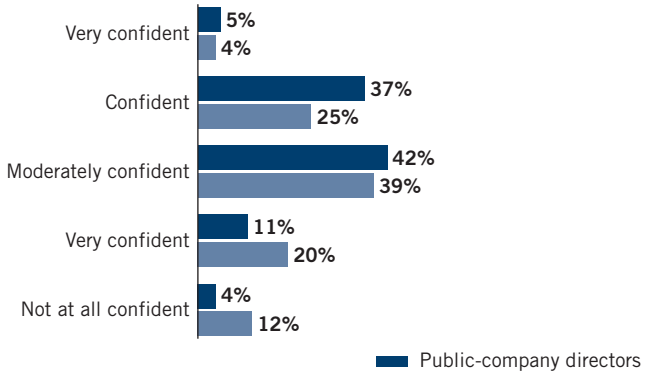
This does not mean that defence is impossible, but it does mean that Board members need to ensure that management is fully engaged in making the organisation's systems as resilient as economically feasible. This includes developing defence and response plans that are capable of addressing sophisticated attack methods.

Balancing cybersecurity with profitability

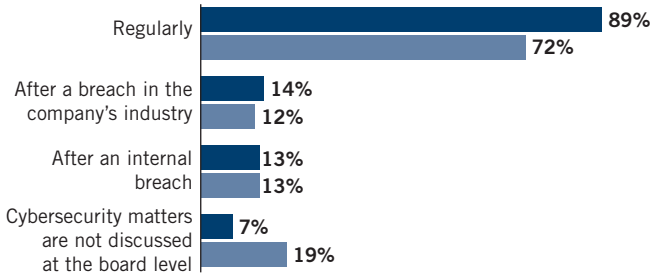
Like other critical risks organisations face, cybersecurity cannot be considered in isolation. Members of management and the Board must strike the appropriate balance between protecting the security of an organisation and mitigating losses, while continuing to ensure profitability and growth in a competitive environment.

FIGURE 1

How confident are you that your company is properly secured against a cyber-attack?



How often is cybersecurity discussed at Board meetings?



Source: This data is compiled from the NACD 2016-2017 public- and private-company governance surveys.

[12] Steve Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019," *Forbes*, Jan. 17, 2016.

[13] Ibid.

[14] Patricia Harmn, "50% of small businesses have been the target of a cyber attack," PropertyCasualty360.com, Oct. 7, 2015.

[15] Mark Smith, "Huge rise in hack attacks as cyber-criminals target small business," *The Guardian*, Feb. 8, 2016.

[16] Gary Miller, "60% of small companies that suffer a cyber attack are out of business within six months," the *Denver Post*, Oct. 24, 2016.

[17] Robert M. Regoli, et al., *Exploring Criminal Justice: The Essentials* (Burlington, MA: Jones & Bartlett Learning, 2011), p. 378.

Why Would They Attack Us?

Some organizations believe they are unlikely to be the victims of a cybe-rattack because they are relatively small in size, are not a well-known brand name, and/or don't hold substantial amounts of sensitive consumer data, such as credit card numbers or medical information.

In fact, adversaries target organizations of all sizes and from every industry, seeking anything that might be of value, including the following assets:

- Business plans, including mergers or acquisition strategies, bids, etc.
- Trading algorithms
- Contracts or proposed agreements with customers, suppliers, distributors, joint venture partners, etc.
- Employee log-in credentials
- Facility informations, including plant and equipment designs, building maps, and future plans
- R&D information, including new products or services in development
- Information about key business processes
- Source code
- Lists of employees, customers, contractors, and suppliers
- Client, donor, or trustee data

Source: Internet Security Alliance

Many technical innovations and business practices that enhance 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 they can also create major security concerns if implemented incorrectly. Properly deployed, they could increase security.

Similarly, trends such as BYOD (bring your own device), 24/7 access to information, the growth of sophisticated "big data" analytics, and the use of long international supply chains may be so cost-effective that they are essential elements in order for a business to remain competitive. However, these practices can also dramatically weaken the security of the organisation.

It is possible for organisations to defend themselves while staying competitive and maintaining profitability. However, successful cybersecurity methods cannot simply be "bolted on" at the end of business processes. Cybersecurity needs to be woven into an organisation's key systems and processes from end to end; and when done successfully, it can help build competitive advantage. One study found that four basic security controls were effective in preventing 85 percent of cyber intrusions:

- Restricting user installation of applications ("whitelisting").
- Ensuring that the operating system is "patched" with current updates.
- Ensuring that software applications are regularly updated.
- Restricting administrative privileges (i.e., the ability to install software or change a computer's configuration settings).[18]

The study showed that not only were these core security practices effective, they also improved business efficiency and created an immediate positive return on investment, even before considering the positive economic impact of reducing cyber-breaches.[19]

To be effective however, cyber strategy must be more than reactive. Leading organisations also employ a proactive, forward-looking posture that includes generating intelligence about the cyber-risk environment and anticipating where potential attackers might strike. This includes subjecting their own systems and processes to regular and rigorous testing to detect vulnerabilities.

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

[18] AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, October 2013. See also: Internet Security Alliance, *Sophisticated Management of Cyber Risk* (Arlington, VA: Internet Security Alliance, 2013).

[19] AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, October 2013.

PRINCIPLE 1

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

Historically, corporations have categorised information security as a technical or operational issue to be handled by the information technology (IT) department. This misunderstanding is exacerbated by corporate structures that leave functions and business units within the organisation feeling disconnected from responsibility for the security of their own data. Instead, this critical responsibility is left to IT, a department that in most organisations is working with restricted resources and budget authority. Furthermore, deferring responsibility to IT inhibits critical analysis and communication about security issues, and hampers the implementation of effective security strategies.

In an increasingly inter-connected ecosystem, every business is a technology business where IT creates and adds value. Most companies invest heavily in IT innovation and making technology infrastructures increasingly central to overall business strategy and operations. Depending on their sector and the services they provide, some companies rely more inherently on IT than others. Cyber risks should be evaluated in the same way an organisation assesses the physical security of its human and physical assets and the risks associated with their potential compromise. In other words, cybersecurity is an enterprise-wide risk management issue that needs to be addressed from a strategic, cross-departmental, and economic perspective.[20] It is not just an IT (or technology) issue, but also about business processes, people, and value.

Cyber risk and the business ecosystem

Some of the highest-profile data breaches to date have had little to do with traditional hacking. For example, spear phishing (a common e-mail attack that targets specific individuals) is a leading cause of system compromise. Product or production strategies that use complex supply chains that span multiple countries and regions can magnify cyber risk. Similarly, mergers and acquisitions requiring the integration of complicated systems, often on accelerated timelines and without sufficient due diligence, can increase cyber risk.

Another obstacle companies face in creating a secure system is how to manage the degree of connectivity that the corporate network has with partners, suppliers, affiliates, and customers. Several significant and well-known cyber-breaches did not actually start within the target's IT systems, but instead resulted from vulnerabilities in one of their vendors or suppliers, as the examples in the section, "Greater connectivity, greater risk," on page 7 reflect. Furthermore, an increasing number of organisations have data residing on external networks or in public "clouds," which they neither own nor operate and have little inherent ability to secure. Many organisations are also connected with elements of the national critical infrastructure, raising the prospect of cybersecurity at one company or institution becoming a matter of public security, or even affecting national security.

As a result, directors should ensure that management is assessing cybersecurity not only as it relates to the organisation's own networks, but also regarding the larger ecosystem in which it operates. Progressive Boards will engage management in a discussion of the varying levels of risk that exist in the company's ecosystem and account for them as they calculate the appropriate cyber-risk

Identifying the Company "Crown Jewels" and Highly Sensitive Categories of Data

Directors should engage management in a discussion of the following questions on a regular basis:

- What are our company's most critical data assets? (i.e. its "Crown Jewels")
- What highly sensitive data does the company hold? (e.g. sensitive personal data)
- What is the backbone of the business and what are the IT infrastructures in use to run the business?
- Where do they reside? Are they located on one or multiple systems?
- How are they accessed? Who has permission to access them?
- How often have we tested our systems to ensure that they are adequately protecting our data?
- Are we building security into the business models and embedding it within the business strategies?

[20] Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs*, 2010.

posture and tolerance for their own corporation.[21] They should also understand what "crown jewels" and highly sensitive data the company needs to protect most, and ensure that management has a protection strategy that builds from those high-value targets outward. The Board should instruct management to consider not only the highest-probability attacks, but also low-probability, high impact attacks that would be catastrophic.[22]

See **Appendix B** for a list of cybersecurity questions that directors can ask management on issues such as situational awareness, strategy and operations, insider threats, supply-chain/third-party risks, incident response, and post-breach response. **Appendix C** outlines cybersecurity considerations related to mergers and acquisitions.

Cyber-risk oversight responsibility at the Board level

How to organise the Board to manage the oversight of cyber risk, and enterprise-level risk more broadly, is a matter of considerable debate. Cyber risk can be mitigated and minimized significantly if approached as an enterprise-wide risk management issue. However, as with traditional risks, cyber risks cannot be eliminated entirely and Boards need to understand the nature of their company's threat environment. The NACD Blue Ribbon Commission on Risk Governance recommended that risk oversight should be a function of the full Board.[23] NACD research finds this to be true at most public-company Boards with so-called "big picture risks" (i.e., risks with broad implications for strategic direction, or discussions of the interplay among various risks). Yet just over half of Boards assign the majority of cybersecurity-related risk-oversight responsibilities to the audit committee (Figure 2), which also assumes significant responsibility for oversight of financial reporting and compliance risks.

There is no single approach that will fit every Board: some choose to conduct all cyber-risk-related discussions at the full-board level; others assign specific cybersecurity-related oversight responsibilities to one or more committees (audit, risk, technology, etc.); and still others use a combination of these methods. The nominating and governance committee should ensure the Board's chosen approach is clearly defined in committee charters to avoid confusion or duplication of effort. The full Board should be briefed on cybersecurity matters at least semi-annually and as specific incidents or situations warrant. Committees with designated responsibility for risk oversight (and for oversight of cyber-related risks in particular) should receive briefings on at least a quarterly basis.

In order to encourage knowledge-sharing and dialogue, some Boards invite all directors to attend committee-level discussions

FIGURE 2

To which group has the Board allocated the majority of tasks connected with the following areas of risk oversight? (Partial list of response choices' multiple selections permitted)

Source: *2016–2017 NACD Public Company Governance Survey*

[21] NACD, et al., *Cybersecurity: Boardroom Implication* (Washington, DC: NACD, 2014) (an NACD white paper).

[22] Ibid. See also: KPMG Audit Committee Institute, *Global Boardroom Insights: The Cyber Security Challenge*, Mar. 26, 2014.

[23] NACD, *Report of the Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward* (Washington, DC: NACD, 2009).

on cyber-risk issues, or make use of cross-committee membership. For example, one global company's board-level technology committee includes directors who are experts on privacy and security from a customer perspective. The audit and technology committee chairs are members of each other's committees, and the two committees meet together once a year for a discussion that includes a "deep dive" on cybersecurity.[24]

While including cybersecurity as a stand-alone item on Board and/or committee meeting agendas is now a widespread practice, the issue should also be integrated into full-board discussions involving new business plans and product offerings, mergers and acquisitions, new-market entry, deployment of new technologies, major capital investment decisions such as facility expansions or IT system upgrades, and the like.

See **Appendix A** for suggested questions to help directors assess their Board's level of understanding of cybersecurity issues or cyber literacy. **Appendix F** contains sample Board evaluation questions related to cybersecurity oversight.

[24] Adapted from Robyn Bew, "*Cyber-Risk Oversight: 3 Questions for Directors*," Ethical Boardroom, Spring 2015.

PRINCIPLE 2

Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

The legal and regulatory landscape with respect to cybersecurity, including required disclosures, privacy and data protection, information-sharing, infrastructure protection, and more, is complex and constantly evolving. Boards should stay aware of current liability issues faced by their organisations – and, potentially, by directors on an individual basis. For example, high-profile attacks may spawn lawsuits, including shareholder and customer class-actions, and could lead to regulatory enforcement actions. Claimants may also allege that the organisation's Board of directors neglected its fiduciary duty by failing to take sufficient steps to confirm the adequacy of the company's protections against data breaches and their consequences. Exposures can vary considerably, depending on the organisation's sector and operating locations. Regardless of the legal merits or ultimate outcome of any challenge, reputational damage to a business from a cyber-breach can be severe and long-lasting.

Boards should consider how they: maintain records of discussions about cybersecurity and cyber risks; stay informed about industry-, region-, and sector-specific requirements that apply to the organisation; analyze evolving risks in relation to business resilience and response plans; and, determine what to disclose in the wake of a cyber-attack. The culture of a company tends to flow from the top down and so boards should take a vigorous approach to cybersecurity to show employees that cyber risk must always be an important consideration. Effective governance structures should then be implemented to underpin that culture and ensure the company is properly focused on managing these risks. It is also advisable for directors to participate in cyber-breach simulations to gain exposure to the company's response procedures in the case of a serious incident to mitigate against its potential impact, and to practice for a potential scenario that requires the board to make an important decision.

To facilitate this, Boards should consider having access to IT-expertise at the Board level, rather than simply relying on other parts of the business, and a transparent allocation of responsibility for oversight of cybersecurity. Among the topics Boards should be mindful of are:

Board minutes

Board minutes should reflect the occasions when cybersecurity was present on the agenda at meetings of the full board and/or of key board committees, depending on the allocation of oversight responsibilities. Discussions at these meetings might include updates about specific risks and mitigation strategies, as well as reports about the company's overall cybersecurity program and the integration of technology with the organisation's strategy, policies, and business activities.

Legal landscape

Legal challenges to organisations include overlapping and conflicting rules and requirements, lack of coordination among rulemaking and legislative authorities, and different priorities driving the development of new regulations. While directors do not need to have deep knowledge about this increasingly complex area of law, they should be briefed by internal or external counsel on a regular basis about requirements that apply to the company. Reports from management should enable the board to assess whether or not the organisation is adequately addressing these potential legal risks.

A company's disclosure and reporting requirements depend on the type of business it runs and the sector in which it operates. However, all board members should keep in mind their overriding duty as directors to exercise reasonable care, skill and diligence.[25] The UK Government has also advised Boards to set up risk management regimes in accordance with its '10 Steps to Cybersecurity' to ensure businesses are adequately protected.[26]

There are three key trends emerging from both UK and EU cyber laws:

1. A broad legal requirement to maintain "appropriate" security standards, informed by the nature of the data requiring protection;
2. Greater transparency requirements, including obligations to notify data breaches to regulators (and in some cases affected individuals) within very short timescales; and
3. Much tougher sanctions for non-compliance and greater risk of private claims.

[25] Section 174 Companies Act 2006

[26] https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/NCSC%2010%20Steps%20To%20Cyber%20Security%20NCSC.pdf

Data controllers and data processors[27]

The General Data Protection Regulation (GDPR) sets out various obligations for organisations who control personal data and those who process it. In particular, it requires the implementation of *"appropriate technical and organizational measures to ensure a level of security appropriate to the risk"*. The Regulation also introduces an enhanced notification obligation to disclose any breaches to the relevant supervisory authority without undue delay (and where feasible within 72 hours). If not followed, a company can be fined up to 4% of its annual worldwide turnover. In addition, supervisory authorities enjoy wide investigative and corrective powers and the GDPR makes it considerably easier for individuals to bring private claims.

Essential service providers[28]

The Network and Information Systems Directive was created specifically to improve the cybersecurity of essential services providers (e.g. in the energy, health and transport sectors) and digital service providers. The principal aim of the Directive is to *"lay down measures with a view of establishing a high common level of security of network and information systems"*.[29] Directive operates to encourage cooperation among networks so that cyber-intelligence is shared quickly and introduces a cyber-breach notification program.

Payment service providers

The Payment Services Regulations impose enhanced cybersecurity requirements for payment service providers (including banks and e-money companies). Providers are required to carry out annual assessments of relevant operational and security risks, which should include cyber risk, and have new reporting obligations for significant incidents.

Publicly traded companies

Neither the Financial Conduct Authority (FCR) nor the London Stock Exchange impose specific cybersecurity rules but boards of publicly traded companies should be aware of their general disclosure obligations in the event of a cybersecurity breach. Boards should consider whether the breach itself constitutes inside information and whether it is disclosable to the market. Key considerations will be whether the information is: precise, not generally available, and likely to have a significant effect on the company's share price if made public.[30] Ultimately, this decision rests with the board after taking appropriate advice. The market-linked aspect of the test means that such advice should generally include both broking and legal components.

Financial institutions

The FCA requires firms to maintain systems and controls to minimise the risk of operational and information assets being exploited by criminals and a number of FCA principles and rules are applicable to cyber resilience. Material cyber incidents must be reported to the FCA and subsequent cooperation is needed with the FCA[31] and the Prudential Regulation Authority (PRA).[32] Some firms are required to appoint a senior manager with responsibility for internal operations and technology.[33] This places personal accountability for cybersecurity on the senior manager.

The PRA also requires firms to establish, implement and maintain adequate systems and procedures, including risk strategies, to safeguard the security, integrity and confidentiality of information. Boards also should be aware of the Bank of England's CBEST framework which tests the cyber resilience of companies considered core to the UK financial system.

---

[27] Regulation (EU) 2016/679 *[NB: This paragraph has been written as if the GDPR is effective. The effective date is May 2018.]*

[28] Directive (EU) 2016/1148 *[NB: This paragraph has been written as if the NIS has been fully transposed into UK law. The deadline for the UK to do so is May 2018.]*

[29] Article 1(1) Directive (EU) 2016/1148 [NB: *This paragraph has been written as if the NIS has been fully transposed into UK law. The deadline for the UK to do so is May 2018.]*

[30] Article 7, 17 of Regulation (EU) No 596/2014 (the Market Abuse Regulation); and Disclosure and Transparency Rule 2.2

[31] Principle 11

[32] Fundamental Rule 7

[33] Senior Management Function 24

Role of legal counsel

In-house legal and compliance teams, together with external counsel play a critical role in the fight against cyber-attacks. Directors should ask management to solicit legal counsel's views on:

- implementing a framework to mitigate against legal and regulatory risks;
- the organisation's cyber incident response plan, including in particular interaction with regulators and document management;
- potential disclosure considerations related to forward-looking risk factors in general.

As disclosure standards, regulatory guidance, formal requirements, and company circumstances all continue to evolve, management and directors should expect to be updated on a regular basis by legal counsel.

Corporate governance

The UK Corporate Governance Code is optional for private businesses but is the reference point for quoted companies. It requires public accounts disclosure of Board risk identification and mitigation and also requires Boards to contain a blend of skills appropriate to the relevant business. Institutional investors take compliance with the Code very seriously and poor adopters may experience negative voting practice and/or partial/total disinvestment by asset managers in businesses which are perceived to be "cyber vulnerable". Good systemic governance is critical to effective mitigation of cyber risk and Boards will need to take particular care to ensure that governance structures enable effective monitoring of threats and the implementation and monitoring of compliance, with controls in place across the entire organisation. It is essential to ensure that there is a distinction between executive and oversight roles.

Litigation

Litigation may be defensive in nature, for example, if action is taken against the company by customers or employees affected by a data breach, or by shareholders alleging that the board failed to take appropriate steps to protect assets, or that it mismanaged the response to a breach.

Organisations may also be required to bring litigation, for example in the form of injunctions freezing money or information stolen by cyber criminals or in claims against responsible third-party suppliers. In each case, the board will be required to make strategic decisions based on a variety of factors such as costs, publicity, prospects of success and duties owed to shareholders.

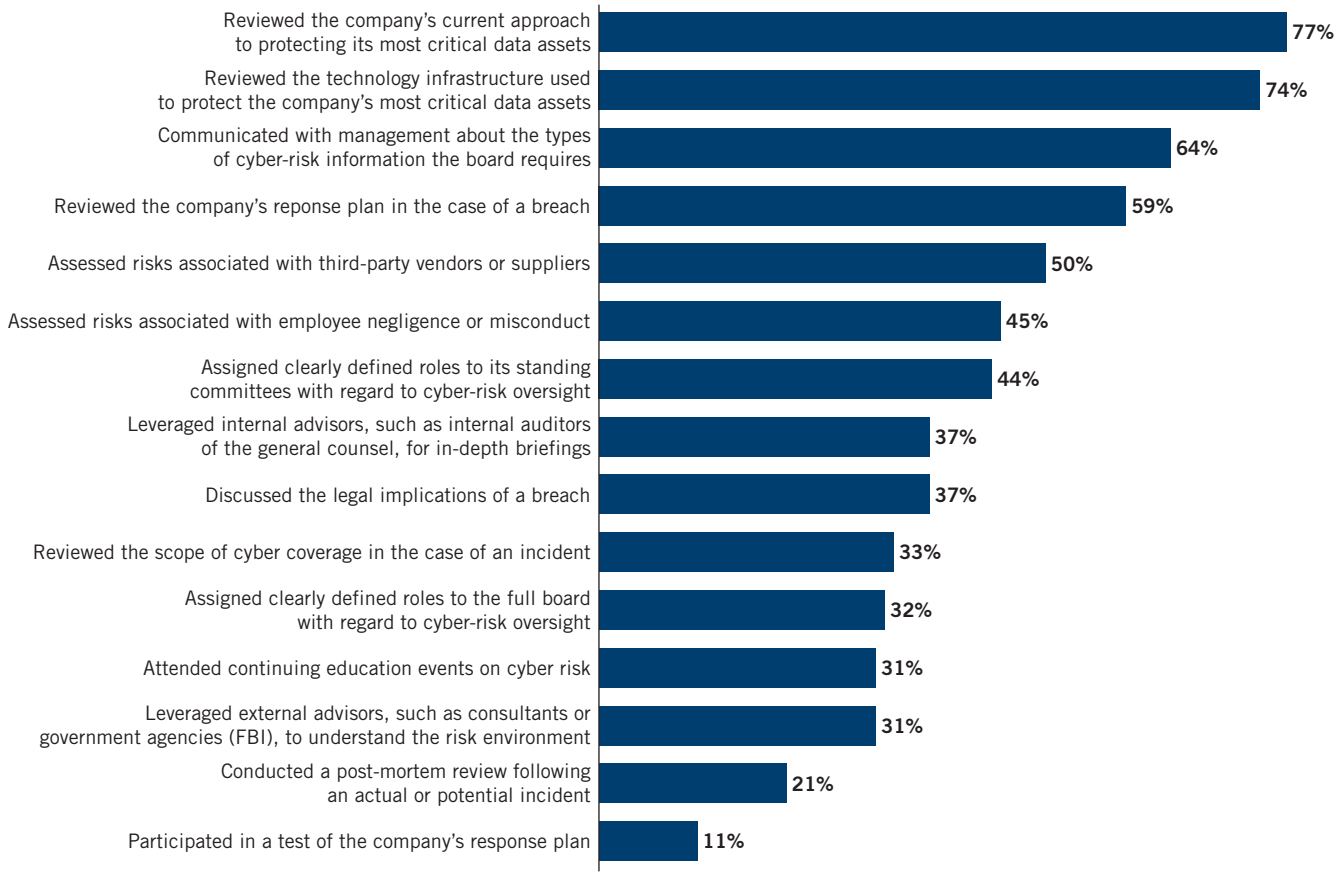
PRINCIPLE 3

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.

In a recent survey of unlisted company directors, 89.1 percent of respondents reported that their Boards discuss cybersecurity "on a regular basis."[34] See Figure 3 for additional details. Despite this level of activity, however, only about 14 percent of directors believe their Board has a "high" level of knowledge of cybersecurity risks.[35] As a director observed, "[Cybersecurity] is very much a moving target. The threats and vulnerabilities are changing almost daily, and the standards for how to manage and oversee cyber risk are only beginning to take shape."[36] At a different peer-exchange session, another director suggested this useful analogy: "Cyber literacy can be considered similar to financial literacy. Not everyone on the board is an auditor, but everyone should be able to read a financial statement and understand the financial language of business."[37]

FIGURE 3

Which of the following cyber-risk oversight practices has the Board performed over the last 12 months?



Source: 2016-2017 NACD Public Company Governance Survey

[34] NACD, *2016-2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p. 28.

[35] NACD, *2016-2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p. 26.

[36] NACD Audit Committee Chair and Risk Oversight Advisory Councils, *Emerging Trends in Cyber-Risk Oversight*, July 17, 2015, p. 1.

[37] NACD, et al., *Cybersecurity: Boardrooms Implications* (Washington, DC: NACD, 2014) (an NACD white paper), p. 3.

RETURN TO TABLE OF CONTENTS

Improving access to cybersecurity expertise

As the cyber-threat has grown, the responsibility (and expectations) of Board members has grown. Directors need to do more than simply understand that threats exist and receive reports from management. They need to employ the same principles of inquiry and constructive challenge that are standard features of board-management discussions about strategy and company performance.

As a result, some companies are considering whether to add cybersecurity and/or IT security expertise directly to the Board via the recruitment of new directors. While this may be appropriate for some companies or organisations, there is no one-size-fits-all approach that will apply everywhere (see "A Cyber-expert on Every Board?"). At an NACD roundtable discussion between directors and leading investors, participants expressed concerns about calls to add so-called "single-purpose" directors, whether narrowly specialized in cybersecurity or other areas, to all boards. As one participant put it, "It can signal risk aversion, a concern that the Board will be sued, so we need one of X, Y, and Z – all the [management] skills du jour. But Board directors aren't running the company."[38]

Nominating and governance committees must balance many factors in filling Board vacancies, including the need for industry expertise, financial knowledge, global experience, or other desired skill sets, depending on the company's strategic needs and circumstances. Whether or not they choose to add a Board member with specific expertise in the cyber arena, directors can take advantage of other ways to bring knowledgeable perspectives on cybersecurity matters into the boardroom, including the following strategies:

- Scheduling deep-dive briefings or examinations from independent and objective third-party experts validating whether the cybersecurity program is meeting its objectives.
- Leveraging the Board's existing independent advisors, such as external auditors and outside counsel, who will have a multi-client and industry-wide perspective on cyber-risk trends.
- Participating in relevant director-education programs, whether provided in-house or externally. Many Boards are incorporating a "report-back" item on their agendas to allow directors to share their takeaways from outside programs with fellow Board members.
- Having a more diverse independent director on the Board (not necessarily an expert in cyber but with knowledge of cyber and related disciplines) with not only a diversity of background (age, gender, ethnicity, nationality) but also a diversity of experience beyond the typical financial and operational expertise of most Board members (including, e.g., technology, governance, risk, compliance, ethics).[39]

Gaining access to adequate cybersecurity expertise

Most directors are specialists in particular fields or areas of expertise. While they may have certain subject matter expertise derived from their previous careers, directors should bring a broader view of enterprise-wide risk management and response. So, how do they gain access to adequate cybersecurity expertise? What is considered adequate cybersecurity expertise? It starts with the basic understanding outlined in Principle One of this Handbook – Boards need to understand that cybersecurity is not an IT issue, it is an enterprise-wide risk management issue and, therefore, Boards need to avoid pushing it to IT departments and IT Security Officers to "figure out."

An organisation does not necessarily need to add a cyber-expert to its Board. That is a decision best left to each unique business to decide what is best. But, Boards should designate Board member(s) whose responsibility is the oversight (not execution) of cybersecurity and the risk management issues that accompany it. With traditional risks (hurricanes, fires, floods, etc.) and economic risks (competition, product liability, asset impairment, etc.) we can deduce the probability of an incident occurring. We have historical data to show trends and magnitude that is used to predict potential future risk), as well as historical market behaviour to help gauge

[38] Discussion at a joint meeting of the NACD Advisory Councils for Audit Committee Chairs and Nominating and Governance Committee Chairs, Oct. 5, 2016.

[39] Andrea Bonime-Blanc, "A Strategic Cyber-Roadmap for the Board: From Sit-Back to Lean-In Governance". The Conference Board, 2016.

the impact of those risks and how they can be mitigated. With cybersecurity, however, we must operate as if everyone will be hacked at some point.

Moreover, cyber risks have some important differences from traditional risks. For example, organisations cannot fully protect themselves in an interconnected and rapidly evolving world. Cyber adversaries, including nation states, may have more resources than even the biggest corporations, and the practical difficulties associated with catching and tracing cyber-criminals are often greater than those associated with more conventional criminals, something the cyber oversight Board member(s) should understand.

There are several ways Boards can consider increasing their access to security expertise. Boards can create a check-and-balance system by seeking advice from multiple sources. For example, an organisation could have different reporting structures from three independent (not necessarily external) sources, which could include the perspective of the person accountable for cyber risk, the perspective of the person assessing cyber risk, and the perspective of the operational manager. This enables an organisation to challenge the functions and approaches, and see cyber risk from varied perspectives.

The Board's risk register[40] should have distinct cyber technology and cyber-risk sections. That would help cyber-risk discussions become a normal aspect of reporting business risk.

Enhancing management's reports to the Board

A 2012 survey found that fewer than 40 percent of Boards regularly received reports on privacy and security risks, and 26 percent rarely or never received such information.[41] Since then, boardroom practices have changed dramatically: As noted on page 17, nearly 90 percent of public-company directors say their Boards discuss

A Cyber-expert on Every Board?

In 2008, NACD, the Council of Institutional Investors, and the Business Roundtable co-developed a set of Key Agreed Principles for corporate governance "intended to assist Boards and shareholders in avoiding routine 'box ticking' in favour of a more thoughtful and studied approach." They included the idea that (presuming compliance with all applicable legal, regulatory, and exchange listing requirements) individual Boards hold responsibility for designing the structures and practices that will allow them to fulfil their fiduciary obligations effectively and efficiently, and that they are obligated to communicate those structures and practices to stakeholders in a transparent manner. Proposals aimed, for example, at requiring all Boards to have a director who is a "cybersecurity expert" – even setting aside the fact that the severe shortage of senior-level cybersecurity talent, with hundreds of thousands of positions vacant in the U.S. alone, makes such proposals impossible to implement – would take the important responsibility for Board composition and director recruitment out of the hands of the only group with first-hand knowledge about a specific Board's current and future skill requirements. The *Key Agreed Principles* publication goes on to say that "valuing disclosure over the [rigid] adoption of any set of [so-called] best practices encourages boards to experiment and develop approaches that address their own particular needs."

Sources: Internet Security Alliance, *The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity* (Washington, DC: ISA, 2016), pp. 335-338; NACD, *Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly-Traded Companies* (Washington, DC: NACD, 2011), p. 5.

[40] According to ENISA, a Risk Register is a tool that captures, describes and assesses risks as they are identified, together with risk accountabilities, actions where required, review dates and dates when actions were completed and the risk item closed. A Risk Register is an important tool that helps boards quantify how great a risk cyber is for the company's profile. If there are several risks for a company, and cyber is among the top ten for the company, then that will demand greater time and budget spend by the management team and the board. However, if there is no cyber risk, then a company can relax a bit more. Risk registers should be used to document the portfolio of potential adverse events a company is subject to.

[41] Jody R. Westby, Carnegie Mellon University, *Governance of Enterprise Security: CyLab 2012 Report*, (Pittsburgh, PA: Carnegie Mellon University, 2012), p. 7 and p. 16.

cybersecurity issues on a regular basis and receive information from a range of management team members (Figure 4). Yet a significant number of directors believe their organisations still need improvement in this area. When asked to assess the quality of information provided by the Board to senior management, information about cybersecurity was rated lowest, with nearly a quarter of public-company directors reporting that they were dissatisfied or very dissatisfied with the quality of information provided by management about cybersecurity. Less than 15 percent said they were very satisfied with the quality of the information they received, as compared with an approximately 64 percent high-satisfaction rating for information about financial performance.[42]

NACD survey respondents identified several reasons for their dissatisfaction with management's cybersecurity reporting, including:

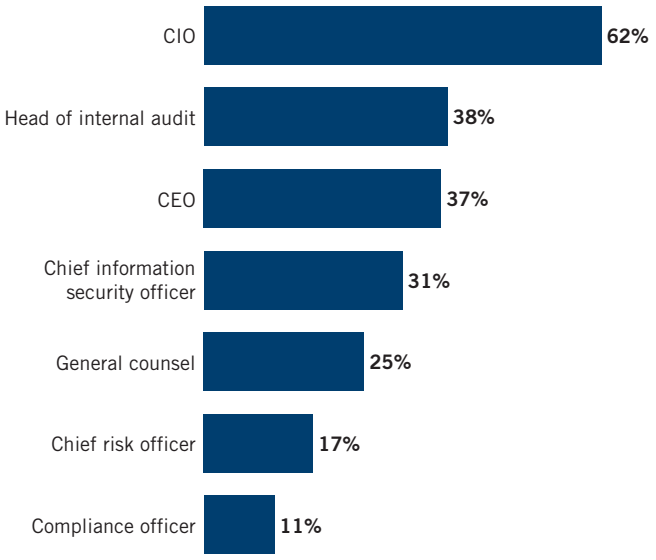
- Difficulty in using the information to benchmark performance, both internally (between business units within the organisation) and externally (with industry peers);
- Insufficient transparency about performance; and
- Difficulty in interpreting the information.[43]

Cybersecurity and cyber-risk analysis are relatively new disciplines (certainly, less mature than financial analysis) and it will take time for reporting practices to mature. Nonetheless, Board members should set clear expectations with management about the format, frequency, and level of detail of the cybersecurity-related information they wish to receive. In reviewing reports from management, directors should also be mindful that there might be an inherent bias on the part of management to downplay the true state of the risk environment. One study found that 60 percent of IT staff do not report cybersecurity risks until they are urgent (and more difficult to mitigate) – and acknowledged that they try to filter out negative results.[44] Boards' should seek to create a culture of open, straightforward and transparent communication on cyber-risk management and reporting.

See **Appendix D** for examples of cyber-risk reporting metrics.

FIGURE 4

Which representatives from management report to the Board about the state of cybersecurity? (Select all that apply)



Source: 2016-2017 NACD Public Company Governance Survey

[42] NACD, *2016-2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p. 28.

[43] Ibid.

[44] Sean Martin, "*Cyber Security: 60% of Techies Don't Tell Bosses About Breaches Unless It's Serious*," *International Business Times*, April 16, 2014.

PRINCIPLE 4

Board directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

Technology integrates modern organisations, whether workers are across the corridor or halfway around the world. But, as noted earlier, the reporting structures and decision-making processes at many companies are legacies of a past, where each department and business unit makes decisions relatively independently, and without fully taking into account the digital interdependency that is a fact of modern life. Directors should seek assurances that management is taking an appropriate enterprise-wide approach to cybersecurity.

Appendix F contains considerations for building a relationship with the CISO and the security team.

Creating an overall approach to cyber-risk management

An organisation should start with an assessment of its unique risk profile and threat environment. The ability of an organisation to implement an effective cybersecurity framework starts with a clear understanding of the risk environment it operates in, its unique risk appetite, and the availability of resources needed to mitigate the potential cyber risks. There is no 'one size fits all'.

Technical controls framework for risk management

In February 2013, U.S. President Barack Obama signed Executive Order 13636 – Improving Critical Infrastructure Cybersecurity. The order instructed the National Institute of Standards and Technology (NIST) to develop a cybersecurity framework that could be voluntarily adopted by the private sector.[45]

Released in 2014, the NIST Cybersecurity Framework is a set of standards, methodologies, procedures, and processes that aligns policy, business, and technological issues to address cyber risks. The framework seeks to provide a common language for senior corporate management to use within the organisation in developing an enterprise-wide approach to cyber-risk management. It suggests that to start their cybersecurity review, corporations engage in a risk-management process that will determine where the organisation sits on a four-tier scale: (1) partial, the lowest tier; (2) risk informed; (3) repeatable; and (4) adaptive, the highest tier.

This level of management may be beyond the practical ability of all organisations, but some elements are available to all companies. According to a 2015 U.S. National Cybersecurity Institute study of information-security professionals, over 50 percent of respondents said their companies were using the framework, and adoption rates were over 80 percent in the U.S. federal government.[46]

Although NIST is used by a number of transatlantic organisations, there is no equivalent government sponsored cybersecurity framework in the United Kingdom. Within the UK there is, however, fairly wide adoption of the international ISO/IEC 27001 information security management standard.[47] In addition, high level guidance is regularly issued by the National Cyber Security Centre, and the National Cyber Security Strategy 2016-2021 contains some broad principles for businesses (albeit that the primary focus is on national security).

At the European level, the European Union Agency for Network and Information Security (ENISA) has also issued advice and recommendations on information security best practice. In September 2017, the European Commission proposed to reform ENISA and establish a voluntary certification framework that will provide a comprehensive EU industry-wide set of rules, technical requirements, standards and procedures on cybersecurity.[48]

It should be noted that there also may be industry specific cybersecurity framework(s) relevant to organisations. For example, the CBEST framework, launched by the UK financial authorities (Bank of England, Her Majesty's Treasury and the Financial Conduct Authority) in 2014, is the primary method used by the UK's financial services industry to voluntarily test cybersecurity resiliency.

[45] Executive Order No. 13636 – Improving Critical Infrastructure Cybersecurity, Federal Register 78, no. 33, (Feb. 19, 2013).

[46] Arieanna Schweber, "Adoption rate soars for NIST framework," InTelligence Blog, Jan. 12, 2016, and Kevin L. Jackson, "*What has NIST done for me lately?*," *Direct2Dell* (blog), Jan. 4, 2016.

[47] ISO/IEC 27001 Information Security Management. (n.d.). Retrieved February 13, 2018. Barlette, Yves & Fomin, Vladislav. (2009). The adoption of Information Security Management Standards: A Literature Review. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions. 119-140. 10.4018/978-1-60566-326-5.ch006.

[48] ENISA. (2017, September 13). European Commission proposal on a Regulation of the European Parliament and of the Council on the future of ENISA [Press release].

An Integrated Approach to Cyber-Risk Governance

1. Establish ownership of cyber risk on a cross-departmental basis. A senior manager with cross-departmental authority, such as the Chief Financial Officer, Chief Risk Officer, or Chief Operating Officer (not the Chief Information Officer), should lead the team.
2. Appoint a cross-organisation cyber-risk management team. All substantial stakeholder departments must be represented, including business unit leaders, legal, internal audit and compliance, finance, HR, IT, and risk management. (See "Roles and Responsibilities of Key Management" excerpt below). A key objective of such a cross-organisational effort is to ensure that there is no cybersecurity weak link or exception within the organisation.
3. The cyber-risk team needs to perform a forward-looking, enterprise-wide risk assessment, using a systematic framework that accounts for the complexity of cyber risk; including, but not limited to, regulatory compliance. This would include assessing the organisation's current threat landscape and risk picture. Then, clearly establishing its risk appetite. Identifying potential risk to the organisation, as well as its risk threshold, will help the cyber-risk team assess which systematic framework aligns most appropriately with its mission and goals.
4. Be aware that cybersecurity laws and regulations differ significantly across jurisdictions and sectors. As noted in Principle 2, management should dedicate resources to tracking the standards and requirements that apply to the organisation, especially as some countries aggressively expand the scope of government involvement in the cybersecurity arena.
5. Take a collaborative approach to developing reports to the Board. Executives should be expected to track and report metrics that quantify the business impact of cyber-threats and associated risk-management efforts. Evaluation of cyber-risk management effectiveness and the company's cyber-resiliency should be conducted as part of quarterly internal audits and other performance reviews. These reports should strike the right balance between too much detail and what is strategically important to report to the Supervisory Board.
6. Develop and adopt an organisation-wide cyber-risk management plan and internal communications strategy across all departments and business units. While cybersecurity obviously has a substantial IT (Technology) component, all stakeholders need to be involved in developing the corporate plan and should feel "bought in" to it, including the legal, audit, risk and compliance functions. Testing of the plan should be done on a routine basis.
7. Develop and adopt a total cyber-risk budget with sufficient resources to meet the organisation's needs and risk appetite. Resource decisions should take into account the severe shortage of experienced cybersecurity talent, and identify what needs can be met in-house versus what can or should be outsourced to third parties. Because cybersecurity is more than IT (or Technology) security, the budget for cybersecurity should not be exclusively tied to one department: examples include allocations in areas such as employee training, tracking legal regulations, public relations, product development, and vendor management. The budget could also include a talent review and succession plan for critical management, such as COO, CTO, CISO, etc. Assessing the readiness of successors and determining if additional training for current employees is needed in order to fulfil these roles in the future or whether outside recruitment of talent is necessary increases the organisation's cyber preparedness. By conducting a talent review, an organization can minimize the disruption caused by employee turnover.

Source: Internet Security Alliance[1]

[1] Adapted from Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs* (Washington, DC: ANSI, 2010). See also Internet Security Alliance, *Sophisticated Management of Cyber Risk* (Arlington, VA: ISA, 2013).

Directors should set the expectation that, in developing the company's cyber-risk defence and response plans, management has considered appropriate cybersecurity framework(s) specific to the organisation and the jurisdictions in which it operates.

Roles and responsibilities of key management

While each organisation will have a unique management structure with varying titles, roles, and responsibilities, it is useful for the roles and responsibilities of key senior management to be clearly established, especially when it comes to creating a cross-organisation cyber-risk management team. The following are examples of roles and related responsibilities:

- **Chief Risk Officer** – cyber-risk detection, prevention and mitigation; training & communications
- **Chief Compliance (& Ethics) Officer** – policy development and enforcement; training and communications; investigations
- **Chief Legal Officer/General Counsel** – legal and regulatory awareness, compliance, policies, litigation; investigations
- **Chief Privacy Officer** – intimate knowledge of privacy laws, rules; policy development and enforcement; training and communications; privacy audits. *(NOTE: ALTERNATIVELY, THIS FUNCTION COULD BE SUBSUMED UNDER THE CHIEF COMPLIANCE OFFICER).*
- **Outside Legal Counsel** – external legal assistance when needed; attorney client privilege; investigations; representation to government and regulatory authorities

PRINCIPLE 5

Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Total cybersecurity is an unrealistic goal. Cybersecurity, as with security in general, is a continuum, not an end state, and security is not the equivalent of compliance. Management teams need to determine where, on a spectrum of risk, they believe the firm's operations and controls have been optimised. As with other areas of risk, an organisation's cyber-risk tolerance must be consistent with its business strategy and objective. When an organisation analyses their cyber risk, they ought to do so as part of their overall risk assessment, properly placing cyber in the context of other risks. A risk register can be helpful in their process.[49] Security resource allocation is a function of balancing business goals with the inherent risks in digital systems (see "Defining Risk Appetite," page 25). There are multiple cyber risks and multiple methods to address them. Management needs to present the Board with a clear picture of the risk landscape and a plan for addressing it. As such, directors and management teams will need to grapple with the following questions:

- **What data, systems and business operations are we willing to lose or have compromised?** Discussions of risk tolerance will help to identify the level of cyber risk the organisation is willing to accept as a practical business consideration. In this context, distinguishing between mission-critical or highly sensitive data (see "Identifying the Company's 'Crown Jewels,' and highly sensitive categories of data" page 11) and other data or systems that are as important, but less essential or sensitive, is a key first step. However, data compromise is not the only component of cyber risk. Legal implications, including regulatory sanctions for data breaches, could exist that far exceed the actual value of the data, and reputational risk from bad publicity may correspond more to external factors than the actual value of the systems compromised.

- **How should our cyber-risk mitigation investments be allocated among basic and advanced defences?** When considering how to address more sophisticated threats, management should place the greatest focus on sophisticated defences designed to protect the company's most critical data and systems. While most organisations would agree with this in principle, in reality, many organisations apply security measures equally to all data and functions. However, research demonstrates that protecting low-impact systems and data from sophisticated threats could require greater investment than the benefits warrant. For those lower-priority assets, organisations should consider accepting a greater level of security risk than higher-priority assets, or choosing instead to transfer the impact of such risks via insurance as the costs of defence will likely exceed the benefits.[50] Boards should encourage management to frame the company's cybersecurity investments in economic terms of (ROI), and to reassess ROI regularly. New analytical tools have recently come on the market that can assist management in better defining cyber risk in economic terms and management should consider if these tools are appropriate for their cyber-risk calculations.

- **What options are available to assist us in mitigating certain cyber risks?** Organisations of all industries and sizes have access to end-to-end solutions that can assist in reducing some portion of cyber risk. They include a battery of preventative measures such as reviews of cybersecurity frameworks and governance practices, employee training, IT security, expert response services and managed security services. Beyond coverage for financial loss, these tools can help to mitigate an organisation's risk of suffering property damage and personal injury resulting from a cyber-breach. Some solutions also include access to proactive tools, employee training, IT security, and expert response services, to add another layer of protection and expertise. The inclusion of these value-added services proves even further the importance of moving cybersecurity outside of the IT department into enterprise-wide risk and strategy discussions at both the management and Board levels. However, management needs to keep the Board informed of the rapidly changing cyber-risk landscape and be agile enough to adjust to quickly changing

[49] According to ENISA, a Risk Register is a tool that captures, describes and assesses risks as they are identified, together with risk accountabilities, actions where required, review dates and dates when actions were completed and the risk item closed. A Risk Register is an important tool that helps boards quantify how great a risk cyber is for the company's profile. If there are several risks for a company, and cyber is among the top ten for the company, then that will demand greater time and budget spend by the management team and the board. However, if there is no cyber risk, then a company can relax a bit more. Risk registers should be used to document the portfolio of potential adverse events a company is subject to.

[50] AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, October 2013, p. 8.

technologies and cyber-attack scenarios such as data theft, data corruption, and even the use of security mechanisms (e.g. encryption) as attack methods (e.g., ransomware).

- **What options are available to assist us in transferring certain cyber risks?** Cyber insurance exists to provide financial reimbursement for unexpected losses related to cybersecurity incidents. This may include accidental disclosure of data, such as losing an unencrypted laptop, or malicious external attacks, such as phishing schemes, malware infections, or denial-of-service attacks. When choosing a cyber-insurance partner, it is important for an organisation to choose a carrier with the breadth of global innovation that best fits the organisation's needs. Insurers frequently conduct in-depth reviews of company cybersecurity frameworks during the underwriting process and policy pricing can be a strong signal that helps companies understand their cybersecurity strengths and weaknesses. Many insurers, in partnership with technology companies, law firms, public relations companies and others, also offer access to the preventative measures discussed above.

- **How should we assess the impact of cybersecurity incidents?** Conducting a proper impact assessment can be challenging given the number of factors involved. In an interconnected world, there may be cyber risks to the organisation that exist outside the organisation's ability to directly mitigate them effectively. For example, publicity about data breaches can substantially complicate the risk evaluation process. Stakeholders (including employees, customers, suppliers, investors, the press, the public, and government agencies) may see little difference between a comparatively small breach and a large and dangerous one. As a result, reputational damage and associated impact (including reactions from the media, investors, and other key stakeholders) may not correspond directly to the size or severity of the event. The Board should seek assurances that management has carefully thought through these implications in devising organisational strategies for cyber-risk management that include operational IT management, but also include strategies such as legal agreements with partners and vendors helping to ensure appropriate security and a communication plan to address reputational risk when an event occurs.

Defining Risk Appetite

"Risk appetite is the amount of risk an organisation is willing to accept in pursuit of strategic objectives. Thus, it should define the level of risk at which appropriate actions are needed to reduce risk to an acceptable level. When properly defined and communicated, it drives behaviour by setting the boundaries for running the business and capitalizing on opportunities.
"A discussion of risk appetite should address the following questions:

- Corporate values – What risks will we not accept?
- Strategy – What are the risks we need to take?
- Stakeholders – What risks are they willing to bear, and to what level?
- Capacity – What resources are required to manage those risks?
- "Risk appetite is a matter of judgement based on each company's specific circumstances and objectives. There is no one-size-fits-all solution."

Source: PwC, Board oversight of risk: Defining risk appetite in plain English (New York, NY: PwC, 2014), p. 3

Conclusion

Cybersecurity is a serious enterprise-level risk issue that affects virtually all levels of an organisation's activities. Several characteristics combine to make the nature of the threat especially formidable: its complexity and speed of evolution; the potential for significant financial, competitive, and reputational damage; and the fact that total protection is an unrealistic objective. In the face of such threats, and despite dramatic increases in private-sector cybersecurity spending,[51] the economics of cybersecurity still favour attackers. Moreover, many business innovations come with increased vulnerability, and risk management in general and cybersecurity measures in particular have traditionally been considered to be cost centres in most for-profit institutions.

Directors need to continuously assess their capacity to address cybersecurity, both in terms of their own fiduciary responsibility as well as their oversight of management's activities, and many will identify gaps and opportunities for improvement. While the approaches taken by individual Boards will vary, the principles in this handbook offer benchmarks and a suggested starting point.

Boards should seek to approach cyber risk from an enterprise-wide standpoint:

- Understand the legal ramifications for the company, as well as for the Board itself.
- Ensure directors have sufficient agenda time and access to expert information in order to have well-informed discussions with management.
- Integrate cyber-risk discussions with those about the company's overall tolerance for risk.

Ultimately, as one director put it, "Cybersecurity is a human issue."[52] The Board's role is to bring its judgement to bear and provide effective guidance to management, in order to ensure the company's cybersecurity strategy is appropriately designed and sufficiently resilient given its strategic imperatives and the realities of the business ecosystem in which it operates.

[51] Steve Morgan, "*Worldwide Cybersecurity Spending Increasing to $170 Billion by 2020*," Forbes, Mar. 9, 2016. See also Piers Wilson, Security market trends and predictions from the 2015 member survey, Institute of Information Security Professionals.

[52] NACD, et al., *Cybersecurity: Boardroom Implications* (Washington, DC: NACD, 2014) (an NACD white paper), p.7.

APPENDIX A

Questions directors can ask themselves to assess their "Cyber Literacy"

Even prior to a Board meeting, directors may do well to self-assess if they have considered various aspects of cybersecurity beyond the technical and operational aspects. In particular, Boards should be thinking of cybersecurity in business terms, and considering if they are preparing their organisation on a strategic level. Among the questions directors may want to ask are the following:

1. Does the CEO encourage open access between and among the Board, external sources, and management about emerging cyber-threats?
2. What do we consider our most valuable business assets? How does our IT system interact with those assets?
3. Are we considering the cybersecurity aspects of our major business decisions, such as M&A, partnerships, new product launches, etc., in a timely fashion?
4. Do we think there is adequate protection in place if someone wanted to get at or damage our corporate "crown jewels" or other highly sensitive data? What would it take to feel confident that those assets/data were protected?
5. Are we spending wisely on cybersecurity tools and training? Do we know if our spending is cost effective? Are we actually improving security or just completing compliance requirements?
6. Who is managing our cybersecurity? Do we have the right talent and clear lines of communication/accountability/responsibility for cybersecurity? Is cyber included in our risk register?[53]
7. Have we considered how we would manage our communications in the case of an event, including communicating with the public, our shareholders, our regulators, our rating agencies? Do we have segmented strategies for each of these audiences?
8. Does our organisation participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organisations? Should we?
9. Is the organisation adequately monitoring current and potential cybersecurity-related legislation and regulation?[54]
10. Does the company have adequate insurance, including Directors and Officers, that covers cyber events? What exactly is covered?[55] Are there benefits beyond risk transfer to carrying cyber insurance?[56]

[53] Lexology.com, Ed Batts, DLA Piper LLP, "Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members," Jan. 23, 2014.

[54] Ibid.

[55] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."

[56] Ibid.

RETURN TO TABLE OF CONTENTS

APPENDIX B

Questions for the Board to ask management about cybersecurity

Principles 4 & 5 in this Handbook relate to the Board's responsibility to have management provide adequate information to manage cyber risk at the strategic level. In implementing these principles, Board members may choose to ask some of the following questions of management. Cybersecurity questions should not only be raised in the context of an existing breach, but at various points in the business development process. For ease of use, the Handbook breaks down the questions into relevant topics that have cybersecurity implications.

Situational awareness

1. What are our critical business services? How do they map to legal entities, regulators' perspectives, IT departments, and suppliers?
2. How are we using IT operations to advance our business goals, and what are the weaknesses in our approach?
3. What are the company's cybersecurity risks, and how is the company managing these risks?[57]
    a. Do we have an inventory of IT systems and list of most critical IT systems?
    b. Where is the highest risk? Where are we in the replacement of outdated programs?
    c. What is our board map to approve these in order to understand age of the systems and when it is time to replace/update?
4. Were we told of cyber-attacks that have already occurred and how severe they were?
5. What is important to protect, and how many times have we seen these assets compromised?
6. Who are our likely adversaries?
7. In management's opinion, what is the most serious vulnerability related to cybersecurity (including within out IT (and technology) systems, personnel, or processes)?
8. If an adversary wanted to inflict the most damage on our company, how would they go about it?
9. Has the company assessed the insider threat?[58]
10. When was the last time we conducted a penetration test or an independent external assessment of our cyber defences? What were the key findings, and how are we addressing them? What is our maturity level?
11. Do we answer to regulators or external auditors? When would an audit likely occur? What would an audit mean for compliance and risk management?
12. Does our external auditor indicate we have cybersecurity-related deficiencies in the company's internal controls over financial reporting? If so, what are they, and what are we doing to remedy these deficiencies?
13. Have we considered obtaining an independent, third-party assessment of our cybersecurity risk management program?
14. Are we members of information sharing communities? If so, what are the lessons learned from our peers who have experienced breaches?

Strategy and operations

1. What are the frameworks we align to, and have you done a gap analysis?
2. Do we have appropriately differentiated strategies for general cybersecurity and for protecting our mission-critical assets?
3. Do we have an enterprise-wide, independently budgeted cyber-risk management team? Is the budget adequate? How is it integrated with the overall enterprise risk management process? What kind of strategy decisions have an impact on cyber risk?
4. Do we have a systematic framework, such as the NIST Cybersecurity Framework, or ISO in place to address cybersecurity and to assure adequate cybersecurity hygiene?
5. Where do management and our IT/Technology teams disagree on cybersecurity?
6. Do the company's outsourced providers and contractors have cybersecurity controls and policies in place? Are those controls monitored? Do those policies align with our company's expectations?
7. What is our insurance coverage for cyber? Is it adequate and what kind do we have? Why do we have that sort of insurance?
8. Is there an ongoing, company-wide awareness and training program established around cybersecurity?
9. What is our strategy to address cloud, BYOD, and supply-chain threats?[59]

[57] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."
[58] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."
[59] Lexology.com, Ed Batts, DLA Piper LLP, "Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members," Jan. 23, 2014.

10. How are we addressing the security vulnerabilities presented by an increasingly mobile workforce?
11. Are we growing organically or buying companies? Are they mature companies or start-ups? Where are we geographically?

Insider threats

1. How do our operational controls, including access restrictions, encryption, data backups, monitoring of network traffic, etc., help protect against insider threats?
2. How have we adapted our personnel policies, such as background checks, new employee orientation, training related to department/role changes, employee exits, and the like, to incorporate cybersecurity?
3. Do we have an insider-incident activity plan that spells out how and when to contact counsel, law enforcement and/or other authorities, and explore legal remedies?
4. Do we have forensic investigation capabilities?
5. What are the leading practices for combating insider threats, and how do ours differ?
6. How do key functions (IT, HR, Legal, and Compliance) work together and with business units to establish a culture of cyber-risk awareness and personal responsibility for cybersecurity? Considerations include the following:

a. Written policies which cover data, systems, and mobile devices should be required and should cover all employees.
b. Establishment of a safe environment for reporting cyber incidents (including self-reporting of accidental issues).
c. Regular training on how to implement company cybersecurity policies and recognise threats.

7. What are we trying to prevent by protecting against insider threats?

Supply-chain/third-party risks

1. What do we currently do and what will need to be done to fully include cybersecurity in our current supply-chain risk management?
2. How much do we know about our supply chain regarding cyber-risk exposure and controls? What due diligence processes do we use to evaluate the adequacy of our suppliers' cybersecurity practices (both during the on-boarding process and during the lifetime of each contract)? Which departments/business units are involved? Are there appropriate contingency arrangements in place in the event of a major problem with critical third-party suppliers?
3. Does the business carry out appropriate strategic monitoring of third party suppliers?
4. What providers do we use for the Cloud? Which critical business functions have we outsourced to third parties, such as Cloud security?
5. How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks?
6. How are cybersecurity requirements built into vendor agreements? How are they monitored, and are we doing our due diligence to enforce contracts? Contracts can be written to include minimum cybersecurity requirements, including for example:
    a. Written cybersecurity policies.
    b. Personnel policies, such as background checks, training, etc.
    c. Access controls.
    d. Encryption, backup, and recovery policies.
    e. Detailed requirements regarding data held by the third party.
        i. Retention and deletion requirements for data held.
        ii. Clear inventories of types of data held.
        iii. Clarity on what is stored, moved, processed, etc.
    f. Secondary access to data.
    g. Countries where data will be stored.
    h. Notification of data breaches or other cyber incidents.
    i. Communication plans for incident reporting and response.
    j. Incident-response plans.
    k. Audits of cybersecurity practices and/or regular certifications of compliance.
7. Do we allow our suppliers to subcontract the delivery of any part of the contract? If so, what level of control/scrutiny do we exercise over the subcontracting arrangements? How do we monitor changes to subcontracting arrangements through the lifetime of the contract?
8. Do we have technology in place to profile suppliers and partners from the cybersecurity point of view to identify potential vulnerabilities and actively manage third party risk?
9. Are we indemnified against security incidents in our supply chain? What is the financial strength of the indemnification?
10. How difficult/costly will it be to establish and maintain a viable cyber-vulnerability and penetration-testing system for our supply chain?

11. How difficult/costly will it be to enhance monitoring of access points in the supplier networks?
12. Do our vendor agreements bring incremental legal risks or generate additional compliance requirements (e.g., GDPR, FCA, etc.)?

Planning for a potential incident, crisis management and response

1. What is our ability to protect, detect and respond to incidents? How does it compare with others in our sector?
2. In the context of our business, what constitutes a material cybersecurity breach? How does this compare to the definition (if any) included in relevant laws and regulations applicable to our business?
3. At what point is the Board informed of an incident? What are the criteria for reporting?
4. What is known about the intent and capability of the attacker? What do we know about how the attacker might use the data?
5. Are we clear as to who must be notified and when? What are the timetables and strategy considerations for reporting incidents to customers? Regulators/relevant government entities? Law Enforcement? Vendors/partners? Internally? Peers? Investors? What timetables are mandated by laws and regulations and what is at the company's discretion?
6. How will management respond to a cyber-attack?[60] Does the company have a validated incident-response plan?[61] Are we adequately exercising our cyber-preparedness and response plan?[62]
7. Do we have a crisis management plan in place? For significant breaches, how good is our communication plan (both internally and externally) as information is obtained regarding the nature and type of breach, the data impacted, and the ramifications to the company and the response plan?
8. What are we doing to avoid making the problem worse for our organization? How do we ensure we have appropriate legal advice in the incident and crisis management teams? Are the legal teams integrated in the incident and crisis plans?

After a Cybersecurity Incident

1. How did we learn about the incident? Were we notified by a third party, or was the incident discovered internally?
2. What do we believe was the motive for the incident? What was the impact, and how do we measure it? Have any of our operations been compromised?
3. Is our cyber-incident/crisis response plan in action, and is it working as planned?
4. What is the response team doing to ensure that the incident is under control and that the attacker no longer has access to our internal network?
5. What were the weaknesses in our system that allowed the incident to occur and why had they not been identified or remediated?
6. Has the security team checked for associated vulnerabilities across all company systems/networks, not just the affected systems or services? Have they checked what happened against the controls framework and made the necessary changes to both security controls and business controls?
7. What steps can we take to make sure this type of event does not happen again? How do we ensure that lessons are learned and remediation actions tracked?
8. What can we do to mitigate any losses caused by the incident?
9. Does the incident alter the risk tolerance of the business? Has this been discussed and have any changes been captured?

Source: NACD, et al., *Cybersecurity: Boardroom Implications* (Washington, DC: NACD, 2014) (an NACD white paper).

[60] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."
[61] Ibid.
[62] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."

APPENDIX C

Cybersecurity considerations during M&A phases

Companies involved in transactions are often prime targets for hackers and cybercriminals, because the value of confidential deal-related information is high, and the short timelines, high-pressure environment, and significant workloads associated with transactions can cause key players to act carelessly and potentially make mistakes. Cybersecurity vulnerabilities exploited during a transaction can pose risks to the deal's value and return on investment:

Short-term risks

- Paralysed operations as a result of ransomware or malware.
- Transaction period might be used by threat actors to gain entry and conduct reconnaissance, an event which often is not detected until well after the deal closes.
- Theft of inside information, including valuations, bids, etc.
- Warranty claims, a change of deal terms, or a reduction in the deal's value.
- Forensic investigations related to a data breach.

Long-term risks

- Exposure to risk from regulatory and other lawsuits.
- Regulatory investigation and penalties.
- Loss of customers, and associated impacts on sales and profit.
- Reputational damage.
- Loss of market share to competitors without a known data breach.

Directors should ask management to conduct a cyber-risk assessment for each phase of the transaction's lifecycle to confirm that systems and processes are secure, and to quantify the risks that may impact the company after the deal closes, including revenues, profits, market value, market share, and brand reputation.

Strategy and target identification phase

The risk of attack starts even before an official offer or merger announcement is made. Law firms, financial advisors, consultants and other associated firms are attractive to hackers because they hold trade secrets and other sensitive information about corporate clients, including details about early-stage deal exploration that could be stolen to inform insider trading or to gain a competitive advantage in deal negotiations. According to a report from CERT-UK[63], law firms may represent the weakest link in the chain to reach their clients' data and the Information Commissioner's Office (ICO) also reported a 32% year on year increase in data breaches from the legal sector in 2015. A Company therefore needs to have an understanding of the controls and security in place at all of the third parties assisting it during the M&A process and a thorough understanding of how sensitive data is to be shared between parties.

Attackers look for hints that a company is considering a merger, acquisition, or divestiture. They may be tipped off by industry gossip, a slowdown in a company's release cycle, staff reductions, or data leakage through social media channels. There are four primary ways that information is at risk:

- A hacker enters the network through gaps in its defences, starting with a company's Internet-facing computers.
- A hacker launches a social engineering attack against a company employee.
- Company insiders (employees, contractors, vendors) release sensitive data and information, either intentionally or as a result of negligence. The risk of insider threats heightens significantly in an M&A.
- Information is exposed through vulnerabilities in third-party vendors or service providers.

During this phase, management should gain an understanding of cyber risks associated with the target company and model the impact of those risks to compliance posture, financial forecasts, and potential valuations. Management can perform the following analysis even before direct engagement with the target company begins:

- Conducting "dark web"[64] (difficult-to-access websites favoured by hackers) searches about the target, their systems, data, and intellectual property. This helps identify whether the company

[63] https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-threats-to-the-legal-sector-and-implications-to-UK-businesses.pdf

[64] The Dark Web is a general term describing hidden Internet sites that users cannot access without using special software such as TOR ("The Onion Router"). While the content of these sites may be accessed, the publishers of these sites are concealed. Users access the Dark Web with the expectation of being able to share information and/or files with little risk of detection.

RETURN TO TABLE OF CONTENTS

is already on hackers' radar, if systems or credentials are already compromised, and if there is sensitive data for sale or being solicited. Management will need to consider the lawfulness of such searches with reference to the information being accessed.

- Profiling the target company from the cybersecurity point of view, while implementing relevant technology.
- Researching malware infections in the target company and gaps in their defences visible from the outside. This information is publicly available and can be used to compare one company to another, allowing management to save time and energy by not pursuing companies whose risk profile is unacceptably high.
- Modelling the financial impact of identified cyber risks. These risks may not only impact a company's return on invested capital, but also result in loss of competitive advantages, costly remediation, fines, and possibly years of litigation, depending on what was stolen. An initial estimate of the impact may be material enough to encourage strategy teams to alter a deal trajectory. The estimate can be refined as the transaction process continues and as risks are mitigated.

Due diligence and deal execution phases

During these phases, the company should perform confirmatory cybersecurity due diligence. Significant problems would call for negotiation of a reduction in purchase price to cover costs of necessary remediation. Depending on the risks identified, the Board may want to defer approving the transaction until remediation is complete, or decide to back out of a transaction if the risks that are identified warrant such action. Identification of cybersecurity risks during the diligence phase can be accomplished by performing cybersecurity diligence that is tailored to discover these risks:

- Identify insufficient investments in cybersecurity infrastructure, as well as deficiencies in staff resources, policies, etc.
- Identify lax cultural attitudes toward cyber risk.
- Determine cybersecurity-related terms and conditions (or, the lack thereof) in customer and supplier contracts that have a potential financial impact or result in litigation for noncompliance.
- Discover noncompliance with cyber-related data privacy laws or other applicable regulations and requirements.
- Identify recent data breaches or other cybersecurity incidents.

Effective due diligence on cybersecurity issues demonstrates to investors, regulators, and other stakeholders that management is actively seeking to protect the value and strategic drivers of the transaction, and that they are aiming to lower the risk of a cyber-attack before integration. These risks and upsides can then be factored into the initial price paid and into performance improvement investments that will raise the transaction value, enabling a robust transaction proposal to be presented to shareholders for approval.

Integration phase

Post-deal integration poses a range of challenges related to people, processes, systems, and culture. Cyber risks add another dimension of complexity and risk to this phase of the transaction. Hackers take advantage of the inconsistencies that exist between the platforms and technology operations of the company and the newly-merged or acquired entity at this phase.

Integration teams need to have the expertise to explore and delve into the smallest of details to identify and mitigate cyber risks such as the following:

- Security gaps identified during preceding phases.
- Prioritization of remediation activities based on potential impact of identified gaps.
- Prioritization of integration activities.
- Employee training on newly integrated systems.

Post-transaction value creation phase

After a transaction is completed, continued monitoring of cyber risks by management will create numerous opportunities for portfolio improvement and growth.

Management should continue to evaluate the cyber maturity of the merged or acquired entity by benchmarking it against industry standards and competition, just as they do with the core business. Low maturity could impact growth projections and brand reputation due to cyber incidents and possible fines. A breach or compliance issue could cause regulators to investigate, leading to a financial loss or stalling of post-transaction exit plans. Cyber issues can also lead to legal action by customers and suppliers causing value loss and lower returns.

RETURN TO TABLE OF CONTENTS

A view from the sell side

Many of the same risks impacting the acquiring company that are described herein will of course equally apply to the seller side. In the post transaction valuation creation phase, the seller is particularly exposed to breach disclosures that may impact the deal price/timing and even the ongoing operations of the selling entity if the transaction falls through. Accordingly, a thorough understanding of existing risk vectors prior to deal execution will better inform the nature of warranties made by the selling corporation and reduce exposure. Information flow to directors of selling companies may be more limited in its nature and frequency as time passes after deal announcement and directors should establish the thresholds and nature for any breach communications in the post announcement period.

Conclusion

Cybersecurity diligence during M&A calls for a two-pronged approach. Companies must conduct rigorous due diligence on the target company's cyber risks and assess their related business impact throughout the deal cycle to protect the transaction's return on investment and the entity's value post-transaction. In addition, all parties involved in the deal process need to be aware of the increased potential for a cyber-attack during the transaction process itself and should diligently maintain their cybersecurity efforts. Applying this two-pronged approach during M&A will serve to ultimately protect stakeholder value.

APPENDIX D

Board-level cybersecurity metrics

Which cybersecurity metrics should be included in a Board-level briefing? This question is deceptively simple. Similar to virtually every other division and function within the organisation, the cybersecurity function collects and analyses a tremendous volume of data and there is little consensus on which are the critical few pieces of data that should be shared with a Board audience. Adding to the challenge is the fact that cybersecurity is a relatively new domain, with standards and benchmarks that are still developing or evolving.

Ultimately, directors will need to work with members of management to define the cybersecurity information, metrics, and other data that is most relevant to them given the organisation's operating environment – including industry or sector, regulatory requirements, geographic footprint, and so on. More often than not, Boards see a high volume of operational metrics which provide very little strategic insight on the state of the organisation's cybersecurity program. Metrics that are typically presented include statistics such as "number of blocked attacks," "number of unpatched vulnerabilities," and other stand-alone, compliance-oriented measures, that provide little strategic context about the organisation's performance and risk position.

As a starting point, directors can apply the same general principles used for other types of Board-level metrics to cybersecurity-related reporting (see Sidebar, "Guiding Principles for Board-Level Metrics").

In addition, the following recommendations provide a starting point for the types of cybersecurity metrics that Board members should consider requesting from management.

1. What is our cyber-risk appetite? This is a fundamental question and one that the Chief Information Security Officer (CISO) should work with the Chief Risk Officer (CRO) function to address. This type of collaboration can produce qualitative and quantitative data points for presentation to the Board that provide context around cyber-risk appetite.
2. What metrics do we have that indicate risk to the company? One organisation has implemented a cybersecurity risk "index" which incorporates several individual metrics covering enterprise, supply chain, and consumer-facing risk.
3. How much of our IT/technology budget is being spent on cybersecurity-related activities? How does this compare to our competitors/peers, and/or to other outside benchmarks? These metrics will support conversations about how management determines "how much spending is enough," and whether increasing investments will drive down the organisation's residual risk. Additional follow-on questions include these:
   - What initiatives were not funded in this year's budget? Why?
   - What trade-offs were made?
   - Do we have the right resources, including staff and systems, and are they being deployed effectively?
4. How do we measure the effectiveness of our organisation's cybersecurity program and how it compares to those of other companies? Board-level metrics should highlight changes, trends and patterns over time, show relative performance, and indicate impact. External penetration-test companies and third-party experts may be able to provide an apples-to-apples comparison within industry sectors.
5. How many data incidents (e.g., exposed sensitive data) has the organisation experienced in the last reporting period? These metrics will inform conversations about trends, patterns, and root causes.
6. Value chain relationships typically pose increased risk for companies given the degree of system interconnectivity and data-sharing that is now part of everyday business operations. How do we assess the cyber-risk position of our suppliers, vendors, JV partners, and customers? How do we conduct ongoing monitoring of their risk posture? How many external vendors connect to our network or receive sensitive data from us? This is a borderline operational metric, but it can help support discussions with management about residual risk from third parties. There are service providers within the cybersecurity market place that provide passive and continuous monitoring of companies' cybersecurity postures. A growing number of firms use these services to assess their high-risk third-party relationships as well as their own state of cybersecurity.
7. What operational metrics are routinely tracked and monitored by our security ream? While operational metrics are the domain of the IT/Security team, it would be beneficial for directors to understand the breadth and depth of the company's cybersecurity monitoring activities for the purposes of situational awareness.

RETURN TO TABLE OF CONTENTS

8. What metrics do we use to evaluate cybersecurity awareness across the organisation? Data about policy compliance, the implementation and completion of training programs, and the like will help to inform conversations about insider risks at various seniority levels and in various regions and divisions.
9. How do we track the individuals or groups that are exempt from major security policies, activity monitoring, etc.? These measures will indicate areas where the company is exposed to additional risk, opening the way for discussions about risk/return trade-offs in this area.

Guiding principles for board-level metrics

- Relevant to the audience (full-board; key committee)
- Reader-friendly: Use summaries, callouts, graphics, and other visuals; avoid technical jargon
- Convey meaning: Communicate insights, not just information
  - Highlight changes, trends, patterns over time
  - Show relative performance against peers, against industry averages, against other relevant external indicators, etc. (e.g., maturity assessments)
  - Indicate impact on business operations, costs, market share, etc.
- Concise: Avoid information overload
- Above all, enable discussion and dialogue

Developing Cyber Economic Metrics

Cyber risk is now accepted as a Board-level conversation. The challenge, however, is how to effectively and precisely communicate the financial impact of cyber incidents to the Board. Before Boards can make informed decisions on how to manage cyber risk, they must first have the ability to translate cybersecurity data into financial metrics. Board directors will need to work with management to outline the most relevant cybersecurity information given the organization's operating environment, including industry or sector, regulatory requirements, geographic footprint, and so on. To get started, the following board-level cyber-risk recommendations provide a starting point that Boards should consider requesting from management:

- What are our quarterly expected loss ration metrics related to our cyber-risk condition across our various business units and operating environments?
- What is the financial impact related to our cyber-risk worst-case scenario?
- What processes have we established related to making cyber-risk acceptance, cyber-risk remediation, and cyber-risk transfer decisions? How do we measure how these decisions reduce our financial exposure to cyber risk?
- How are we measuring and prioritizing our control-implementation activies and cybersecurity budgets against our financial exposure to cyber risk? Have we connected our control implementation strategy and cybersecurity programs, including budgets, with our cyber-risk transfer strategy?
- Based on our financial performance targets, how can cyber risk impact our financial performance? What is our annual cyber-risk expected loss value?
- What is our cyber-risk remediation plan to achieve our target expected loss tolerance level? Is our plan producing a net positive financial return?
- How does our cybersecurity program align cyber-risk based expected loss ratio analysis and expected loss tolerance targets? How are we measuring, tracking, and demonstrating how our cybersecurity investments are reducing our financial exposure to cyber incidents and delivering cybersecurity return on investment?
- How are we measuring and aligning our cyber risk based expected loss ration analysis and cybersecurity planning with our cyber insurance risk-transfer plan?
- How do we measure the effectiveness of our organization's cybersecurity program and how it compares to those of other companies?

Source: Secure Systems Innovation Corporation (SSIC) and X-Analytics

APPENDIX E

Building a relationship with the CISO and the security team

Until recently, the notion of a senior executive whose efforts were dedicated to ensuring the company's cybersecurity was an alien concept to businesses outside of the technology arena. Times have changed; dedicated C-suite managers responsible for controlling digital risk are on the rise in medium- and large-sized companies in many different industries, a consequence of conducting business in today's always-connected world.

According to one study, 54 percent of companies world-wide employ a Chief Information Security Officer (CISO).[65] Another survey found that organizations with CISOs in place were more likely to have dedicated incident-response teams and plans, and were more confident about the strength of their company's defences against threats such as malware.[66] Where there is no CISO, it will be the security team that carries the responsibilities for cybersecurity. The key is that the Board develops the relationship with those leading on cybersecurity.

Building the right relationships between the CISO or equivalent and the Board is essential. As corporate information security functions become more mature, a new question has arisen: How does the Board effectively communicate with the security function? The CISO or equivalent is responsible for managing significant operational, reputational, and monetary risk, so a relationship of trust with the Board is essential. Many Board members now seek to establish an ongoing relationship with the CISO, and include the security executive in discussion about cybersecurity matters at full-board and/or key-committee-level meetings.

The questions and guidelines below are designed to assist directors in establishing or enhancing a relationship with the CISO or equivalent. They can also help Board members improve their communications with the security team and help Boards to gain a better understanding of the company's overall approach to cybersecurity. Because not every question will have relevance for every company, directors should select those that are most appropriate to the issues and circumstances at hand.

1. Understand the security team's role and mandate.

- What is the security team's charter and scope of authority in terms of resources, decisions rights, budget, staffing, and access to information? How does this compare to leading practice in our industry and generally?[67]
- How is the organisation's cybersecurity budget determined? Comparing this figure with industry spending trends is probably the best way to gain context over the adequacy of funding. What is its size (e.g., percentage of total IT/Technology spending), and how does this figure compare with leading practice in our industry and generally? What role does the security team play in cybersecurity budget allocation and investment decisions? Which security tools or other investments were below the "cut" line in the budget?
- What is the security team's administrative reporting relationship (e.g., CIO, CTO, COO, Head of Corporate Security, other)? Does it differ from the functional reporting relationship? What protocols are in place to ensure that the security team has an independent channel to escalate issues and to provide prompt and full disclosure of cybersecurity deficiencies?[68]
- What role does the security team play in the organisation's enterprise risk management (ERM) structure and in the implementation of ERM processes?
- What role, if any, does the security team play beyond setting and enforcing cybersecurity policies and related control systems?
  - For example, does the security team provide input on the development process for new products, services, and systems or on the design of partnership and alliance agreements, etc., such that cybersecurity is "built in" rather than "added on" after the fact?

[65] PwC, Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016 (New York, NY: PwC, 2015), p. 26, and see Paul Solman, "Chief information security officers come out from the basement," *Financial Times*, Apr. 29, 2014.

[66] Kris Monroe, "Why are CISOs in such high demand?," *Cyber Experts Blog*, Feb. 8, 2016.

[67] See, for example, Marc van Zadelhoff, Kristin Lovejoy, and David Jarvis, *Fortifying for the Future: Insights from the 2014 IBM Chief Information Security Officer Assessment* (Armonk, NY: IBM Center for Applied Insights, 2014).

[68] A 2014 study of global information security issues found that organizations with CISOs reporting outside the CIO's office have less downtime and lower financial losses related to cybersecurity incidents as compared with those who report directly to the CIO. See Bob Bragdon, "Maybe it really does matter who the CISO reports to," *The Business Side of Security* (blog), June 20, 2014.

- Does the security team have the necessary skills, and is the company able to attract and retain the level necessary to be effective?
- How is the division of risk decided? How is company's security posture determined, how is it signed off and how often is it reviewed?
- What are the arrangements in place to be able to scale up the security team in case of a crisis? Do we have the right relationships with suitable third parties?

2. Spending time with the security team before an incident reaps dividends.

- A crisis is the wrong time for directors to get acquainted with the security team and key staff. Board members can arrange to visit the security team and receive orientations first-hand from personnel situated on the front lines of cybersecurity, perhaps scheduled in conjunction with a regular Board meeting or site visit. These sessions will provide valuable insights and learning opportunities for Board members. The security team will appreciate it, too, since visits like this can increase its visibility, raise morale, and reinforce the need to focus on this area.
- Directors can also ask the security executive for an assessment of their personal cybersecurity situation, including the security of their devices, home networks, etc. These discussions are not only informative for individual directors, but also will help safeguard confidential information Board members receive in the course of their service.
- Many security teams routinely produce internal reports for management and senior leadership on cyber-attack trends and incidents. Directors can discuss with the security team, corporate secretary, and Board leaders whether this information might be relevant and useful to include in Board materials.
- Boards can suggest a quarterly or monthly meeting with the key security personnel to access the current state of security and risk exposure. Boards should understand that security is continuously evolving and changing and, therefore, regular meetings to assess the current state of an organisation's risk profile provides insight into what resources are needed and where attention needs to be turned. Boards should also request that a simulation or "table-top exercise" of incident response plans be conducted at least annually.

3. Gain insight into the security team's relationship network.

Inside the organisation

- How does the information-security team collaborate with other departments and corporate functions on cybersecurity-related matters? For example, does the security team coordinate with:
  - Business development regarding due diligence on acquisition targets and partnership agreements;
  - Internal audit regarding the evaluation and testing of control systems and policies;
  - Human resources on employee training and access protocols;
  - Purchasing and supply chain regarding cybersecurity protocols with vendors, customers, and suppliers; and/or
  - Legal regarding compliance with regulatory and reporting standards related to cybersecurity as well as data privacy?
- The security team should be able to articulate how cybersecurity isn't just a technology problem; it's about enabling the company to implement its strategy as securely as possible.
- What support does the security team receive from the CEO, CIO, and senior management team?
- How does the information security team develop and maintain knowledge of the organisation's strategic objectives, business model, and operating activities?
  - For example, in companies that are actively pursuing a "big-data" strategy to improve customer and product analytics, to what extent does the security team understand the strategy and contribute to its secure execution?
- What continuing education activities are undertaken by the information security team in order to remain current in cybersecurity matters?

Outside the organisation

- Does the information security team participate in cybersecurity information-sharing initiatives (e.g., industry-focused, IT/Technology-community-focused, or public-private partnerships)? How is the information that is gathered from participation in such initiatives used and shared within the organisation?
- Does the information security team have relationships with public-sector stakeholders such as law enforcement agencies and regulatory agencies' cybersecurity divisions?

4. Assess performance.

- How is the security team's performance evaluated? How is the information security team's performance evaluated? Who performs these evaluations, and what metrics are used?
- What cybersecurity performance measures and milestones have been established for the organisation as a whole? Do we use a risk-based approach that provides a higher level of protection for the organisation's most valuable and critical assets?
- To what extent are cyber-risk assessment and management activities integrated into the organisation's enterprise-wide risk-management processes? Are we using appropriate cybersecurity to assess cybersecurity hygiene from an organisation-wide perspective?

5. Engage the security infrastructure in discussion about the "state of the organisation."

- What was the organisation's most significant cybersecurity incident during the past quarter? How was it discovered? What was our response? How did the speed of detection and recovery compare with that of previous incidents? What lessons did we learn, and how are these factored into the organisation's continuous improvement efforts?
- What was our most significant "near miss" on cybersecurity in the past quarter? How was it discovered? What was our response? What lessons did we learn, and how are these factored into the organisation's continuous improvement efforts?
- Where have we made the most progress on cybersecurity in the past six months, and to what factor(s) is that progress attributable? Where do our most significant gaps remain, and what is our plan to close those gaps?

RETURN TO TABLE OF CONTENTS

APPENDIX F

Assessing the Board's cybersecurity culture

In 2010, the Report of the NACD Blue Ribbon Commission on Board Evaluation defined boardroom culture as "the shared values that underlie and drive board communications, interactions, and decision making. It is the essence of how things really get done."[69] Five years later, at the National Association of Corporate Directors' (NACD's) first Global Cyber Summit, more than 200 directors from Fortune Global 500 companies and cybersecurity experts discussed several ways in which boardroom culture can support, or hinder, management's cybersecurity efforts. In the words of one participant:

> *Boards need to change their mindsets. We must move from asking, "What's the likelihood we'll be attacked?" to saying, "It's probable that we've been attacked"; from viewing cybersecurity as a cost to viewing it as an investment that helps us stay competitive; from expecting management to prevent or defend against cyber-threats to asking how quickly they can detect and respond to them.*[70]

Directors wishing to incorporate a cybersecurity component into their Boards' self-assessments can use the questions in the table below as a starting point. A rating of 1 is low, a rating of 5 is excellent.

Use the numerical scale to indicate where the Board's culture generally falls on the spectrum shown below. ◄——►							Action Item
Our Board mostly thinks of cybersecurity primarily as an IT/Technology issue.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Our Board understand cybersecurity as an enterprise wide risk management issue.	
Our Board relies on the legal environment for cybersecurity as largely stable and generally applicable to most companies in the same way.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Our Board appreciates the need to regularly seek legal counsel as to an emerging cyber legal landscape tailored to our evolving business plans and environments.	
Our Board does not need regular updating on cybersecurity from industry experts in the field.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Our Board regularly seeks cyber expertise relative to our emerging cyber needs and threat picture.	
Our Board does not feel the need for management to provide a specific plan for managing cyber risk.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Our Board expects management to provide us with an operational and a management framework that reflects the modern impact of digital technology, and how we are to manage that technology, consistent with our business needs and risks.	
Our Board does not expect management to uniquely assess and manage cyber risks.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Our Board expects management to provide us with a clear analysis of what our cyber risks are, which to accept, what we can mitigate, and what we can transfer consistent with our business goals.	

[67] *Report of the NACD Blue Ribbon Commission on Board Evaluation: Improving Director Effectiveness* (Washington, DC: NACD, 2010), p. 7.

[70] Italicized quotations are from participants in the Global Cyber Summit, held Apr. 15-16, 2015, in Washington, DC. Discussions were conducted under the Chatham House Rule.

RETURN TO TABLE OF CONTENTS

About the contributors

The Internet Security Alliance (ISA) is an international trade association, founded in 2000, that is focused exclusively on cybersecurity. The ISA Board consists of the primary cybersecurity personnel from international enterprises, representing virtually every sector of the economy. ISA's mission is to integrate economics with advanced technology and government policy to create sustainably secure cyber systems. In 2014, ISA produced the first Cyber-Risk Oversight Handbook, specifically addressing the unique role corporate Boards play in managing cyber risk. In their annual Global Information Security Survey, PricewaterhouseCoopers (PwC) reported that the Handbook was being widely adopted by corporate Boards and that its use resulted in better cybersecurity budgeting, better cyber-risk management, closer alignment of cybersecurity with overall business goals, and helping to create a culture of security in organizations that use it. For more information about ISA, visit www.isalliance.org.

American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. 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 | Twitter: @AIGinsurance | LinkedIn.

2500 Wilson Blvd. #245
Arlington, VA 22201, USA
+1 (703) 907-7090
isalliance.org