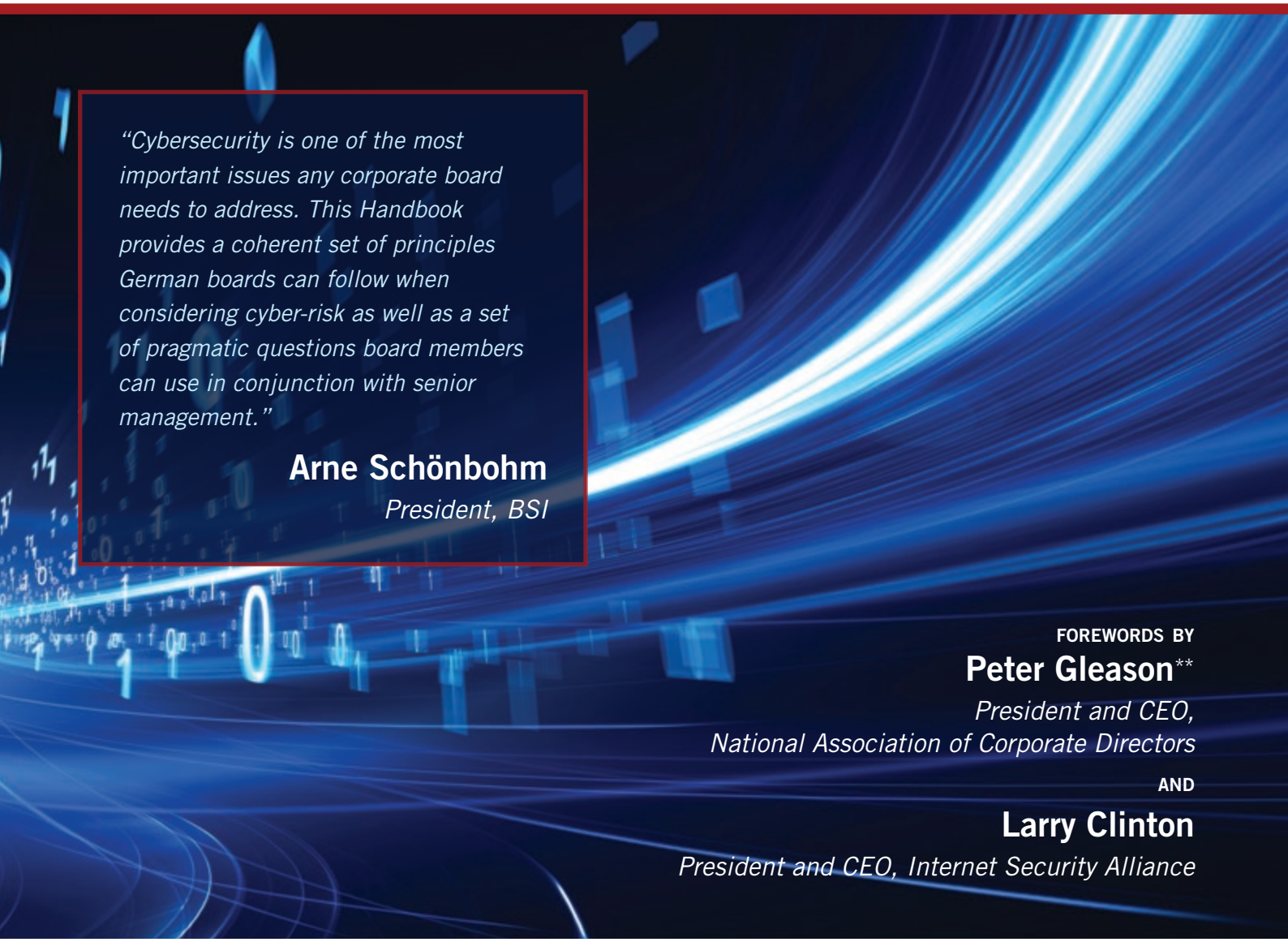
The Cyber Security Alliance is an affiliate of the Federal Office for Information Security

Managing Cyber Risk:

A Handbook for German Boards of Directors



"Cybersecurity is one of the most important issues any corporate board needs to address. This Handbook provides a coherent set of principles German boards can follow when considering cyber-risk as well as a set of pragmatic questions board members can use in conjunction with senior management."

Arne Schönbohm
President, BSI

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 German 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?

Cyberattacks is the fastest growing – and perhaps most dangerous – threat facing modern organizations. Boards of directors are increasingly focused on addressing these threats. However, due to the recency of the threat and its ever-changing nature, boards are seeking a coherent approach to deal with the issue at the 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 organization'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, teleconferences, 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 organizations 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 **Garin Pace***
AIG **Sebastian Hess**
AIG **Chloe Green**
AIG **Susanne Pauer**
AIG **Mark Camillo**
AIG **Richard Hebblethwaite**
AIG **Nepomuk Loesti**
AIG **Oliver Delvos**
RAYTHEON ANSCHÜTZ **GmbH Dirk Sann**
BUNGE **Angelo Micciche**
DLA PIPER **Christian Schoop**
DLA PIPER **Jan Pohle**
DLA PIPER **Jim Halpert**
DLA PIPER **Jan Spittka**
DLA PIPER **Dr. Andreas Meyer-Landrut**
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS **Peter Gleason**
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS **Erin Essenmacher**
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS **Robyn Bew**
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK **Arne Schönbohm**
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK **Roland Hartmann**
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK **Stefan Wunderlich**
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK **Till Kleinert**
CYBER SECURITY COUNCIL OF GERMANY **Philipp v. Saldern**
CYBER SECURITY COUNCIL OF GERMANY **Hans-Wilhelm Dünn**
CYBER SECURITY COUNCIL OF GERMANY **Florian Till Patzer**
FORMER HEAD OF NATO C&I AGENCY **Koen Gijsbers**
CONNECTING TRUST **Tom Koehler**
CYCLESEC GMBH **Sebastian Klipper**
SWISS REINSURANCE COMPANY LTD **Maya Bundt**
HATHAWAY GLOBAL STRATEGIES **Melissa Hathaway**
RICHARD KNOWLTON ASSOCIATES **Richard Knowlton**
GEC RISK ADVISORY **Andrea Bonime-Blanc**
AXIO **Scott Kannry**
BASF SE **Patrick Fiedler**
COMMERZBANK **Thoralf Reichelt**
DEUTOR CYBER SECURITY SOLUTIONS **Stefanie Frey**
DEUTOR CYBER SECURITY SOLUTIONS **Michael Bartsch**
DEUTSCHE BANK **Osama Jamaleddine**
KEYIDENTITY GMBH **Arved Graf von Stackelberg**
KÖBERICH FINANCIAL LINES GMBH & CO. KG **Harald Köberich**
MARSH **Göran Weinert**
MARSH **Ute Sauer**
MARSH GMBH **Michael Rieger-Goroncy**
VARD **Peter Dehnen**
FIS GLOBAL **Kara Hill**
CLEARSTREAM **Nancy Jansen**
ISABEL GROUP **Cedomir Karlicic**
DAIMLER **Sascha Kazmaier**
ANAPUR **Kruschitz Erwin**

Thanks and acknowledgments are given for the support and participation of all the organizations 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 that 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.

Additional thanks and acknowledgements are given to Sebastian Hess, AIG, for his linguistic expertise in translating this final deliverable from English to German.

Special thanks also go out to DLA Piper for their legal expertise.

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 US' oldest and largest non-profit education association serving the Supervisory Board Director 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 Supervisory Board Directors that have stood the test of time, even as the cyber-threat environment has continued to evolve.

NACD congratulates the ISA, AIG, 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 German 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

Foreword: 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 asset value has changed significantly, shifting away from the physical and toward the virtual. Close to 90 percent of the total value of the Fortune 500 now consists of intellectual property (IP) and other intangibles.[7] Along with the rapidly expanding "digitalization" of corporate assets, there has been a corresponding digitization of corporate risk. Accordingly, policy makers, regulators, shareholders, and the public are more attuned to corporate cybersecurity risks than ever before. Organizations are at risk from the loss of IP and trading algorithms, destroyed or altered data, declining public confidence, 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 arena for two reasons. First, the complexity of cyber threats has grown dramatically. Corporations now face increasingly sophisticated events that outstrip traditional defenses. As the complexity of these attacks increases, so does the risk they pose to corporations. The potential effects of a data breach are expanding well beyond information loss or disruption. Cyberattacks can have a severe impact on an organization'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 cyberattacks. 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 these aspects 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 organized according to these five key principles:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber 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 public companies, these principles are applicable to – and important for – all directors, including members of private-company and nonprofit boards. Every organization 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, cyberattacks were largely the province of hackers and a few highly sophisticated individuals. While problematic, many corporations could chalk up these events as simply a frustrating cost of doing business.

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

One of the defining characteristics of these attacks is that they can penetrate virtually all of a company's perimeter defense systems, such as firewalls or intrusion-detection systems. Intruders look at multiple avenues to exploit all layers of cybersecurity vulnerabilities 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 cybersecurity

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

program, equally balanced between 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 amount of interconnection among data systems, it is no longer adequate that organizations secure only "their" network. Vendors, suppliers, partners, customers, or any entity connected with the company electronically can become a potential point of vulnerability. 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 interconnection of traditional information systems with nontraditional equipment 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 cyberattackers, and thus the need for organizations to expand their thinking about cyber-risk defense. 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 cyberattack. While such attacks are technically possible and could have very serious consequences, the vast majority of incidents are economically motivated.[11] Cyberattackers 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, cyberattackers are employing tactics that encrypt an organization's data, effectively holding it hostage until they receive a payment – so-called "ransomware." Estimating the damage of cyberattacks is difficult, but some estimates put it at $400-500 billion or more annually, with a significant portion of costs

Cyber Threats by the Numbers

- Forty-eight percent of cyberbreaches result from criminal or malicious attacks.[i] Eighty percent of black hat hackers are affiliated with organized crime.[ii]
- Top methods of access by cybercriminals include using stolen access credentials and malware.iii Attacks on mobile devices and cyberextortion attacks are both on the rise.[iv]
- The median number of days an organization is compromised before discovering a cyberbreach is 146.[v] Fifty-three percent of cyberattacks are first identified by law enforcement or third parties, compared with 47 percent that are discovered internally.[vi]
- Forty-eight 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]
- Thirty-eight percent of IT organizations do not have a defined process for reviewing their cyberbreach 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.

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 cyberattacks.[14,15] In addition to being targets in their own right, smaller firms are often an attack pathway into larger organizations via customer, supplier, or joint-venture relationships, making vendor and partner management a critical function for all interconnected entities.

There is general consensus in the cybersecurity field that cyberattackers are well ahead of the corporations that must defend against them. Cyberattacks are relatively inexpensive yet highly profitable, and the resources and skills necessary to launch an attack are quite easy to acquire. It is no wonder that many observers believe cyber-risk defense tends to lag a generation behind the attackers. It is difficult to demonstrate return on investment (ROI) for cyberattack prevention, and successful law enforcement response to such attacks is virtually nonexistent. According to some estimates, less than 1 percent of cyberattackers are successfully prosecuted.[16]

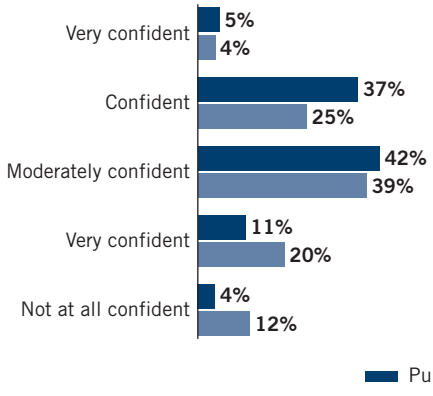
This does not mean that defense is impossible, but it does mean that board members need to ensure that management is fully engaged in making the organization's systems as resilient as economically feasible. This includes developing defense and holistic response plans, beyond organizational boundaries, that are capable of addressing sophisticated attack methods more efficiently.

Balancing cybersecurity with profitability

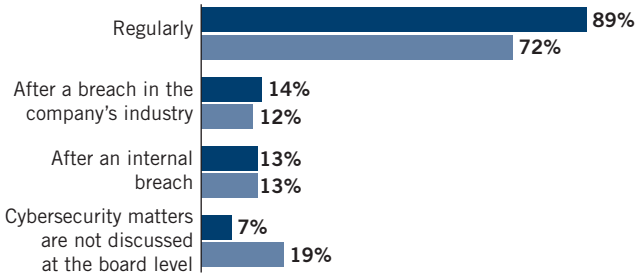
Like other critical risks organizations face, cybersecurity cannot be considered in a vacuum. Members of management and the board must strike the appropriate balance between protecting the security of an organization and mitigating downside losses, while continuing to ensure profitability and growth 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 cyberattack because they are relatively small in size, are not a well-known brand name, and/or do not 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 cybersecurity. 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 cybersecurity concerns if implemented haphazardly. Properly deployed, they could increase security, but only at a cost. Corporate boards need a broad strategy that includes digital operations to improve their oversight strategy.

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 required in order for a business to remain competitive. However, these practices can also dramatically weaken the cybersecurity of the organization.

It is possible for organizations 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 organization'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).[17]

The study showed that not only were these core cybersecurity practices effective, they also improved business efficiency and created an immediate positive return on investment, even before considering the positive economic impact of reducing cyberbreaches.[18]

But to be effective, cyber strategy must be more than simply reactive. Leading organizations also employ an affirmative, forward-looking posture that includes generating intelligence about the cyber-risk environment and anticipating where potential attackers might strike, as well as subjecting their own systems and processes to regular, rigorous testing to determine vulnerabilities.

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

[17] 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).

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

PRINCIPLE 1

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

Historically, corporations have categorized information security as a technical or operational issue to be handled by the information technology (IT) department. This misunderstanding is fed by siloed corporate structures that may leave functions and business units within the organization feeling disconnected from responsibility for the security of their own data. Instead, this critical responsibility is handed off to IT, a department that in most organizations is strapped for resources and budget authority. Furthermore, deferring responsibility to IT inhibits critical analysis and communication about security issues, and hampers the implementation of effective cybersecurity strategies.

With increased digitization, the value of data in a company grows. Safeguarding of data is increasingly fundamental for the business continuity of the enterprise. Therefore, cyber risks should be evaluated foremost within the context of the business, much in the same way an organization 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, operational, cross-departmental, and economic perspective.[19]

Cyber risk and the business ecosystem

While good cyber hygiene is vital to ward off many attacks the root cause of some of the highest-profile data breaches to date have had little to do with traditional hacking. For example, many studies indicate that disgruntled or poorly trained individuals who have approved access to the system are at the root of many compromises. Multiplying permitted access points via vendor relationships or even customer contact can multiply cyber risk. Product launches or production strategies that use complex supply chains spanning 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 interconnection the corporate network has with partners, suppliers, affiliates, and customers, which is likely dependent upon the size and complexity of the company. Several significant and well-known cyberbreaches did not actually start within the victim'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 8 reflect. Furthermore, an increasing number of organizations have some amount of data residing on external networks or in public "clouds," which they neither own nor operate and have little inherent ability to secure. These interdependencies can undermine the cybersecurity of the "home office." Many organizations also are interconnected with elements of the national and cross-national critical infrastructure, raising the prospect of cyber-insecurity at one company or institution becoming a matter of public security or even national security or extra-national or regional security.

As a result, directors – both Supervisory Board and Executive Board — should ensure that management is assessing cybersecurity not only as it relates to the organization's own networks, but also with regard to the larger ecosystem in which it operates. Progressive and proactive boards will engage management in a discussion of the varying levels or risk that exist in the company's ecosphere and take them into consideration as they calculate the appropriate cyber-risk posture and tolerance for their own corporation.[20] They should also understand what "crown jewels" the company most needs to protect, and ensure that management has an aligned protection strategy that builds from those high-value targets outward. The board should instruct management to consider not only the

Identifying the Company "Crown Jewels"

Supervisory Board Directors should engage the Executive Board and the Executive Board should in turn engage line management in a discussion of the following questions on a regular basis:

- What are our company's most critical data assets?
- 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?

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

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

highest-probability attacks and defenses, but also low-probability, high impact attacks that would be catastrophic.[21]

See **Appendix B** for a list of cybersecurity questions that Supervisory Board and Executive Board 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. **Appendix E** describes the differences among German board structures, e.g., Beirat, Aufsichtsrat, and Vorstand boards.

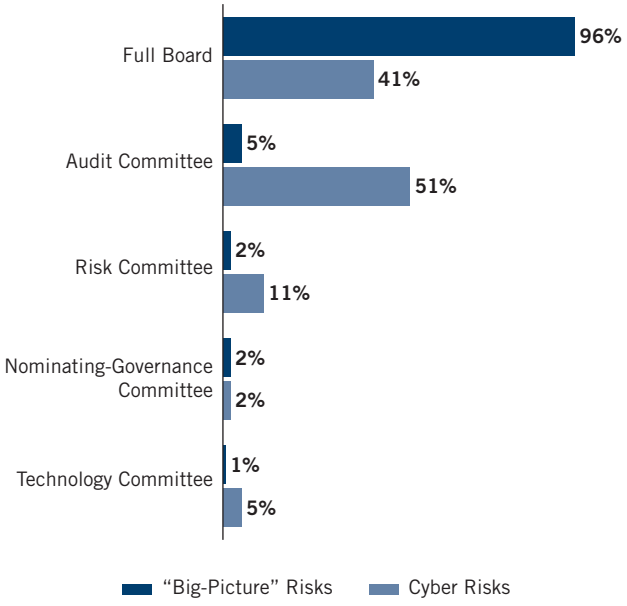
Cyber-risk oversight responsibility at the board level

How to organize the Supervisory Board to manage the oversight of cyber risk – and, more broadly, enterprise-level risk oversight – is a matter of considerable debate. Each company is organized differently, according to its unique business and regulatory environment. In Germany, certain types/sizes of businesses are mandated by regulation to establish and maintain boards of directors. While for others, it is a voluntary decision on whether a board is appropriate for the unique business structure. For those companies with Supervisory Boards Directors (whether mandated or voluntary), the size and structure of the board should be responsive to business risk. Determining whether the board has a management function or an advisory function is critical for deciding cyber-risk oversight responsibilities. For instance, Supervisory Boards have clear roles and competencies that position them to provide advice to the company.

The NACD Blue Ribbon Commission on Risk Governance recommended that risk oversight should be a function of the full board.[22] 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 or finance and risk committee (Figure 2), which also assumes significant responsibility for oversight of financial reporting and compliance risks.

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*

The new General Data Protection Regulation requires specific attention to data protection at the board level. The board needs to ensure that data protection and privacy is safeguarded and well organized. Data loss can lead to significant penalties (up to 4% of yearly worldwide turnover) and personal liability of board members.

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.). 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

[21] Ibid. See also: KPMG Audit Committee Institute, *Global Boardroom Insights: The Cyber Security Challenge*, Mar. 26, 2014.
[22] NACD, *Report of the Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward* (Washington, DC: NACD, 2009).

matters at least semiannually 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 at least quarterly.

To encourage knowledge-sharing and dialogue, some boards invite all directors to attend committee-level discussions 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. At this company 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.[23]

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. **Appendix H** contains sample board evaluation questions related to cybersecurity oversight.

[23] 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 frequently evolving. Boards should stay aware of current liability issues faced by their organizations – and, potentially, by directors on an individual or collective basis. German law currently poses external liability risk for board members not under data protection or cybersecurity law, but under general duty of care principles that may be enforced against Executive Board members by the company's Supervisory Board. For example, high-profile attacks may trigger Directors and Officers (D&O) liability claims accusing the board of mismanagement, waste of corporate assets, or neglecting their fiduciary duty by failing to take sufficient steps to confirm the adequacy of the company's protections against cyber attacks or data breaches. Exposures can vary considerably, depending on the company's or organization's sector and operating locations.

The business judgment rule (sec. 93 para. 1 sent. 2 of the German Sock Corporation Act) is likely to protect directors following a serious cybersecurity incident, provided that the board of directors reasonably oversaw the company's cybersecurity program based on adequate information. Maintaining records of boardroom discussions about the organization's cybersecurity program, cyber risks and risk management strategy; staying informed about industry-, region-, or sector-specific requirements that apply to the organization; and determining what to disclose in the wake of a cyberattack are all strongly recommended. It is also advisable for directors to participate in one or more cyberbreach simulations, or "table-top exercises," to gain exposure to the company's response procedures in the case of a serious incident.

Although many incidents of cyber-attacks against companies have become publicly known (e.g. the 2017 attacks by "Wannacry" and "Petya/NotPetya" or cases of CEO fraud) court judgments addressing D&O-liability in this context have not yet been rendered.

At the same time, directors should be briefed by their organization's Data Protection Officer (DPO), or if there is no DPO then by counsel, regarding how to structure the organization's cybersecurity program, including the implementation of a data governance strategy, monitoring of the organization's network and other IT infrastructure to prevent and detect attacks, in a way that complies with data protection and workers' rights.

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 organization's strategy, policies, and business activities. The record from the minutes should demonstrate that the Board's decisions balanced and prioritized risks facing the organization.

Public disclosures and reporting requirements

Companies and organization may be subject to a range of disclosure or compliance obligations related to cybersecurity risks and cyber incidents, including the following:

- GDPR and BDSG (German Federal Data Protection Act, Bundesdatenschutzgesetz) data breach notification requirements, and restrictions under data protection, data secrecy and labor laws that affect the organizations' cybersecurity program;
- NIS Directive and cybersecurity incident notification requirements and information sharing opportunities that enable the organization to learn about cybersecurity threats;
- Critical infrastructure providers[24] must disclose significant disruption to the availability, integrity, authenticity or confidentiality or an exceptional IT disruption to the German Federal Office for Information Security (BSI) under Sec. 8b(4) of the IT Security Act ("BSIG").
- Industry-specific regulations for the communications, financial services, energy and nuclear energy sectors all mandate disclosures of significant disruptions due to a cybersecurity event and or other significant IT disruption. (BSI may in turn notify other parties of the disruption if the report does not conflict with the interests of the disclosing party.)

[24] Critical infrastructure is organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences. Most commonly associated with the term are, for example, facilities for shelter, heating, agriculture, food production and distribution, water supply, transportation systems or public health.

- Other applicable country-specific laws, regulations and standards in other countries to which the organization is subject. These may include affirmative security requirements, different data protection restrictions, restrictions on deploying security technologies such encryption and data localization requirements, as well as on restrictions on "hacking back" against hackers.
- Although, there is no specific duty to inform the Public Prosecutor's Office, the involvement of the Public Prosecutor's Office in some cases can help to clarify the fact scenario and to collect evidence relevant for damage claims asserted by and against the company.

Challenges include overlapping and conflicting rules and requirements, lack of coordination among regulatory and legislative authorities, and different priorities driving the development of new regulations – including divergent views on fundamental issues such as the definition of personal data, different weight given to legitimate interests and employee rights. While directors do not need to have deep knowledge about this increasingly complex area of law, they should be briefed by inside or outside counsel on a regular basis about data governance and legal compliance requirements that apply to the company. Reports from management should enable the board to assess whether or not the organization is adequately addressing these potential legal risks.

Disclosures of cybersecurity risks in public filings and disclosures are not yet required, but may be in the future.

Directors should ask management to solicit external counsel's point of view on potential disclosure considerations related to forward-looking risk factors in general, and also in terms of the company's emergency and crisis plan for response to a major breach or other cyber incident.

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 counsel. Finally, directors should challenge management to build an integrated cyber risk management, combining legal risks, cyber threats and business impact perspectives in order to enhance their overall risk mitigation strategy.

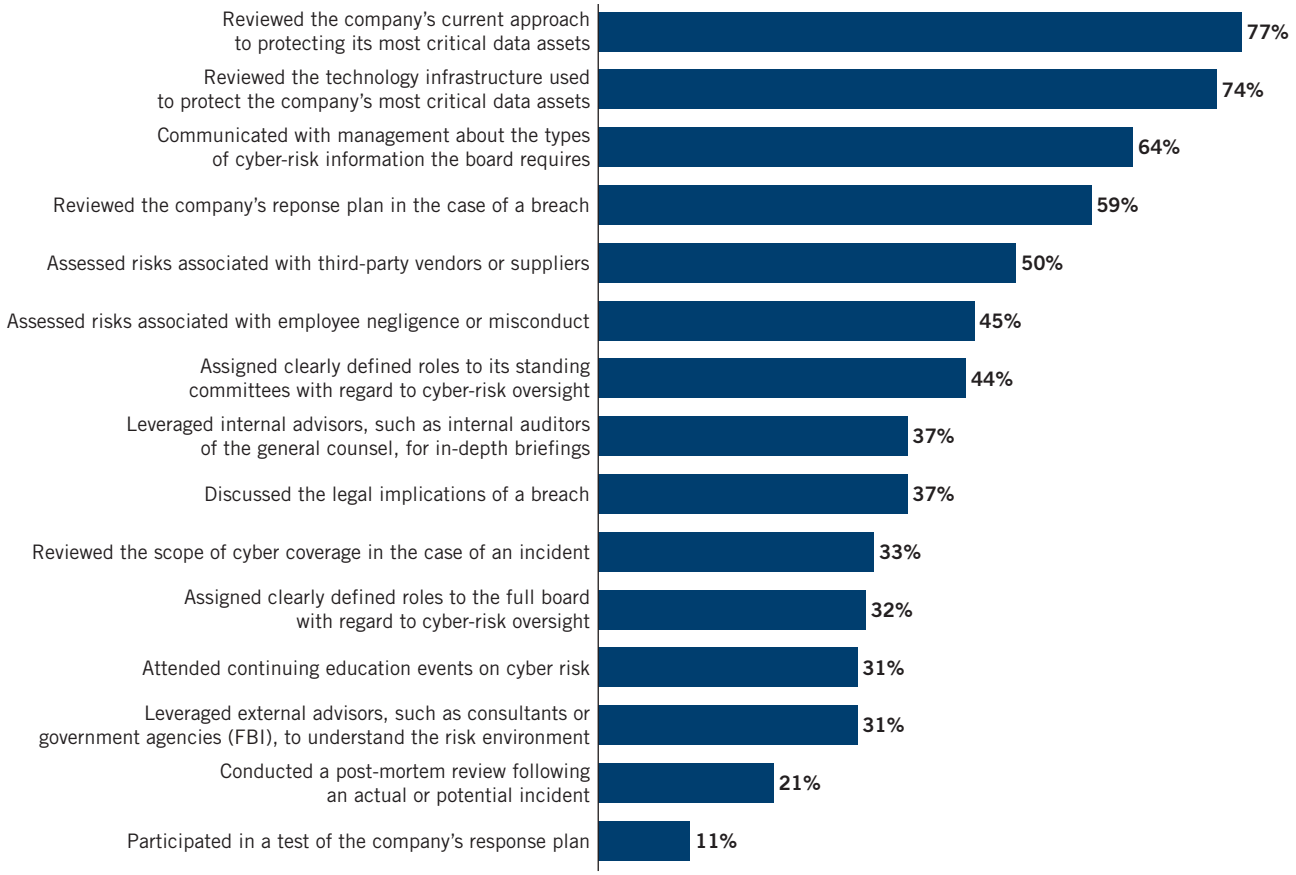
PRINCIPLE 3

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 its report "The State of IT Security in Germany 2017"[25], the German Federal Office for Information Security finds that the cyber risk situation is continuously tense and at a high level. The report illustrates how information security has become an essential precondition for the success of digitalization in Germany. In a recent survey of U.S. public-company directors, 89.1 percent of respondents reported their boards discuss cybersecurity "on a regular basis."[26] 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.[27] 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."[28] At a different peer-exchange session, another director suggested this useful analogy: "Cyber literacy can be considered similar to financial

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

[25] https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html

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

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

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

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."[29]

Improving access to cybersecurity expertise

As the cyber threat has grown, the responsibility (and expectations) of board members has grown also. Directors need to do more than simply understand 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, corporate transformation 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 organizations, there is no one-size-fits-all approach that will apply everywhere (see "A Cyberexpert 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.[30]

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 aligned with the corporate strategy and 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.

There are several ways boards can consider increasing their access to cybersecurity expertise. Cybersecurity is like washing hands in hospitals – everyone just has to do it. Organizations need to decide which approach works best for their strategic goals and business objectives, whether adding a cybersecurity expert to the board or increasing access to cybersecurity expertise. Bottom line, boards should avail themselves periodically to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.

Gaining access to adequate cybersecurity expertise

Most boards are increasingly expected to know more and more about key interconnected business risks. While they may have certain subject matter expertise derived from their previous careers, director should bring a broader view related to 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."

If an organization determines that it would be appropriate to add someone with cyber expertise – or increasing access and visibility to cyber expertise – to its board is in the company's best interest, they should request that nominating committees review the way someone is chosen for the board. They should look at skillsets, diversity, and quality of board members as a way to attempt to enhance cybersecurity expertise. Cyber risks are different than traditional or economic risks, something the prospective board member should understand. 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

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

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

that, for example, show weather trends and number of incidents that is used to predict potential future risk (traditional risks), as well as historical market behavior to help inform the impact of those risks and how they can be mitigated (economic risks). With cyber and security, 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, organizations cannot fully protect themselves in an interconnected world. Cyber adversaries, including nation-states, may have greater resources than even the biggest corporations, and the legal protections in the physical world far out-strip what is available in the cyber world, something the cyber oversight board member(s) should understand and consider for their cybersecurity program governance.

Boards can create a check-and-balance system by soliciting advice from multiple sources. For example, an organization 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 organization to challenge the functions and approaches, and see cyber risk from many perspectives, which helps lower the risk threshold.

Boards can also engage external consultants to act as "cyber coaches." This would be a resource that understands the cybersecurity issues and can approach them diplomatically across departments. This resource would have both cybersecurity and broad management expertise.

Enhancing management's reports to the board

A 2012 survey found that fewer than 40 percent of boards regularly received reports on privacy and cybersecurity risks, and 26 percent rarely or never received such information.[31] Since then, boardroom practices have changed dramatically: As noted on page 9, nearly 90 percent of public-company directors say their boards discuss cybersecurity issues on a regular basis and receive information from a range of management team members. Yet a significant number of directors believe their organizations 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.[32]

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 rote 'box ticking' in favor 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 fulfill 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 firsthand 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.

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

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

Respondents to recent survey of board members 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 organization) and externally (with industry peers);
- Insufficient transparency about performance; and
- Difficulty in interpreting the information.[33]

Cybersecurity and cyber-risk analysis are relatively new disciplines – certainly, much 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. They should set the expectation to implement a common taxonomy and make an attempt to make cyber risk part of the financial risk of the company, whether the risk is cost to fix damage of a successful attack, indirect cost as a result of not being able to operate, stolen assets, penalties as a result of non-compliance or loss of stock value as a result of damaged image. 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.[34]

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

[33] Ibid.

[34] 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

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

Technology integrates modern organizations, whether workers are across the hall or halfway around the world. But, as noted earlier, the reporting structures and decision-making processes at many companies are legacies of a siloed 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 understands this digital interdependency and is taking an enterprise-wide approach to cybersecurity assigns sufficient resources and authority.

Appendix F outlines the German government's cybersecurity resources available to the private sector to help inform directors' discussions with management about how the organization is utilizing such resources. Appendix G contains considerations for building a relationship with the CISO/IT-Sicherheitsbeauftragte.

EU standards

The EU has issued regulations and directives that are directly impacting cybersecurity risk practices in companies. Two of the regulations have an especially high impact on companies' business and practice.

- The General Data Protection Regulation (GDPR) becoming enforceable as of May 25, 2018, provides for a harmonization of data protection regulations throughout the EU. It extends the scope of the EU data protection law to all foreign companies processing data of EU residents.
- The Directive on security of network and information systems (NIS Directive) is enforcing cyber standards to companies that are part of Europe's and national critical infrastructures. Some of these regulations are or will be translated into German law before coming into effect. These rules are not just in effect for companies that have European ownership, but also to foreign companies that operate in Europe. This is also reciprocal for European companies operating for example in the USA or China. They have to follow local regulations as well.

BSI standards and IT-Grundschutz-Kataloge

With IT-Grundschutz, the German Federal Office for Information Security (BSI) provides a comprehensive framework that enables public authorities and companies to achieve an appropriate security level for all types of information of an organization. IT-Grundschutz uses a holistic approach to this process. Through proper application of well-proven technical, organizational, personnel, and infrastructural safeguards, organizations can attain a security level that is suitable and adequate to protect business-related information having normal protection requirements. In many areas, IT-Grundschutz even provides advice for IT systems and applications requiring a high level of protection. IT-Grundschutz is compatible to ISO/IEC 27001.

The corresponding BSI Standards contain recommendations on methods, processes, procedures, approaches and measures

Roles and Responsibilities of Key Management

While each organization will have a unique management structure with varying titles, roles, and responsibilities, it is imperative that boards clearly establish the roles and responsibilities of key senior management, especially when it comes to creating an integrated and cross-organization cyber-risk management team. For example, an organization could have the following structure and role definitions:

- 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 Information Officer – technical expertise
- Chief Privacy Officer – intimate knowledge of privacy laws, rules; policy development and enforcement; training and communications; privacy audits
- Datenschutzbeauftragter (Data Protection Officer) – legal person, as mandated by GDPR, looks at security through a legal and compliance lens.
- Chief Information Security Officer/ Informations Sicherheitsbeauftragter (IT Security Officer) – responsible for security of all information, not just the digitized data.
- Legal Counsel – Outside Legal Counsel – external legal assistance when needed; attorney client privilege; investigations; representation to government and regulatory authorities.

An Integrated Approach to Cyber Risk Governance

Competing effectively in the digital age may require rethinking of traditional business and governance structures. These modifications could generate tensions among staff who are comfortable with historic, if possibly outdated, mechanisms. Care must be taken to fully involve appropriate input from employees into any such modifications to engender buy in and support. Evolving business structures that take into account modern digital security can potentially enhance employee privacy and corporate productivity. One model being adapted by many companies is a cross departmental approach to expand input from across the spectrum of the organization and should help create a culture of cybersecurity for both the organization and its employees. Some steps in creating this enterprise-wide approach are:

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, chief operating officer, or similar person with broad authority, should lead the team.
2. Appoint a cross-organization cyber-risk management team. All substantial stakeholder departments must be represented, including business unit leaders, legal, and compliance, finance, Datenschutz, HR, IT, and risk management. (See "Roles and Responsibilities of Key Management" excerpt below). A key objective of such a cross-organizational effort is to ensure that there is no cybersecurity weak link or exception within the organization. Internal audit should be independent and not part of this team.
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, identification of high value data ("crown jewels") and processes, and regulatory compliance.
4. Assess the organization's current threat landscape and risk picture. Then, clearly establish its risk appetite. Identifying potential risk to the organization, as well as its risk threshold, will help the cyber-risk team assess which framework or standards (e.g., BSI IT-Grundschutz) aligns most appropriately with its mission and goals.
5. Be aware that cybersecurity regulation differs significantly across jurisdictions (among German federal states (Länder)), between other countries, from sector to sector, and from industry to industry). As noted in Principle 2, management should dedicate resources to tracking the standards and requirements that apply to the organization, especially as some countries aggressively expand the scope of government involvement into the cybersecurity arena.
6. Develop and adopt an organization-wide cyber-risk management and resiliency plan and internal communications strategy across all departments and business units. While cybersecurity obviously has a substantial IT 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 organization's needs and risk appetite. Resource decisions should take into account the severe shortage of experienced cybersecurity talents 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 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.
8. 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 Directors.

Source: Internet Security Alliance. 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).

relating to the various aspects of information security. The current versions of the BSI-Standards (200-1, 200-2 and 200-3) were published in October 2017 (see Appendix F for details). As a complement to the BSI Standards, the IT-Grundschutz-Kompendium describes specific requirements in the form of modules (IT-Grundschutz-Bausteine) covering different aspects of information security such as applications, industrial security or information security management systems.

Supervisory Board Directors should set the expectation that management has considered the BSI Standards in developing the company's cyber risk defense and response plans. By doing so, such directors ensure their organizations are creating a baseline for cybersecurity. Using the BSI Standards does not translate into absolute cybersecurity for a company, just as compliance with any framework or regulation does not equal absolute cybersecurity. Creating a cybersecurity baseline, however, helps organizations identify where their starting point for cybersecurity ought to be, how cybersecurity can benefit their unique business needs, and areas in need of improvement. Supervisory Board Directors need to understand that implementation of a framework is not a one-time activity – it requires continuous monitoring, assessments, and application of the standards in order to remain responsive to a changing threat environment.

PRINCIPLE 5

Board-management discussion about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or share 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 optimized. As with other areas of risk, an organization's cyber-risk tolerance must be consistent with its business strategy and objectives. Cybersecurity resource allocation is a function of balancing business goals with the inherent risks in digital systems (see "Defining Risk Appetite," page 24). 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 with its business impact and a plan for addressing it. Directors and management teams will need to grapple with the following questions:

- **What raw data assets and information, 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 organization is willing to accept as a practical business consideration. In this context, distinguishing between mission-critical assets (see "Identifying the Company's 'Crown Jewels,'" page 9) and other data or systems that are as important, but less essential, is a key first step. However, the compromising of raw data assets and information is not the only variation of cyber risk. Legal risks could exist that exceed the actual value of data losses, 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 defenses?** When considering how to address more sophisticated threats, management should place the greatest focus on sophisticated defenses – both technical and organizational--designed to protect the company's most critical data and systems. While most organizations would agree with this in principle, in reality, many apply security measures equally to all data and system 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, organizations should consider accepting a greater level of cybersecurity risk than higher-priority assets, or choosing instead to transfer the impact of such risks via insurance as the costs of defense will likely exceed the benefits.[35] Boards should encourage management to frame the company's cybersecurity risks and investments in economic terms of Return on Investment, and to reassess it 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?** Organizations of all industries and sizes have access to end-to-end solutions that can assist in lessening 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 consultative cybersecurity services. Beyond coverage for financial loss, these tools can help to mitigate an organization's risk of suffering from property damage and bodily injury resulting from a cyberbreach. Some solutions also include access to proactive tools to add another layer of protection and expertise. The inclusion of these value-added services proves even further the importance of moving cybersecurity governance 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 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).[36]

- 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,

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

[36] Examples of analytical tool include those from Secure System Innovations Corp and X-Analytics, and the FAIR Institute, to name a few. Also, in AIG's December 12, 2017 Executive Summary Report, AIG references their patented method for measuring and modeling cyber risk in economic terms, which they use in the underwriting process.

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 organization to choose a carrier that best fits the organization's needs, whether that is a carrier with a breadth of global experience or the small insurance company from their localized region. 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. If a company shares information with its insurance provider, they can work together to find a cost-effective program to manage cyber risk. Many insurers, in partnership with technology companies, law firms, public relations companies and others, also offer access to the preventative and emergency response measures discussed above. Cyber risk can also be transferred through outsourcing options; sourcing contracts should have clear language about risk mitigation and acceptance by the technology partner, as well as penalties for breaches 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, including unforeseen risks that management has not planned for. In an interconnected world, there may be cyber risks to the organization that exist outside the organization'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 organizational strategies for cyber-risk management that include operational IT management; strategies on legal agreements with partners and vendors assuring appropriate cybersecurity; and breach communication plans to address reputational risk when an event occurs.

Defining Risk Tolerance

"Risk tolerance is the amount of risk an organization 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 behavior by setting the boundaries for running the business and capitalizing on opportunities.

"A discussion of risk tolerance 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 tolerance is a matter of judgment 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 organization's operating 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 fact of these threats, and despite dramatic increases in private-sector cybersecurity spending,[37] the economics of cybersecurity still favor attackers. Moreover, many business innovations come with increased vulnerability, and risk management in general – IT- and cyber-related security measures in particular – has traditionally been considered to be a cost center in most for-profit institutions.

Directors need to continuously assess their competence maturity and 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."[38] The board's role is to bring its judgment 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.

[37] 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.

[38] 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 organization on a strategic level.

1. Does the CEO encourage open access between and among the board, external sources, and management about emerging cyber threats?
2. Do we discuss cyber risk within the board meetings on a regular basis? Do we receive metrics that show where we stand with respect to cyber resilience and the threat?
3. What do we consider our most valuable business assets? How do our IT systems interact with those assets?
4. Do we think there is adequate protection in place if someone wanted to get at or damage our corporate "crown jewels"? What would it take to feel confident that those assets were protected?
5. Are we considering the cybersecurity aspects of our major business decisions, such as M&A, partnerships, new product launches, etc.?
6. Are we spending wisely on cybersecurity tools and training? Do we know if our spending is cost effective?
7. Who is managing our cybersecurity? To whom is cybersecurity reporting? Is there enough checks and balance? Do we have the right talent and clear lines of communication/accountability/responsibility for cybersecurity? Do I know the person at my company who is responsible for cybersecurity (IT Sicherheitsbeauftragte, CISO)?
8. Is cyber included in our risk register?[39]
9. Have we considered how we would manage our communications in the case of an event, including communicating with the public, our clients, our shareholders, our regulators, our rating agencies? Do we have communication strategies for each of these audiences? And what about a cyber crisis? Are we trained and ready?
10. Does our organization participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organizations? Should we?
11. Is the organization adequately monitoring current and future cybersecurity-related legislation and regulation?[40]
12. Does the company have adequate insurance, for example Cyber Insurance Directors and Officers insurance (Organhaftpflicht), that covers cyber events? What exactly is covered, and to what maximum amount?[41] Are there benefits beyond risk transfer to carrying cyber insurance?[42]
13. Do we have enough cyber experts in our staff? Are we doing enough to promote cybersecurity workforce development?

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

RETURN TO TABLE OF CONTENTS

APPENDIX B

Questions a board may ask management about cybersecurity

Situational awareness

1. Do we as a board know where we stand in terms of cybersecurity situational awareness? Were we informed of cyberattacks that have already occurred and how severe they were? Did we notice those incidents?
2. What are the company's cybersecurity risks, and how is the company managing these risks?[43] What are our mitigation strategies?
3. Have we identified our most critical digital assets – our digital "crown jewels"? Do we have adequate situational awareness of the threats to these assets?
4. How will we know if we have been hacked or breached, and what makes us certain we will find out?
5. Who are our likely adversaries?[44] Which of those adversaries have the actual capabilities to harm me?
6. In management's opinion, what is the most serious vulnerability related to cybersecurity (including within our IT systems, personnel, or processes)? What additional vulnerabilities exist?
7. If an adversary wanted to inflict the most damage on our company, how would they go about it? Have we run through different scenarios, such as a minimum/maximum damage attack or a system shutdown? Where would it hurt us most?
    a. Ask management for specific business scenarios. This should include multiple parts:
    i. IT response.
    ii. Business strategies to address the incident after the IT department has responded to the incident.
8. Has the company assessed the potential risks for human error?[45]
9. How are we having our security system tested for vulnerabilities? When was the last time we conducted these independent and external assessments? What were the key findings, and how are we addressing them? What is our maturity level?
10. 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?
11. Have we considered obtaining an independent, third-party assessment of our cybersecurity risk management program?

Strategy and operations

1. What are the leading practices for cybersecurity, and where do our practices differ?
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?
4. Do we have a systematic framework, such as the ISO 27000 or the BSI Framework, in place to address cybersecurity and to assure adequate cybersecurity hygiene?
5. If you had an additional XXX dollars, where would you spend those additional financial resources?
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. Does the company have cyber insurance? If so, is it adequate?
8. Is there an ongoing, company-wide awareness and training program established around cybersecurity?
9. Is our security team involved with the strategic decisions to adopt new emerging technologies? How is security integrated into business processes and products and design and life cycle? Are we aware of the potential risks and opportunities for our company in new technologies?
10. How are we addressing the security vulnerabilities presented by an increasingly mobile workforce?

Human error

1. How could employees, through accidental human error, become unintentional threats when operating with the best of intentions?
2. What are the leading practices for combating human errors, and how do ours differ?

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

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

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

After a Cybersecurity Incident

1. How did we learn about the incident? Were we notified by an outside agency, or was the incident discovered internally?
2. Could information sharing with our partners have prevented the incident; why did it not help us prepare our defences better?
3. What do we believe was stolen, copied, modified or altered?
4. How has our organization, or others, been affected by the incident?
5. What can we do to mitigate any losses caused by the incident?
6. Do we have a notification insurance?
7. Have any of our operations including through partnerships or other relationships been compromised?
8. Is our cyber-incident response plan in action, and is it working as planned?
9. What is the response team doing to ensure that the incident is under control and that the hacker no longer has access to our internal network?
10. Do we believe the hacker was an internal or an external actor; could the hacker have been given help from within?
11. What were the weaknesses in our system that allowed the incident to occur (and why)?
12. What steps can we take to make sure this type of event does not happen again? What are the lessons learned from this incident? What is our policy for sharing incident-related information, both internally and externally?

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

3. How do key functions (IT, HR, Data Privacy Officer, Legal, Compliance, and Executive Management) 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 be required for 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 recognize threats.
   d. Consultation with Workers Counsels and how to best apply security measures.
4. How have we adapted our personnel policies, such as new employee orientation, training related to department/role changes, employee exits, and the like, to incorporate cybersecurity? Do we have personnel access restrictions in place based on roles and responsibilities?
5. How do our operational controls, including access restrictions, encryption, data backups, monitoring of network traffic, etc., help protect against accidental human error?

Supply-chain/third-party risks

1. Do we currently have an inventory of our suppliers and third-party servicers, and a process to keep the list up to date? How do we organize our list of those that supply to us? Do we prioritize our security based on the potential risk exposure of the supplier, size and relationship to our most valuable data?
2. Do we have a management system in place to fully include cybersecurity in our supply-chain risk management?
3. How much visibility do we currently have across our supply chain regarding cyber-risk exposure and controls? Which departments/business units are involved?
4. How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks?
   a. Are we adequately indemnified against security incidents on the part of our suppliers/vendors?
   b. Can we make cyber insurance mandatory for a supplier?
5. How are cybersecurity requirements built into contracts and service-level agreements? How are they monitored, and are we doing our due diligence to enforce contracts? Contracts and service-level agreements can be written to include requirements for the following:
   a. Written cybersecurity policies; regulatory compliance (e.g., GDPR, NIS).
   b. Personnel policies, such as background checks, training, etc.
   c. Access controls.

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

d. Encryption, backup, and recovery policies.
e. Secondary access to data.
f. Countries where data will be stored.
g. Notification of data breaches or other cyber incidents.
h. Incident-response plans.
i. Audits of cybersecurity practices and/or regular certifications of compliance.

6. How difficult/costly will it be to establish and maintain a viable cyber-vulnerability and penetration-testing system for our supply chain?
7. Do our vendor agreements bring new legal risks or generate additional compliance requirements? Have we considered all applicable laws, such as industry- or sector-specific laws and regulations?
8. How are we managing the data privacy laws when transferring data from Europe to another country?

Incident response

1. What is our ability to detect incidents?
2. How fast can we respond to an incident?
3. Whom must we notify and when? What are the timetables for reporting incidents to consumers? Regulators? Vendors/partners? Internally? Peers? How do we contact those who we must notify?
4. How will cybersecurity incidents be disclosed to investors and what criteria will be used for these disclosures?
5. What is our policy for reporting incidents to the board, and at what point should the board be informed of an incident?
6. Under what circumstances will law enforcement and other relevant government entities be notified?[46]

Contacting External Parties

In addition to external counsel, boards and management teams should consider whether to notify the following:

- Independent forensic investigators.
- The company's insurance provider.
- The company's external audit firm.
- Crisis communications advisors.
- Law enforcement agencies.
- Public authorities (e.g. Federal Office for Information Security).
- Computer Emergency Response Team (CERT).

Adapted from Jody Westby's post on Forbes.com, "Don't Be a Cyber Target: A Primer for Boards and Senior Management," Jan. 20, 2014

7. How will management respond to a cyberattack?[47] Are we adequately exercising our cyber-preparedness and response plans?
8. Have we trained/tested the crisis management plan?
9. What is our communication and PR strategy for a cyber-induced crisis?
10. What are we doing to avoid making the problem worse for our organization? Are we talking to counsel for advice? Is our legal team prepared to receive such notifications?

APPENDIX C

Cybersecurity considerations during mergers and acquisition phases

Companies that are acquiring or merging with other companies are also acquiring the target company's cyber risk posture. As such, the acquiring company must conduct as much due diligence as is practical before the deal is closed and be prepared to mitigate those risks after closure. Similarly, the acquired company will face new cyber risks based on the perception, right or wrong, that the smaller company would represent an easy way to gain access to the larger company. Regardless of which side of the transaction you are on, as a Director you have responsibility to ensure management recognizes the risks and acts accordingly. Failure to address cyber risks during the acquisition process, poses real risk to the deal's value and return on investment.

Short-term risks

- Breaches of law firms or financial institutions involved in the transaction could reveal information, such as valuations or negotiating positions that would derail the transaction.
- Premature open source discussion of the transaction period might trigger threat actors to attempt to gain entry to the target's network as a means of getting to the acquirer's network.
- Failure to disclose warranty claims, ongoing breaches or the intellectual property losses of previous breaches could distort the deal's valuation.
- Potential Impact from current employees for real or rumored consequences of the M&A activity.

Long-term risks

- Regulatory or legal actions that result from circumstances not discovered during due diligence could put the deal's return on investment at risk. The loss of customers, reputational damage and associated hits to sales and profit, resulting from circumstances not discovered during due diligence could also reduce the return on investment.
- Similarly, failure to properly integrate the merged entities' systems into a sustainably secure structure could result in a breach that will reflect on both companies and possibly lead to loss of market share to competitors without a known data breach.

Directors should ensure management engages their cybersecurity leadership 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, 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.

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.

Boards need to be aware of the dangers surrounding the potential merger and become comfortable that management is performing its due diligence. This would include modeling the financial impact of a target company's 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 reevaluate the deal strategy. If the team elects to continue forward despite risks identified in this phase, those risks should be evaluated much more thoroughly during due diligence discussions with the target. Management can perform the following analysis even before direct engagement with the target company begins:

- Has management gained 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?
- Has management considered conducting open source searches about the target, their systems, data, and intellectual property? This may help identify whether the company is already on hackers' radar, if systems or credentials are already compromised, or if there is sensitive data for sale or being solicited.
- Has management researched malware infections in the target company and holes in their defenses visible from the outside? This information is publicly available, or can be acquired through a service, 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.

Due diligence and deal execution phases

During these phases, the company should evaluate the target's cyber risk posture as part of their discussions with the target's management. Those conducting the evaluation should bear in mind that those with the most knowledge of the target's cyber posture may not be among the limited number of the target company's employees aware of the proposed sale. As such the Board must understand that all cyber issues may not be uncovered prior to closing. Nevertheless, significant problems identified in this phase might call for negotiation of a reduction in purchase price to cover costs of necessary remediation or setting aside funds to remediate deficiencies after closing. 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, data protection measures, as well as deficiencies in staff resources, policies, etc.
- Identify lax cultural attitudes toward cyber risk or privacy.
- 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 cyberattack 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

The post-deal integration period a high risk to both parties to the transaction. In general, any acquisition faces a range of challenges related to merging people, processes, systems, and culture. Cyber risks add yet another dimension of complexity and risk to this phase of the transaction. With the transaction now public, hackers will attempt to take advantage of the inconsistencies that exist between the platforms and technology operations of the parent company and the newly-merged or acquired entity. This is also the period where new cyber risks may surface as the parent company's cyber leadership is able to engage with all of the target's employees to gain a more thorough understanding of the target's cyber posture. Finally, during this period inconsistencies in the privacy policies and agreements in the two companies must be harmonized.

With this period of risk in mind, the Board should ensure management has made the strategic choice to fully integrate the acquired company into the parent's IT infrastructure or to leave the target as a stand-alone entity. This fundamental decision determines the cyber strategy. If the choice is to integrate, then the Board should assess the proposed integration time-line and ensure funding for cyber remediation is not diverted. If the choice is to leave the target as a stand-alone entity, the Board must ensure management invests enough in the target to bring it in line with the parent company's technical capabilities and risk tolerance. With this choice, it is also critical to ensure that the parent company's cybersecurity official maintains governance oversight of the acquired entity. With either choice, speed is critical to reduce the period of cyber risk.

This is also the period where the Board of the target company must ensure their management is aware of the increased likelihood that hackers will target their employees.

The end result of the integration phase must be a cyber risk posture where the acquired company does not increase the risk to the parent company and the privacy controls are consistent.

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, especially if that entity remains a stand-alone organization. This can be done by benchmarking

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.

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 cyberattack during the transaction process itself and should vigilantly 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 organization, the cybersecurity function collects and analyzes 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 organization'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 organization'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 organization'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").

Guiding Principles for Board-Level Metrics

- Ensure relevance to the audience (full-board; key committee).
- Make it 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.
- Be concise: Avoid information overload.
- Above all, enable discussion and dialogue.

Source: NACD

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 organization 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 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 organization'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 organization'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 organization experienced in the last reporting period? This 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

RETURN TO TABLE OF CONTENTS

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 team? 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.
8. What metrics do we use to evaluate cybersecurity awareness across the organization? 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.

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 activities 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

Understanding German board structures – Aufsichtsrat / Vorstand

As indicated at the outset, this handbook is based on work published in the U.S. by the National Association of Corporate Directors, which have been shown to be effective in independent global research. However, German boards have a somewhat different structure than some other countries. While these structures will be well-known to German companies, since many organizations operate in multiple environments, it is useful to briefly outline some of the unique characteristics of German boards in this document. While the structures of boards may differ, the core principles of cyber risk management and best practices for implementing these principles should remain effective, regardless of the corporate structural differences.

The two main concepts that need further attention are *Aufsichtsrat* (Board of Non-Executive Directors) and *Vorstand* (Executive Committee). Depending on the size, structure, and nature of the business, a business is required to have an *Aufsichtsrat* and / or *Vorstand*.

Aufsichtsrat:

The role of the *Aufsichtsrat* is purely one of advising and checking the actions of the *Vorstand* by engaging in oversight. The *Aufsichtsrat* has no executive power at all. The establishment of an *Aufsichtsrat* is mandatory for *Kapitalgesellschaften* (incorporated / Public Corporation / joint-stock company) and some other organizations (e.g. Genossenschaft (cooperative associations). The legal foundation is anchored with the German Stock Law (Aktiengesetz). The size and structure (e.g. the requirement to have representatives of the employees integrated) of a given *Aufsichtsrat* varies greatly between the different kinds of businesses and organizations. A detailed analysis of the requirements when it comes to an *Aufsichtsrat* is outside of the scope of this handbook.

The main task of the *Aufsichtsrat* is to act as a controlling body toward the *Vorstand*. It is the main task of the *Aufsichtsrat* to verify the actions of the *Vorstand*, which, among other tasks, at a minimum, requires the validation of the annual reporting. This also includes that the *Vorstand* might be required to have certain actions or decisions approved by the *Aufsichtsrat*. In other words, the *Aufsichtsrat* represents the whole *Gesellschaft* (Enterprise) toward the *Vorstand*, which includes the selection and appointment of the members of the *Vorstand*.

The detailed roles and responsibilities of a given *Aufsichtsrat* are defined in its *Satzung (bylaws / statue).*

Vorstand:

The *Vorstand* is the executive body of a business that represents the company externally in a legal capacity, but also internally by directing the actions of the business. The *Satzung* (bylaws) of the company define the roles and responsibilities of the *Vorstand* as a body, but also the roles and areas of responsibility of the individual members. A member of the *Vorstand* can be a shareholder of the company, but is prohibited from belonging to the *Aufsichtsrat*. The *Vorstand* is empowered to act independently. While the accountability for the business always resides with the *Vorstand*, certain responsibilities can be delegated throughout the business. The members of the *Vorstand* are personally liable for culpable actions of the *Vorstand*.

This setup allows for a clear handling of all aspects of cybersecurity within a business. Within the *Aufsichtsrat* it will be key to understand and validate the risk appetite toward cybersecurity risks. Additionally, the *Aufsichtsrat* needs to be able to understand the content and prioritization of internal and external cybersecurity audits, to determine if the risks to the enterprise are mitigated in an appropriate fashion. Since it is unlikely that the whole *Aufsichtsrat* will be able to become knowledgeable on the topic, it may suffice that one member, or group of members, be selected (or appointed) to be the subject matter experts on cyber risks. Whereas in the past such a general recommendation would have been questionable, in today's business world, especially considering how businesses operate and are more and more dependent on information technology and value generation through digitization (aka Industry 4.0), such a general recommendation ought to be considered.

Within the *Vorstand*, cybersecurity needs to be addressed slightly differently. First, it is key to understand that the accountability for all matters regarding cybersecurity, data privacy, and compliance are with the *Vorstand*. Using the same rational for the *Aufsichtsrat*, it is key to identify (at least) one subject matter expert on all matters cyber, as a responsible person / cyber sponsor within the *Vorstand*. The best suited person within the *Vorstand* is heavily dependent on the nature of the business, but in lieu of existing, sufficient capabilities within the existing members of the *Vorstand*, companies ought to seriously consider the option of creating the position of a Chief (Information) Security Officer, and making that position part of the *Vorstand*.

RETURN TO TABLE OF CONTENTS

APPENDIX F

German government resources

The Internet Security Alliance strongly recommends that companies do not wait until after they have experienced a cyberbreach or other cyber event to contact government agencies. All organizations can benefit from proactively establishing relationships with authorities on the federal or state level. In this Appendix, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), the national cybersecurity authority in Germany, gives an overview over relevant resources available for the business community.

BSI as single point of contact for cybersecurity

The German Federal Office for Information Security (BSI) as the national cybersecurity authority shapes information security in digitalisation through prevention, detection and reaction for government, business and society.

The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions. To help minimise or avoid these risks, the BSI offers services in the core areas of information, consulting, development and certification to a variety of target groups, including manufacturers, distributors and users of information technology.

The functions and competences of the BSI are regulated by the Bill on IT Security (IT-Sicherheitsgesetz) and include the following activities:

- The BSI, as the central point of contact for reporting security incidents, collects and evaluates information about security vulnerabilities and new attack patterns. These are used to create reliable reports on the current IT security situation, to enable the early detection of attacks, and to inform countermeasures.
- The BSI, after informing the manufacturers, may communicate information and alerts regarding vulnerabilities in IT products or services to authorities or the public.
- The BSI is the central point of contact for reporting security incidents regarding Critical Infrastructures.

Frameworks/standards

With **IT-Grundschutz** BSI provides a proven methodology for improving the level of information security in public authorities and companies of any size. IT-Grundschutz is compatible to ISO/IEC 27001. It consists of the BSI Standards 200-x and the IT-Grundschutz-Kompendium:

- 200-1: Information Security Management Systems (ISMS)
- 200-2: IT-Grundschutz methodology
- 200-3: Risk Analysis based on IT-Grundschutz
- 100-4: Business Continuity Management
- IT-Grundschutz-Kompendium: Describes specific requirements in the form of modules (IT-Grundschutz-Bausteine) covering different aspects of information security to help with the implementation of the IT-Grundschutz methodology. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
- The **IT-Grundschutz Profiles** provide templates which allow users to set up a security process based on IT-Grundschutz with the help of sample scenarios which can be adapted to the specific security requirements of their organisation.
- The **Cloud Computing Compliance Controls Catalogue (C5)** is intended primarily for professional cloud service providers, their auditors and customers of the cloud service providers. It is defined which requirements (also referred to as controls in this context) the cloud providers have to comply with or which minimum requirements the cloud providers should be obliged to meet. https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html

Networks

- Via the initiative **Alliance for Cyber Security (ACS)**, the BSI supports businesses in Germany with the planning and implementation of appropriate technical as well as organizational measures to increase their level of cybersecurity. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html
- **UP KRITIS** is a public-private partnership between operators of Critical Infrastructures (KRITIS), their associations and the relevant public authorities. The joint goal is to improve the protection of critical infrastructure across sectors. https://www.kritis.bund.de/SubSites/Kritis/EN/Home/home_node.html

Information sharing

- **CERT-Bund** (Computer Emergency Response Team for federal agencies) is the central point of contact for preventive and reactive measures regarding security-related computer incidents. CERT-Bund collaborates closely with the more than 40 CERTs organised in the CERT-Verbund as well as with the EU CSIRTs Network, which was created in the context of the NIS Directive. https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund_node.html
- The goals of the BSI's **IT Situation Centre** are to always have a reliable picture of the current IT security situation in Germany, and to assess the need for action and possible mitigation steps against IT security incidents at state level and within the private sector in a quick and competent way. https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/IT-Situation-Centre/itsituationcentre_node.html

Information security consulting

- The BSI offers consulting for developing appropriate solutions regarding questions of information security, balancing individual security requirements with economic considerations. BSI consulting services are available to public authorities and enterprises.
- Contact:
  Phone: 0228 99 9582-333
  E-Mail: Sicherheitsberatung@bsi.bund.de

Cyber-incident reporting

Notification requirement for operators of critical infrastructures

- Critical infrastructure providers must disclose significant disruption to the availability, integrity, authenticity or confidentiality or an exceptional IT disruption to the German Federal Office for Information Security. This requirement currently applies to the sectors Energy, Information Technology & Telecommunication, Water, Food, Finance & Insurance, Health, and Transport & Traffic.
- Companies that need to fulfill this requirement will receive information on how to report incidents via their Single Point of Contact.
- Operators of critical infrastructures that do not fall under the IT Security Act can report exceptional IT disruptions on a voluntary basis using the incident reporting process on the Alliance for Cyber Security website. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/meldestelle.html

Incident reporting via Alliance for Cyber Security

- Companies wishing to contribute to the BSI's IT security situation reports can report IT security incidents via the Alliance for Cyber Security website. The reports can be submitted anonymously, and all submitted information will be handled confidentially. Insights derived from those reports will be used for the creation of situation reports and alerts for the various target audiences of the BSI. Reported vulnerabilities in IT products will also be forwarded to the manufacturer using the "responsible disclosure" model.
- Online form: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/meldestelle.html
- Reporting via e-mail: Meldestelle@bsi.bund.de

What to report

- New methods of attack
- Corporate espionage attacks
- Attacks against process control systems
- Attacks against security infrastruktures
- New vulnerabilities
- Data breaches which may enable large-scale or targeted attacks (e.g. disclosure of critical passwords, code signing certificates)

Contacting police authorities (Zentrale Ansprechstellen Cybercrime, ZAC)

- Companies should also consider reporting cyber attacks to law enforcement agencies. In case of a successful attack against company assets, they should whether it is possibBitte prüfen Sie bei Angriffen und Schäden in Ihrem Unternehmen daher aktiv, ob die Erstattung einer Anzeige möglich ist.
- Contact information for central contact points for cybercrime (Zentrale Ansprechstellen Cybercrime) on state or federal level: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/ZAC/polizeikontakt.html

APPENDIX G

Building a relationship with the CISO/IT-Sicherheitsbeauftragte

Not long ago, 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 single accountable individual responsible for cybersecurity. This individual is increasingly given the title of chief information security officer (CISO) as a reflection of the importance of the function.[48] Another survey found that organizations with a single individual in place were more likely to have dedicated incident-response teams and plans in place, and were more confident about the strength of their company's defenses against threats such as malware.[49]

As corporate information-security functions become more mature, a new question has arisen: How can the board effectively communicate with the security executive? The individual occupying that position is responsible for managing vast amounts of operational, reputational, and monetary risks, so a relationship of trust with the board is essential.

At NACD's inaugural global Cyber Summit in 2015, more than 200 directors from Fortune Global 500 companies and cybersecurity experts discussed the evolving role of the security official, including the potential for this individual to serve as a critical source of information and insight for the board. As one director observed, "A strong cybersecurity program allows our business to compete and flourish. A security leader with the right skills can be a tremendous asset, including as an informed set of eyes and ears for directors. Yet, at too many companies they are still viewed as tactical support for the CIO."[50]

Many board members now seek to establish an ongoing relationship with the security executive, and include him or her in discussions about cybersecurity matters at full-board and/or key-committee-level meetings.

The questions and guidelines below can assist directors in establishing or enhancing a relationship with the cybersecurity executive. They also can help board members improve their communications with the executive and – more broadly – they can 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 IT Security Official's role and mandate.

- What is the official's charter and scope of authority in terms of resources, decisions rights, budget, staffing, and access to information and company personnel, including the Board (see Appendix E on German board structures)? How does this compare to leading practice in our industry and generally?[51] A key question to ask yourself would be whether or not you can understand the entire cybersecurity posture of the company by talking to a single individual. If not, then your security official's scope is too narrow.
- What is the security official's organizational relationship to the Data Protection Officer and other executives responsible for privacy?
- Is the company structured to provide visibility into the overall cybersecurity posture, including the budget, e.g. through dashboards? The answer to that question should lead to a discussion of how the company's cybersecurity budget is determined? Comparing this figure with industry spending trends is probably the best way to understand the adequacy of funding. What is its size (e.g., percentage of total IT spending), and how does this figure compare with leading practice in our industry and generally? What role does the security official play in cybersecurity budget allocation and investment decisions? And perhaps, most revealing, is the question of which security tools or other investments were below the "cut" line in the budget?

[48] 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.

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

[50] Quotation is from a participant in the Global Cyber Summit, held Apr. 15-16, 2015, in Washington, DC. Discussions were conducted under the Chatham House Rule.

[51] 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).

- What is the official's administrative reporting relationship (e.g., CIO, CTO, COO, CRO, head of corporate security, the Board, other)? Does it differ from the functional reporting relationship? If not, what protocols are in place to ensure the official has an independent channel to escalate issues and to provide prompt and full disclosure of cybersecurity deficiencies?[52]
- What role does the official play in the organization's enterprise risk management structure and associated processes?
- What role, if any, does the official play beyond setting and enforcing cybersecurity policies and related control systems?
  - For example, does the official 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?

2. Spend time with the security team before an incident occurs.

- A crisis is the wrong time for directors to get acquainted with the security official and key staff. Board members can arrange to visit the security team and receive orientations firsthand 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 the volumes of confidential information board members receive in the course of their service.
- Many security teams routinely produce internal reports for management and senior leadership on cyberattack trends and incidents. Directors can discuss with the CISO, corporate secretary, and board leaders whether this information might be relevant and useful to include in board materials.

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

Inside the organization

- How does the security official or the information-security team collaborate with other departments and corporate functions on cybersecurity-related matters? For example, does he or she coordinate with
  - The Data Protection Officer regarding the balance of privacy and security monitoring;
  - The Senior Risk Officer regarding the technical/digital risk as part of the overall company's risk;
  - 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 official should be able to articulate how cybersecurity is not just a technology problem; it is about paving the way for the company to implement its strategy as securely as possible.

- What support does the security official receive from the CEO, CIO, and senior management team? This is often reflected in the budget, but it is also often reflected in how many communities or functions within the company are exempted for key security policies or controls.

Outside the organization

- Does the security official or the information security team participate in cybersecurity information-sharing initiatives (e.g., industry-focused, IT-community-focused, or public-private partnerships)? How is the information that is gathered from participation in such initiatives used and shared within the organization?

[52] 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 official (or the information security team) have relationships with public-sector stakeholders such as law enforcement agencies (e.g. state police (Landeskriminalamt, LKA)), federal police (Bundeskriminalamt, BKA), regulatory agencies' cybersecurity divisions, the Computer Emergency Response Team (CERT-Bund, Deutscher CERT-Verbund), etc.?

Inside and outside the organization

- How does the security official or the information security team develop and maintain knowledge of the organization's strategic objectives, business model, and operating activities?
  - For example, in companies actively pursuing a cloud strategy, to what extent does the security official understand the strategy and contribute to its secure execution?
- What continuing education activities are undertaken by the security official and the information security team in order to remain current in cybersecurity matters?

4. Assess performance.

- How is the security official'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 organization as a whole? Do we use a risk-based approach that provides a higher level of protection for the organization's most valuable and critical assets?
- To what extent are cyber-risk assessment and management activities integrated into the organization's enterprise-wide risk-management processes? Are we using a recognized framework to assess cybersecurity hygiene from an organization-wide perspective?

5. Engage the security official in discussion about the "state of the organization."

- What was the organization'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 organization'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?

APPENDIX H

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."[53] 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.*[54]

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 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 those digital risks, 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.	

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

[54] 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 Alliance for Cyber Security (ACS), an initiative of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), supports companies with head or branch offices in Germany in increasing the level of information security and effectively protecting their assets and business processes against potential cyber threats. Via the ACS, BSI is working actively with partners and multipliers in order to provide companies of any size and across industries with strategic and practical guidance. Members receive insights into the current threat landscape as well as good practices and effective countermeasures for the protection of their business via the ACS website. Events and working groups organised by ACS enable the confidential exchange of information and experiences among members of the business and research communities.
As an association of all major players in the field of cyber security in Germany, the Alliance for Cyber Security counts about 2.600 members, 100 partners and 45 multipliers (February 2018).

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.

INTERNET SECURITY ALLIANCE

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