Allianz für Cyber-Sicherheit

INTERNET SECURITY ALLIANCE

Managing Cyber Risk

A Handbook for German Boards of Directors

With the support of:

SAP

Legal notice

Publisher

Allianz für Cyber-Sicherheit
Godesberger Allee 185-189
53175 Bonn

Phone

+49 (0) 22899 9582-0

Fax

+49 (0) 22899 9582-5400

E-mail

info@cyber-allianz.de

Internet

www.allianz-fuer-cybersicherheit.de

Date

October 2022

Texts and Editors

Allianz für Cyber-Sicherheit

Images

Titel, Rückseite: AdobeStock © Alex; Titel: AdobeStock © Gondex, AdobeStock © derplan13; S. 06, S. 07: BSI; S. 10, S. 12, S. 14, S. 17, S.28, S. 29: AdobeStock © Simple Line; S. 20: AdobeStock © samuii; S. 30: AdobeStock © riz; S. 31: AdobeStock © the8monkey

This brochure is distributed free of charge by the Allianz für Cyber-Sicherheit and it is not intended for sale.

Table of Contents

Acknowledgements

We wish to thank the following individuals for their contributions to this handbook (in alphabetical order by organization):

Internet Security Alliance Board of Directors

Justin Acquaro
Interim Global Chief Information and Product Cyber Security Officer
GE

Wil Bennett
Vice President, Chief Information Security Officer
USAA

Robyn M. Boerstling
Vice President of Infrastructure, Innovation and Human Resources Policy
National Association of Manufacturers

Ryan Boulais
Chief Information Security Officer
AES

Andrew Cotton
Partner and Americas Cybersecurity Leader
Ernst & Young, LLP

Deneen DeFiore
Vice President and Chief Information Security Officer
United Airlines

Jason Escaravage
Chief Information Security Officer
Thomson Reuters

John Frazzini
President and CEO
X-Analytics

Mike Gordon
Chief Information Security Officer
Lockheed Martin Corporation

Ron Green
Executive Vice President and Chief Security Officer
Mastercard

Tracie Grella
Global Head of Cyber
AIG

Michael Higgins
Vice President, Information Security and Chief Information Security Officer
L3 Harris

Lisa Humbert
Operational Risk Management Officer for the Americas
MUFG Americas

Andy Kirkland
Chief Information Security Officer, Global Cyber Security
Starbucks

Shaun McAdams
Executive Director, Cyber Operations
Raytheon Technologies

Tim McKnight
Chief Security Officer
SAP

Tim McNulty
Associate Vice President of Government Relations
Carnegie Mellon University

Greg Montana
Corporate Executive Vice President, Chief Risk Officer
FIS

Richard Rocca
Chief Information Security Officer
Bunge Ldt.

Carolann Shields
Chief Information Security Officer, Digital Technology
Baker Hughes

Richard Spearman
Group Corporate Security Director
Vodafone

Dimitrios Stratakis
Chief Technology Risk Officer
Bank of New York Mellon

Ted Webster
Senior Vice President, Security Governance, Risk and Compliance
Centene Corporation

J.R. Williamson
Senior Vice President and Chief Information Security Officer
Leidos

Larry Clinton
President and Chief Executive Officer
Internet Security Alliance

Josh Higgins
Senior Director of Policy and Communications
Internet Security Alliance

Anton Marx
Senior Executive Assistant to the President and CEO
Internet Security Alliance

National Association of Corporate Directors

Peter R. Gleason
Chief Executive Officer

Erin Essenmacher
President and Chief Strategy Officer

Friso van der Oord
Director of Research and Editorial

Leah Rozin
Senior Research Manager

Barton Edgerton
Senior Manager Governance Analytics

Ted Sikora
Manager of Benchmarking and Data Insights

Reaa Chadha
Senior Research Analyst

Andrew Lepczyk
Research Analyst

Margaret Suslick
Senior Copy Editor

Patricia W. Smith
Art Director

Alex Nguyen
Graphic Designer

Contributors

Sebastian Hess
AIG

Torben Schwierzke
AIG

Erwin Kruschitz
Anapur

Matteo Große-Kampmann
AWARE7

Gregor Buerner
BASF Digital Solutions

Dietrich Kästner
BMW

Stefan Becker
Federal Office for Information Security (BSI)

Simona Autolitano
Federal Office for Information Security (BSI)

Benedikt Scherer
Federal Office for Information Security (BSI)

Agnieszka Pawlowska
Federal Office for Information Security (BSI)

Fabian Nißing
Federal Office for Information Security (BSI)

Adrian Schneider
Commerzbank

Jens.Berwanger
Commerzbank

Sebastian Klipper
CycleSEC

Axel Petri
Deutsche Telekom

Christian Schoop
DLA Piper UK

Jan Pohle
DLA Piper UK

Niels Hoffmann
DLA Piper UK

Michael Ebner
Energie Baden-Württemberg

Gerhard Oppenhorst
ESC – Enterprise Security Center

Koen Gijsbers
Former Head of NATO NCI Agency

Larry Clinton
Internet Security Alliance

Josh Higgins
Internet Security Alliance

Anton Marx
Internet Security Alliance

Daniel Schatz
QIAGEN

Milen Volkmar
Q-SOFT

Tim McKnight
SAP

Niall Brennan
SAP

Florestan Peters
SoSafe

Foreword

Since the publication of the first manual “Managing Cyber Risks” in 2018, the general conditions of our working world have changed significantly. The coronavirus pandemic has not only sped up the rapid expansion of home working but has also influenced global supply chains. Digitalization in the state, economy, and society has advanced rapidly in recent years. At the same time, the threat situation for information security has further intensified. In 2021, the Federal Office for Information Security (BSI), as the federal cyber security authority, had to announce the highest warning level for acute vulnerabilities twice - an unprecedented event in BSI history. At the Federal Press Conference in October 2021, when presenting the BSI situation report, we declared a red alert level in some areas.

The advancing digitalization and the simultaneously increasing threat situation make one thing clear above all else: information security must be considered from the very beginning in process and product planning. It must no longer be misunderstood as an obstacle to innovation but must be seen as an investment in the future. Only if we consistently take this into account will we be able to use the full potential of digitalization. More than ever before, information security is the prerequisite for sustainably secure digitalization. This is a simple formula that is not always easy to convey, because successful cybersecurity is invisible. Only when something happens do deficiencies in protection become visible. Ransomware incidents cause production downtimes and paralyze companies and supply chains. Together with the often necessary rebuilding of IT systems, companies often suffer high financial losses.

I am deeply convinced that decision-makers in companies must adopt this mindset when analyzing their corporate risk. Cybersecurity is a matter for the top management. For this reason, the BSI, as the organizer of Germany’s largest IT Security Congress, has chosen this motto in 2022. In order to make the right decisions, supervisory board members must have adequate access to cyber expertise. That is why I am particularly pleased with the updated version of this handbook and recommend reading it. Just as the threat landscape grows, we need to develop our capabilities to proactively manage cyber risks.

International experts have contributed to the success of this project with their knowledge and best practice experiences. My thanks go to them and especially to the Internet Security Alliance for this important contribution to more cybersecurity in companies.

Dr. Gerhard Schabhüser,
Vice-President, German Federal Office for Information Security

Foreword

The Internet Security Alliance congratulates the German Office of Information Security (BSI) on its second edition of the Cyber Risk Oversight Handbook for Corporate Boards. It has been ISA's honor to collaborate with BSI on both of these documents.

This handbook addresses a critical, and often overlooked, aspect of cybersecurity – the unique role of the boards of directors. Although the senior corporate staff have the responsibility to manage cyber risk for the organization, the board's job it to provide proper oversight on the management team and assure that the considerations around cyber risk are incorporated into all significant business decisions.

This handbook provides the clear and concise principles and tools for the board to implement the critical collaboration with between the board and the management team on cybersecurity.

The current edition builds on the previous edition as well as lessoned learned from the development of similar handbooks that are now in circulation on four continents and in five languages. Previous editions have been sponsored by the ISA and partner organizations similar to BSI including the US Department of Homeland Security, the US Department of Justice, and the Organization of American States.

Just as BSI collaborated with the German Cybersecurity Federation, previous editions have been co-sponsored by the European Conference of Director Associations, to the US National Association of Corporate Directors, the Japanese Business Federation.

In addition, the principles and practices outlined in this book are the only set of best practices for cyber risk oversight that have ever been independently assessed and found to substantially improve organizational cyber security. PWC in their Global Information Security Study found that organizations that use these principles and practices generate improved budgeting, better cyber risk management, closer alignment between business goals and cybersecurity and help to generate the creation of a culture of security.

Moreover, this is the first edition of the Cyber Risk Oversight handbook that also incorporates the Principles developed by The World Economic Forum in collaboration with ISA and NACD in 2021. This new content embraces the notion that corporate boards need to go beyond their corporate walls when considering cyber risk and focus on the needs of the full cyber-ecosystem.

This principle is a natural alignment with the movement toward greater appreciation of environmental and social governance (ESG). The defining characteristic of the Internet is the vast interconnection among disparate systems. No one system – not government nor industry -- can secure itself acting alone. It is the responsibility for corporate boards to not only recognize their broader responsibilities but to act on them.

This handbook calls on corporate boards to not only practice sound principles and practices to assure they own cybersecurity but asserts it is an affirmative responsibility for boards and management to reach beyond their own entity and collaborate with government and industry partners in a collective defense model.

By following the prescriptions and recommendations in this handbook, organizations will not only secure themselves better but also help forge the development of a sustainably secure cyber system for all.

Larry Clinton

Larry Clinton,
President, Internet Security Alliance

Introduction

Corporate fiduciaries and boards of directors[1] are responsible for overseeing management strategy, as well as for identification and planned response to enterprise-wide risks impacting the company and its value to stakeholders and shareholders. However, in the past 25 years, the nature of corporate asset value has changed significantly, shifting away from the physical and toward the virtual.

This rapid "digitization" of corporate assets has resulted in a corresponding transformation of strategies and business models—as well as the digitization of corporate risk. Indeed, digital transformation brings with it advantages for organizations but also potential new risks.

As mentioned in the Global Risks Report 2019, as well as in the more recent Global Risks Reports 2022, business leaders in advanced economies rank cyberattacks among their top concerns.[2] A serious attack can destroy not only a company's financial health but also have systemic effects causing harm to the economy as a whole and even national security.

Starting in 2014, the National Association of Corporate Directors (NACD), in conjunction with the American International Group (AIG) and the Internet Security Alliance (ISA), created this handbook series, which identified five principles boards should consider as they seek to enhance their oversight of cyber risks.

That handbook has been independently assessed and found to enhance cyber-risk management, improve budgeting, and create closer alignment between business goals and cybersecurity while enhancing the culture of security within organizations that use it.[3]

With the objective to make cybersecurity "a matter for the top management", the Alliance for Cyber Security has also published a revised handbook for the German market in 2018, in close cooperation with the ISA, NACD and AIG.

The five key principles that boards should follow to fulfill their cybersecurity responsibilities are these:

1. **Boards need to understand that cybersecurity is not just an IT issue:** Directors need to understand and approach cybersecurity as a strategic, enterprise risk, not just an IT risk.

2. **Boards should be aware of existing legal issues in cybersecurity:** Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

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

4. **Boards should demand from management a framework for cybersecurity:** Directors should set the expectation that management will establish an enterprise-wide, cyber-risk management framework with adequate staffing and budget.

5. **Boards should demand from management a clear and comprehensive cyber risk assessment:** Board-management discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach.

This edition of the handbook builds on these five key principles and includes an additional sixth principle:

6. **Boards should encourage systemic collaboration and sharing of best practices:** Directors should encourage collaboration across their industry and with public and private stakeholders to ensure that each entity supports the overall resilience of the interconnected whole.

[1] While companies in the United States are characterized by a one-tier system, in Germany companies are characterized by a two-tier system, which includes a management board and a supervisory board. With the term "boards of director" or simply "directors", the text refers to the overall top management of a company.

[2] World Economic Forum. (2019). Global Risks Report 2019. Geneva, Switzerland: World Economic Forum, p. 6.

[3] PwC. (2016). The Global State of Information Security Survey 2016. Online: PwC.

[4] The Alliance for Cyber Security is an initiative of the Federal Office for Information Security (BSI). The Alliance for Cyber Security is a public-private partnership that since 2012 offers a platform for information exchange, sharing of best practices and collaboration between the members of the network. You can find more information of the website of the Alliance for Cyber Security.

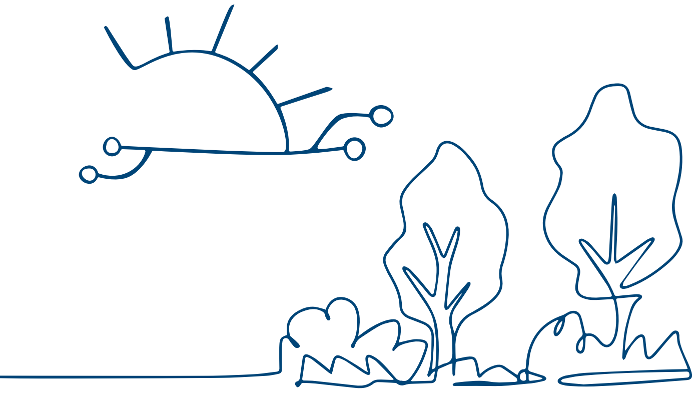
[5] The first edition of the German Handbook is available on the website of the Alliance for Cyber Security (in German only).

Moreover, this book includes an extensive toolkit to help boards implement these principles.

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 cybercriminals or other adversaries.

A rapidly evolving cyber-threat landscape

The 2018 CSIS/McAfee report on cybercrime concluded, “cybercrime is relentless, undiminished, and unlikely to stop. It is just too easy and too rewarding, and the chances of being caught and punished are perceived as being too low. Cybercriminals at the high end are as technologically sophisticated as the most advanced IT companies and, like them, have moved quickly to adopt cloud computing, artificial intelligence, [...] and encryption.”[6]



Along this line, the Federal Office for Information Security (BSI) has observed a continuation of this trend. Between June 2020 and May 2021, attackers utilizing malware for mass cybercriminal attacks on private citizens, commercial enterprises and other institutions have grown exponentially.[7] Compared to the previous reporting period, attackers have significantly accelerated their production of new malware variants. While an average of 322,000 new variants a day were identified in the previous reporting period, this daily indicator reached an average of 394,000 variants in the current period – an increase of over 22 percent. Attackers therefore produced around 144 million new malware variants in total during the current reporting period.

Who Gets Attacked, What Gets Attacked, and How

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, and even access cloud-based data where companies are not directly managing security. Intruders look at multiple avenues to exploit all layers of security 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, attackers hacking into a system, insider threats including contract workers and employees – whether disgruntled or merely poorly trained – present at least as big an exposure for companies as attacks from the outside.

According to McKinsey, insider threats are present in half of all cyber breaches.[8] This highlights the need for a strong and adaptable security program, equally balanced between external and internal cyber threats. Organizations cannot deal with advanced threats if they are unable to stop low-end attacks. More recently, cyber extortion through ransomware attacks has significantly increased as a key risk for organizations of all sizes. (See Tool D – Incident Response.)

The vast majority of cyber incidents are economically motivated.[9] Cyber criminals routinely attempt to steal, corrupt, or encrypt all manner of data. Typical targets include personal information, financial data, business plans, trade secrets, and intellectual property. However, any data of value or essential information system can be a target for attack.

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

[6] Lewis, J. A. (2018). Economic Impact of Cybercrime. At $600 Billion and Counting - No Slowing Down. Online: Center for Strategic and International Studies (CSIS) and McAfee, p. 4.

[7] Bundesamt für Sicherheit in der Informationstechnik. (2021). The State of IT Security in Germany 2021. Online: BSI, p. 9.

[8] Bailey T., Kolo B., Rajagopalan K., Ware D. (September 2018). Insider Threat: The Human Element of Cyber Risk. Online: McKinsey & Company.

[9] Columbus L. (May 15, 2018). 76% Of IT Security Breaches Are Motivated By Money First. Online: Forbes.

“We Are Too Small for the Attackers to be Interested” – Wrong!

Some organizations believe that 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 don’t hold substantial amounts of sensitive consumer data, such as credit card numbers or medical information.
In fact, adversaries target organizations of all sizes and from every industry, seeking anything that might be of value, including the following assets:

- Business plans, including merger or acquisition strategies, bids, etc.
- Trading algorithms
- Contracts or proposed agreements with customers, suppliers, distributors, joint venture partners, etc.
- Employee log-in credentials
- Facility information, 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

majority of small and medium-sized businesses have been victims of cyberattacks. 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.

Balancing cybersecurity with growth and profitability is the way forward

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 the organization and mitigating downside losses, while continuing to ensure profitability and growth in a competitive environment.

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 six 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.

PRINCIPLE 1

Boards need to understand that cybersecurity is not just an IT issue

Directors need to understand and approach cybersecurity as a strategic, enterprise risk, not just an IT risk.

To implement this principle see:

- **Tool A:** "Questions for a Board Member to Ask About Cybersecurity"

Background

Historically, many companies and organizations categorized information security as a technical or operational issue to be handled by the information technology (IT) department. However, cybersecurity is more than an IT issue. This misunderstanding was fed by siloed operating structures that left functions and business units within the organization feeling disconnected from responsibility for the security of their own data. Instead, this critical responsibility was handed off to IT, a department that in most organizations is strapped for resources and budget authority. Furthermore, deferring responsibility to IT inhibited critical analysis of and communication about security issues, and hampered the adoption of effective, organization-wide security strategies.

Over the last several years, technology and data have moved out of their supporting roles and taken center stage as critical drivers of strategy. For example, organizations are investigating new ways to manage data, (e.g., having some data residing on external networks or in public "clouds,"), which can improve cost-effectiveness and efficiency, but also introduce new risks. This means that cybersecurity is more than an IT issue, and the IT component is one piece a risk general management strategy and should be evaluated alongside other forms of security. Executives and board members now need to recognize that cybersecurity is an integral element in the critical and often very challenging transformations that their companies are undertaking to grow and compete in the digital age. While progress has been made, many management teams and boards still hold dated views about cybersecurity. The 2019-2020 NACD Public Company Governance Survey noted that a majority of board members continue to regard cybersecurity as an area for improvement[10] and expect changing cybersecurity threats to have a major impact on their business in the next 12 months.[11] A global information security survey conducted by EY reached similar conclusions, finding that "77% of organizations are still operating with only limited cybersecurity and resilience [against cyber threats], while 87% of organizations warn they do not yet have sufficient budget to provide the levels of cybersecurity and resilience they want."[12] Along this line, in a recent survey conducted by the Federal Office for Information Security (BSI), only about half of all responders – regardless of their size – stated that they apply the principle of "cybersecurity is a matter for the top management" in their enterprise.[13]

The Way Forward

Against this background, the key questions for the board are no longer limited to how technological innovation can enable business processes, but how to balance their own major digital transformations with effective management of inherent cyber risk that can compromise the enterprise's long-term strategic interests.

Boards members should also understand what "crown jewels" the company most needs to protect, and ensure that management has a protection, detection, and response strategy.

Further, boards can ask management about the process for inventorying cyber risks across the organization, including how they work across business verticals, to help identify potential vulnerabilities. The board should instruct management to consider not only the highest-probability attacks and defenses, but also low-probability, high-impact attacks that would be catastrophic attacks. With emerging disruptive technologies on the horizon, it is critical for boards and management to continually evaluate whether their current definition of crown jewels is still valid.

Management teams and boards are starting to integrate the use of new digital technologies and data capabilities into discussions about key strategy and plans that cut across the entire organization. Ideally, cybersecurity should be part of the same dialogue as well.

To sum up, cybersecurity should be seen as an enterprise-wide strategy and risk-management issue that should be addressed holistically and proactively considered when making major strategic decisions. Specific suggestions about how this can be done are described in Principles 4 and 5, as well as throughout the Toolkit.

Identifying the Company's "Crown Jewels"

Directors should engage 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 make sure that they are adequately protecting our data?

[10] National Association of Corporate Directors. (2019). 2019–2020 NACD Public Company Governance Survey. Arlington, VA: NACD, p. 13.
[11] Ibid. p. 12.
[12] Ernest & Young (2021). Global Information Security Survey. Online: EY.
[13] Bundesamt für Sicherheit in der Informationstechnik (2021). Survey on IT Security im Home-Office. Online: BSI.

PRINCIPLE 2

Boards should be aware of existing legal issues in cybersecurity

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

To implement this principle see:

- **Tool C:** "Supply Chain and Third Party Risk"
- **Tool D:** "Incident Response"
- **Tool G:** "Enhancing Cybersecurity Disclosures"

Background

The legal and regulatory landscape with respect to cybersecurity, including public disclosure, privacy and data protection, information sharing, and infrastructure protection requirements, is complex and constantly evolving. Boards should stay informed about the current compliance and liability issues faced by their organizations—and, potentially, by board members on an individual or collective basis.

At European Union's level, the regulatory landscape is very complex. In the past few years, the European institutions have put forward a series of regulations directly applicable to companies, willing to operate in the Union. For instance, with the adoption of the General Data Protection Regulation (GDPR) in 2016, companies had to put in place a series of mechanisms to ensure swift reporting in case of breaches of personal data.

Next to the GDPR, the 2016 European Union's Network and Information Security (NIS) Directive has also put forward important requirements directed at both, the member states and those companies falling under the category of "Operators of Essential Services" and "Digital Service Providers". The Directive is currently under revision, at the time of writing, a political agreement between the European Parliament and the Council has been reached. Among other things, the revised directive updates the list of sectors and activities subject to cybersecurity obligations, and improves their enforcement.

Other relevant European Union's initiatives in the area of cybersecurity are to be found in the certification and standardization field, such as with the adoption of the Cybersecurity Act in 2019.

More recently, additional harmonization efforts can be found in the Directives on certain aspects concerning contracts for the supply of digital content/services and goods, as well as the proposal for a Regulation for harmonized rules on AI.

Companies should keep in mind that, given the inherent nature of the European Union's Directives, EU member states must implement European legislation but often maintain a certain leeway. This is intended to achieve a minimum harmonisation in the EU internal market while keeping into account the diversity of EU member states. Beyond this minimum harmonisation, therefore, they can (but do not have to) include additional regulations if they do not collide with EU law. For this reason, the aforementioned acts are not the only ones regulating cyber security risks. Member States are partly able to adopt additional requirements despite a European harmonizing act when not in contrast with European law. As a result, industries could still face different obligations across the EU.

As this brief non-exhaustive overview of legislative measures at European level shows, the European regulatory landscape is very complex. Consistently, due to the complexity of the regulatory situation, it is recommended to seek internal or external legal advice, if needed.

The same complexity applies to the US, where each industry faces increasing requirements at state and federal level. Some of these requirements now include governance structures, rapid notification of incidents, oversight of third-parties and vendors. Therefore, boards should understand whether management has an effective compliance program to meet changing requirements, reporting responsibilities, and related obligations. While some of these regulations are highlighted in this principle and throughout the handbook, they are examples and far from all-inclusive.

High-profile attacks may spawn lawsuits, including (for public companies) shareholder derivative suits accusing the organization of mismanagement, waste of corporate assets, and abuse of control. Plaintiffs may also allege that the organization's board of directors neglected its fiduciary duty by failing to take sufficient steps to confirm the adequacy of the company's protections against data breaches and their consequences. Exposures can vary considerably, depending on the organization's dependence on technology and data, sector, and operating locations.

Directors may protected by such exposures so long as the board takes reasonable oversight in advance of and investigation steps following a cybersecurity incident. Some considerations include maintaining records of boardroom discussions about cybersecurity and cyber risks; 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. It is also advisable for directors to participate with management in one or more cyber breach simulations, or "table-top exercises", to better understand their roles and the company's response process in the case of a serious incident.

The Way Forward

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. Simply being aware is not enough. Documenting awareness and consulting with outside counsel can be helpful in order to reduce liability, and address risk.

Challenges include overlapping and conflicting rules and requirements, lack of coordination among rulemaking and legislative authorities, and different priorities driving the development of new regulations.

While directors do not need to have deep knowledge about this increasingly complex area of law, they should be briefed by inside or outside counsel on a regular basis about requirements that apply to the company. Reports from management should enable the board to assess whether or not the organization is adequately addressing these potential legal risks.

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

1. 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.

2. NIS Directive and cybersecurity incident notification requirements and information sharing opportunities that enable the organization to learn about cybersecurity threats.

3. Critical infrastructure providers[14] 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").

4. 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 otherparties of the disruption if it receives the report and if such does not confl ict with the interests of the disclosing party).

5. Pursuant to Section 8f (7) and (8) of the BSI Act (BSIG), companies in the special public interest must report the following disruptions to the BSI without delay:
   a. Disruptions to the availability, integrity, authenticity and confidentiality of the IT systems, components or processes which have led to a failure or to a significant impairment of the provision of value creation or to an incident in accordance with the Incident Ordinance,
   b. Significant disruptions of the availability, integrity, authenticity and confidentiality of the IT systems, components or processes that may lead to an impairment of the provision of value creation or to an incident pursuant to the Major Accidents Ordinance.[15]

6. 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.

7. 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.

Disclosures of cybersecurity risks in public filings and disclosures are not yet required, but may be in the future.[16] Therefore, 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.

[14] 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.

[15] Companies in the special public interest are defined in § 2 para. 14 BSIG. Further information on the obligations and from when they apply to the companies defined in section 2 (14) can be found in section 8f BSIG. You can also click here for more details.

[16] See the recent proposal of the Securities and Exchange Commission on "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies" of March 9, 2022.

PRINCIPLE 3

Boards should have adequate access to cyber expertise

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.

To implement this principle see:

- **Tool A:** "10 Questions for a Board Member to Ask About Cybersecurity"
- **Tool B:** "The Cyber-Insider Threat - A Real and Ever-Present Danger"
- **Tool F:** "Building a Relationship with the CISO"
- **Tool H:** "Personal Cybersecurity for Board Members"

Background

As the cyber threat has grown, the responsibility (and expectations) of board members also has grown. Directors need to do more than simply understand that threats exist and receive reports from management. They need to employ the same principles of inquiry and constructive challenge that are standard features of board-management discussions about strategy and company performance. As a director at an NACD forum observed, "Cyber literacy can be considered similar to financial literacy. Not everyone on the board is an auditor, but everyone should be able to read a financial statement and understand the financial language of business."[17]

As discussed in Principle 1, leading boards now understand that cybersecurity is not simply a separate discussion item to be addressed for a few minutes at the end of a board meeting. Rather, cybersecurity is an essential element of many board-level business decisions and needs to be integrated into discussions about issues like mergers, acquisitions, new product development, strategic partnerships, and the like at an early stage. As a result, boards need to be accessing information not simply from IT and technical operations but from a wide range of sources including human resources, finance, public relations, legal/compliance, and others. Greater detail on how the management team can better engage in this modern conception of cyber risk management can be found in Cybersecurity for Business[18] the companion volume to the Cyber Risk Oversight Handbooks.

[17] National Association of Corporate Directors, et al. (2014). Cybersecurity: Boardroom Implications. Washington DC: NACD, p. 3.

[18] Clinton, L. ed. (2022). Cybersecurity for Business: Organization-wide Strategies To Ensure Cyber Risk is NOT Just an "IT" Issue. London, New York, New Delhi: Kogan Page.

Over the past decade, boards have become more active in overseeing cybersecurity and requiring information from management. A 2012 Survey found that fewer than 40 percent of boards regularly received reports on privacy and security risks, and 26 percent rarely or never received such information.[19] Since then, boardroom practices have changed dramatically. In an NACD survey of public-company directors, 79 percent now believe their "board's understanding of cyber risk today has significantly improved, compared to two years ago."[20]

In fact, most public-company directors say their boards discuss cybersecurity issues on a regular basis and receive information from a range of management team members. A majority of boards have reviewed their company's response plans, received briefings from internal advisors, reviewed the company's data privacy protections, and communicated with management about cyber-risk oversight over the past year. In fact, more than 75 percent of boards reviewed their company's current approach to securing its most critical assets against cyberattacks within the past year.[21]

Despite these signs of progress, a majority of directors "are looking to improve cybersecurity oversight across the coming year."[22] Boards often have legal and financial expertise, but lack cybersecurity expertise. In fact, only a small percentage of directors believe their board has a "high" level of knowledge of cybersecurity risks, and few organizations say their information security reporting currently fully meets their expectations.[23]

To sum up, as board responsibility in cyber-risk oversight increases, so does the need for information and cybersecurity expertise.

The Way Forward

There are different ways on how the board can access cybersecurity information. There is no single approach that will fit every board: some choose to conduct all cyber-risk-related discussions at the full-board level; others assign specific cybersecurity-related oversight responsibilities to one or more committees (audit, risk, technology, etc.); and still others use a combination of these methods.

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. This should begin with using the cybersecurity expertise within the company enhance their knowledge.

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. This should begin with using the cybersecurity expertise within the company enhance their knowledge. Boards should be in direct contact with the Chief Information Security Officer (CISO) about cybersecurity risks to the organization. Boards can work with the CISO and the security team to schedule deep dives and education programs to educate the board on cyber issues.

In order to ensure up-to-date information of the state of IT security in the company, boards should ask management to adopt a more comprehensive an enterprise-wide risk framework and reporting structure discussed in Principle 4.

Moreover, what is that board's chosen approach is clearly defined in committee charters to avoid confusion or duplication of effort. The full board should be briefed on cybersecurity matters regularly and as specific incidents or situations warrant. Committees with designated responsibility for risk oversight— and for oversight of cyber-related risks in particular—should receive briefings on at least a quarterly basis. In order to encourage knowledge-sharing and dialogue, some boards could also invite all directors to attend committee-level discussions on cyber-risk issues or make use of cross-committee membership.

Management reporting to the board on relevant cybersecurity matters should also be flexible enough to reflect the changing threat envi¬ronment, as well as evolving company circumstances and board needs.

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 a

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

[20] National Association of Corporate Directors (2019). 2019–2020 NACD Public Company Governance Survey. Arlington, VA: NACD, p. 20.

[21] Ibid. p. 10.

[22] National Association of Corporate Directors (2019). Current and Emerging Practices in Cyber Risk Oversight. Arlington, VA: NACD, p.1.

[23] Ernest & Young (August 16, 2019). EY Global information Security Survey. Online: EY.

wide range of issues to be presented to the board including discussions on new business plans and product offerings.

As discussed in Principle 1, as corporate assets have increasingly become digital assets, virtually all major business decisions before the board will have cybersecurity components to them. In many ways, cybersecurity is now a cross-cutting issue similar to legal and finance. Effective boards approach cybersecurity as an enterprise-wide risk management issue.
Other methods to augmenting their in-house expertise include:

- Scheduling deep-dive briefings or examinations from independent and objective third-party experts validating whether the cybersecurity program is meeting its objectives.

- Leveraging the board's existing independent advisors, such as external auditors and outside counsel, who will have a multiclient and industry-wide perspective on cyber-risk trends.

- Participating in relevant director-education programs, whether provided in-house or externally, and events such as the German IT Security Congress ("IT-Sicherheitskongress"). Such events provide great opportunities for exchange and learning. Here Boards can learn from each other and share relevant information to minimize the systemic and individual risk. Important is also that boards incorporate a "report-back" item on their agendas to allow directors to share their takeaways from outside programs with fellow board members.

- Establishing time and relationships with cyber law enforcement and government agents, with whom the organization will be collaborating in the event of a cyber incident or breach to investigate and respond to attacks. For example, companies can establish relationships with the German Federal Office for Information Security and local law enforcement agencies, so there is pre-established industry-government coordination in advance of a breach. The Alliance for Cyber Security, also known as ACS, is one of the possible ways industries can cooperate with the German Federal Office for Information Security. The ACS is a public-private partnership that since 2012 offers a platform for information exchange, sharing of best practices and collaboration between the members of the network.

Snapshot: Current Debate

How to organize the board to manage the oversight of cyber risk — and, more broadly, enterprise-level risk oversight — is a matter of considerable debate. 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. There are several questions a board should consider before opting for this strategy:

- How are we defining "cyber expert"? The very first principle in this handbook is that cyber security is not simply an "IT" issue, but rather an enterprise-wide risk-management issue. So, is the board looking to add an expert in enterprise-wide security issues?
- Is this strategy really deferring to one individual a responsibility that the full board should undertake? Might it be more appropriate for the full board to increase their understanding of cybersecurity systems in a way that is similar to the understanding that non-lawyers and non-financial experts have with these respective issues?
- How does having a single cyber expert on the board mesh with the cross-functional cyber-management structures that are becoming increasingly common?
- Does placing a cyber expert on the board set a precedent for assigning seats to other specialized areas such as diversity or environmental, social, and governance (ESG) matters?

PRINCIPLE 4

Boards should demand from management a framework for cybersecurity

Directors should require that management provide an enterprise-wide technical and structural framework for cyber-risk management with adequate staffing and budget.

To implement this principle see:

- **Tool B:** "The Cyber-Insider Threat – A Real and Ever-Present Danger!"
- **Tool C:** "Supply Chain and Third-Party Risks"
- **Tool D:** "Incident Response"
- **Tool E:** "Board-Level Cybersecurity Metrics"
- **Tool F:** "Building a Relationship with the CISO"
- **Tool G:** "Enhancing Cybersecurity Oversight Disclosures – 10 Questions for the Board"
- **Tool I:** "German Government Resources"

Background

While Principle 1, 2 and 3 of the handbook focus on what the board should be doing itself, Principles 4 and 5 focus more on what the board should be expecting from management. In order for boards to engage in effective oversight, it is important to understand the responsibilities that management has in addressing the organization's cyber risks.

In line with Principle 1, directors should seek assurances that management is taking an appropriate enterprise-wide approach to cybersecurity. Boards should underscore that meeting regulatory requirements do not necessarily mean the organization is secure, and therefore, such a framework should be adapted to the dynamic structure of their business to meet the risk appetite set by the board and management.

The Way Forward

Boards should assess whether management has established both an **enterprise-wide technical framework** as well as a **management framework** that will facilitate effective governance of cyber risk:

1. Establishing A Technical Framework

Modern digital technology systems are immensely complicated. Clearly, directors cannot be expected to fully track and understand the implications of new technologies – such as artificial intelligence (AI), cloud configurations, or blockchain – for cybersecurity. However, boards should understand from management that they use the appropriate cybersecurity framework to defend the digital technology systems that the enterprise relies on. Although some organizations choose to adopt a single cybersecurity framework, it is more likely that organizations will select specific aspects of various frameworks and adapt them to their unique business needs.
To date, no one framework has been empirically demonstrated as superior from a security perspective (possibly due to the vast variance in cyberattack methods), but increasingly tools are being developed that map to various frameworks and will enable management to determine and in some cases quantify security management of the systems they choose to use.

1.1. 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.

1. 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.

2. 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.

1.2. IT- Grundschutz

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 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.

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. The IT-Grundschutz-Kompendium is updated every year by February.

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.

1.3. Additional Frameworks

Different technical frameworks can be mixed and matched to meet the needs set by the board. There are a variety of different frameworks to choose from. The most commonly used technical frameworks management are outlined below. These frameworks serve as examples and are non-prescriptive:

- The National Institute of Standards and Technology (NIST) cybersecurity framework, which consists of "standards, guidelines, and best practices to manage cybersecurity-related risk."[24] The NIST cybersecurity framework's "core" includes five key functions: identify, protect, detect, respond, and recover.[25] The framework is presented in both a 55-page PDF document[26] and Excel table that lists more than one hundred security recommendations.[27]

- The International Organization for Standardization (ISO) created the ISO/IEC 27000 standards for information security.[28] ISO explains that "using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties."

- The Center for Internet Security's "CIS Controls" include a list of 20 different security controls for organizations, categorized as "basic," "foundational," or "organizational."[29] These controls range from establishing an inventory of hardware and software assets to penetration testing and red team exercises.[30]

- The Payment Card Industry (PCI) Data Security Standards set "operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions."[31]

2. Establishing A Management Framework

Consistent with the understanding outlined in Principle 1, cybersecurity needs to be managed across the enterprise, and many different parts of the organization need to take responsibility for specific activities and be held accountable for their contribution to an effective enterprise-wide program.

Having an enterprise-wide approach means that all the players need to be pulling in the same direction to manage cybersecurity on an enterprise-wide basis—as opposed to different systems in different parts of the enterprise.

The implication of this is that a company's best chance of success is to centralize as much as possible. This has organizational, financial, and operational implications. Organizationally, if you have security run by each line of business or geographic region with a loose federation, your chances of having each business run equally well are slim. From a financial perspective, a centrally run security function will be less expensive: duplication will be reduced, and you will have more leverage over vendors. Operationally, monitoring from a single location means all potential incidents can be prioritized and acted upon.

There is no one model that will apply perfectly to all organizations, but a cross-functional, multistakeholder approach is almost certainly something boards should

[24] Additional information on the Cybersecurity Framework is available on the website of the National Institute of Standards and Technology.

[25] National Institute of Standards and Technology. (April 16, 2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Online: NIST.

[26] Ibid.

[27] National Institute of Standards and Technology. (April 16, 2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Excel). Online: NIST.

[28] Additional information on the ISO/IEC 27001 Information Security Management is available on the website of the International Organization for Standardization.

[29] Additional information on "The 18 CIS Critical Security Controls" is available on the website of the Center for Internet Security.

[30] Ibid.

[31] Additional information is available on the website of the PCI Security Standards Council.

consider having management implement. Recognizing that organizations will want to tailor their approach to fit their needs, we offer two different models, which can be used as a starting point.

2.1. The ISA-ANSI Framework

One of the first multistakeholder models developed was created by the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI) in their joint 2008 publication, *The Financial Management of Cyber Risk: 50 Questions Every CFO Should Ask.*

This basic model stresses not only that multistakeholders ought to be involved but also advocates for an identified leader — not from IT — who has cross-organizational authority. It also advocates for a separate cybersecurity budget as opposed to the traditional model of folding cybersecurity into the IT budget.

The ISA-ANSI framework outlines the following seven steps[32]:

1. Establish ownership of cyber risk on a cross-departmental basis. A senior manager with cross-departmental authority, such as the chief financial officer, chief risk officer, or chief operating officer (not the chief information officer), should lead the team.

2. Appoint a cross-organization cyber-risk management team. All substantial stakeholder departments must be represented, including business unit leaders, legal, internal audit and compliance, finance, human resources, IT (including information security), and risk management.

3. The cyber-risk team needs to perform a forward-looking, enterprise-wide risk assessment, using a systematic framework that accounts for the complexity of cyber risk — including, but not limited to, regulatory compliance.

4. Be aware that cybersecurity regulation differs significantly across jurisdictions. 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.

5. Take a collaborative approach to developing reports to the board. Executives should be expected to track and report metrics that quantify the business impact of cyber threats and associated risk-management efforts. Evaluation of cyber-risk management effectiveness and the company's cyber resiliency should be conducted as part of quarterly internal audits and other performance reviews.
6. Develop and adopt an organization-wide cyber-risk management 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. Testing of the plan should be done on a routine basis.

7. Develop and adopt a comprehensive 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 talent and identify what needs can be met in-house versus what can or should be outsourced to third parties. Because cybersecurity is more than IT 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.

2.2. The Tree Lines of Defense Model

A second conceptual model has emerged over the past few years, originating in the financial services sector but increasingly being adopted by leading organizations in various sectors. This "Three Lines of Defense" model stresses multiple independent operations within the organization having varied and increasing roles in assessing and checking cyber-risk management.

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

The model may be summarized this way:

- **Line 1:** operates the business, owns the risk designs, and implements operations.
- **Line 2:** defines policy statements and defines the Risk Management framework. It provides a credible challenge to the first line and is responsible for evaluating risk exposure so that the board can determine risk appetite.
- **Line 3:** commonly, internal audit is responsible for independent evaluation of the first and second lines.

Roles for each level of defense can be further detailed in this way:

Line 1:

- Provide a thorough exam of Line 1's work—is the business doing enough? Each business line defines the cyber risk they face and weaves cyber risk and self-assessment into risk, fraud, crisis management, and resiliency processes.
- Business lines need to actively monitor existing and future exposures and vulnerability threats and assess what impact cyber risk has on new tech deployment, client relationships, and business strategies.

Line 2:

- Line 2 should be established as a separate independent function. Line 2 manages enterprise cyber-risk appetite and the risk-management framework within overall enterprise risk. Line 2 challenges the first line, determines how to appropriately measure cyber risk, and integrates results into a risk-tolerance statement for the company.
- The focus of the first and second lines needs to be on effectively managing risk, not on regulatory compliance, although compliance can be integrated into these lines.

Line 3:

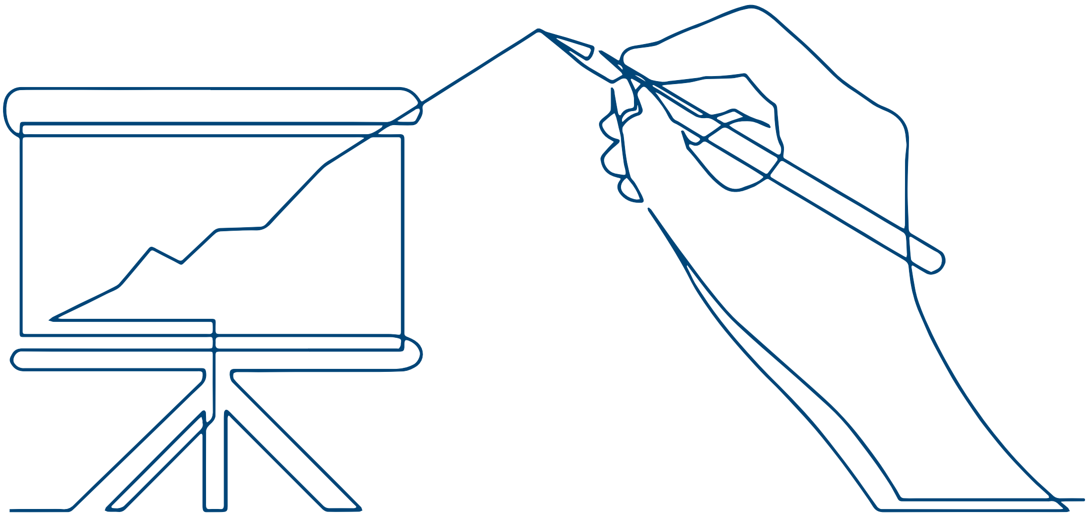
- Line 3 provides an independent, objective assessment of company processes and controls across lines one and two with a focus on operational effectiveness and efficiency. Traditionally, internal audit has focused its testing work on technical IT controls but will need to expand its scope to assess whether cybersecurity is effectively managed as an enterprise risk.
- Internal audit performs process and control assessments, validates technology infrastructure, reviews controls to mitigate third-party risks, conducts independent penetration testing, and stays abreast of new threats.

2.3. Best Practices for Management Consistent with the Enterprise-Wide Model for Cybersecurity

A more detailed explanation of roles and responsibilities for numerous corporate divisions consistent with the enterprise wide cyber risk organizational model can be found in the companion document to the "Cyber Risk Oversight Handbook", the "Cybersecurity for Business".[33]

This book is based on the Principles for board oversight of cyber risk articulated in this handbook and defines management practices consistent with this modernized approach. The book covers best practices for the Human Resources, Supply Chain, Legal, Incident Response, Audit and Technical Operations perspectives consistent with an enterprise wide cyber risk assessment method.

[33] Clinton, L. ed. (2022). Cybersecurity for Business: Organization-wide Strategies To Ensure Cyber Risk is NOT Just an "IT" Issue. London, New York, New Delhi: Kogan Page.



PRINCIPLE 5

Boards should demand from management a clear and comprehensive cyber risk assessment

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

To implement this principle see:

- **Tool D:** "Incident Response"
- **Tool E:** "Board-Level Cybersecurity Metrics"

Background

Perfect cybersecurity is an unrealistic goal yet understanding and managing financial exposure to cyber risk is a critical component to board risk oversight. Managing cyber risk – as with all risks in general – is a continuum, not an end state. Beyond existing security initiatives and compliance discussions, understanding cyber risk in economic terms is increasingly important as related to enterprise cyber-risk oversight.

Boards need to understand how management has determined the effectiveness of the firm's controls and processes in reducing the exposure to cyber risk to an acceptable level. Management being able to communicate cyber risk from an economic perspective is essential because those are the terms in which the board makes its decisions. This level of quantification of effective cyber-risk management allows the company to make better risk-informed decisions about its strategy and, in turn, its resource-allocation choices (See the table below "Defining Risk Appetite").

Traditional risk assessment approaches have had difficulty fulfilling these requirements. Historically, cyber-risk assessments tended to follow long check lists of highly technical information or control requirements – often 500 or more. These methods have historically been qualitative assessments and have not assessed cyber risk through economic terms.[34] However, quantitative economic assessments of cyber risk have matured to the point where cyber risks can now be quantitatively assessed. Accordingly, just as other disciplines financially model major risks such as market, credit, insurance, and strategic risks, cyber risks can now be modeled quantitatively to improve risk-management performance.

[34] Jones J. (2019). Understanding Cyber Risk Quantification: A Buyer's Guide. Online: Fair Institute.

It is rather common to see cyber-risk assessment outcomes expressed as “critical,” “high,” “medium,” etc. While this kind of rating does provide a measure of order of magnitude (ordinal measurement), it does not help decision makers to compare different kinds of cyber risk or to compare cyber risks with other kinds of risks faced by the organization.

On the other hand, quantitative assessments allow organizations to drill down and consider the likelihood, impact, velocity, and duration for cyber risks, which helps management and boards to make informed decisions about the relative criticality of these risks and funding strategies for their mitigation.

Defining “Risk Appetite”

“Risk appetite” is the amount of risk an organization is willing to accept in pursuit of strategic objectives. Thus, it should define the level of risk, through measurement, 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 appetite should address the following questions:

- Corporate values – What risks will we not accept?
- Strategy – What are the risks we need to take?
- Stakeholders – What risks are stakeholders willing to bear, and to what level?
- Capacity – What resources are required to manage those risks.
- Financial – Are we able to adequately quantify the effectiveness of our risk management and harmonize our spending on risk controls?
- Measurement – Can we measure and produce reports to ensure proper monitoring, trending and communication is reporting is occurring?

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

The Way Forward

As companies recognize the value of quantification of cyber risk, much work is being done to enable more advanced quantitative analysis.

Under this approach, organizations can identify assets and risks, and then approach a solution from that standpoint. This should be a circular and ongoing process aimed at continual improvement. Under this approach, the economics of risk should be prioritized alongside liability.

1. Ensuring The Shift from Cybersecurity Defense to Comprehensive Cyber-Risk Management

Directors should ask the right questions to the management in order to assess whether it is carrying out clear and comprehensive cyber risk assessment. At a conceptual level, boards should consider asking questions such as the following:

- **What data, and how much data, are we willing to hold, lose, share, or have compromised as a practical business matter?** In this context, distinguishing between mission-critical assets and other data that is important is a key first step.

- **How long can we afford to be down?** Besides data loss, business disruption must also be considered.

- **How should cyber-risk mitigation investments be allocated among basic and advanced defenses?** For those lower-priority assets, organizations should consider accepting a greater level of security risk than higher-priority assets, as the costs of defense will likely exceed the benefits. Boards should encourage management to frame the company's cybersecurity spending in terms of Return on Investment (ROI), and probability of occurrence associated with exploitation. They should also reassess probability of occurrence and reassess ROI regularly, as the costs of protection, the company's asset priorities, and the magnitude of the threat will change over time.

- **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 by directly reducing the probability of exploitation. Further, organizations should consider the inclusion of preventative measures, such as reviews of cybersecurity frameworks and governance practices, employee training, IT security, expert response services, and consultative security services.

- **What options are available to assist us in transferring certain cyber risks?** Cyber insurance could represent practical option when the risk reduction it achieves versus is cost is a better value than the risk reduction other measures would provide. When choosing a cyber-insurance partner, it is important for an organization to choose by keeping in mind the need of the organization. Insurers frequently conduct in-depth reviews of company cybersecurity frameworks. This can help companies understand their cybersecurity strengths and weaknesses, providing a potential path to improve their cybersecurity maturation. Many insurers, in partnership with technology companies, law firms, public relations companies and others, also offer access to the preventative measures discussed above.

- **How should the impact of cybersecurity incidents be assessed?** Conducting a proper impact assessment can be challenging given the number of factors involved. To take just one example, publicity about data breaches can substantially complicate the risk-evaluation process. Stake-holders—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 priorities for cyber-risk management.

2. Basic Method for Economically Assessing Cyber Risk

Management can use systematic methods to determine their exposure to cyber risk. Effective assessments include technical analysis but go beyond that to fold in other aspects of the business.

Key steps toward more advanced cyber-risk assessment and management may include these:

- Management should seek out the best data available to make assessments of possible attack scenarios.

- Management should focus on scenarios that are probable and would yield an expected loss significant enough to matter to the business.

- Calculate the best case, worst case, and most likely case of attack and identify what degree of loss is acceptable (risk appetite).

- Determine the investment required to mitigate, or transfer, risk to an acceptable level.

- Option: run multiple scenarios using methods such as Monte Carlo simulations to more accurately define risk and mitigation costs to various scenarios.

PRINCIPLE 6

Boards should encourage systemic collaboration

Boards should encourage collaboration and sharing of best practices

To implement this principle see:

- **Tool F:** "Building a Relationship with the CISO"

Background

Effective cyber-risk strategy includes improving the cyber resilience of industries and sectors. The highly interconnected nature of modern organizations means we run the risk of failures that spread beyond one enterprise to affect entire industries, sectors and economies. One organization, product, or service's vulnerability could cause downstream impacts on your organization. As a result, it is no longer sufficient just to ensure the cybersecurity of your own enterprise; rather, cyber resilience demands that organizations work in concert.

In 2020, malware was uploaded to much of the US federal government, including the Department of Defense, to 425 companies in the US Fortune 500, and to as-yet-untold other customers worldwide, by compromising an update installed by SolarWinds, a US-based technology infrastructure vendor.

In March 2021, Microsoft published an unscheduled security update for its widely used groupware and email server, Exchange. At the time the vulnerabilities were made public, some 98 percent of systems analyzed in Germany were vulnerable. To respond to this threat, the BSI raised the threat level to 'Extremely Critical' – the second-highest level – to reflect both the sheer number of servers open to attack and the easy availability of exploit kits.[35]

And the list goes on.

As a number of examples clearly show, cyber risks can arise anywhere: from a company's network of partners, suppliers and vendors.

The Way Forward

Recognizing that only collective action and partnership can meet the cyber-risk challenge effectively, senior strategic leaders must encourage collaboration across their industry and with public and private stakeholders to ensure that each entity supports the overall resilience of the interconnected whole.

Organizations may be reluctant to share information. In fact, often information and data can be unclear and therefore make aggregating risk assessments a large

[35] To learn more on this topic, you can listen to the Podcast of the Alliance for Cyber-Security "Cybersnacs" (in German only).

challenge. However, collective risk and information sharing is essential to reducing ecosystem-wide risk.

While the board's role may be limited in this space, boards should be aware of and invest thought into collaborative practices. Below are several key considerations for how boards can keep in mind systemic cyber risk in their overall risk oversight decision-making:

Key considerations for the board:

- Develop a 360-degree view of the organization's risk and resiliency posture to operate as a socially responsible party in the broader environment in which the business operates
- Develop peer networks, including other board members, to share best governance practices across institutional boundaries
- Ensure management has plans for effective collaboration, especially with the public sector, on improving cyber resilience
- Ensure that management takes into account risks stemming from the broader industry connections (e.g. third parties, vendors and partners)
- Encourage management participation in industry groups and knowledge and information-sharing platforms

Conclusion

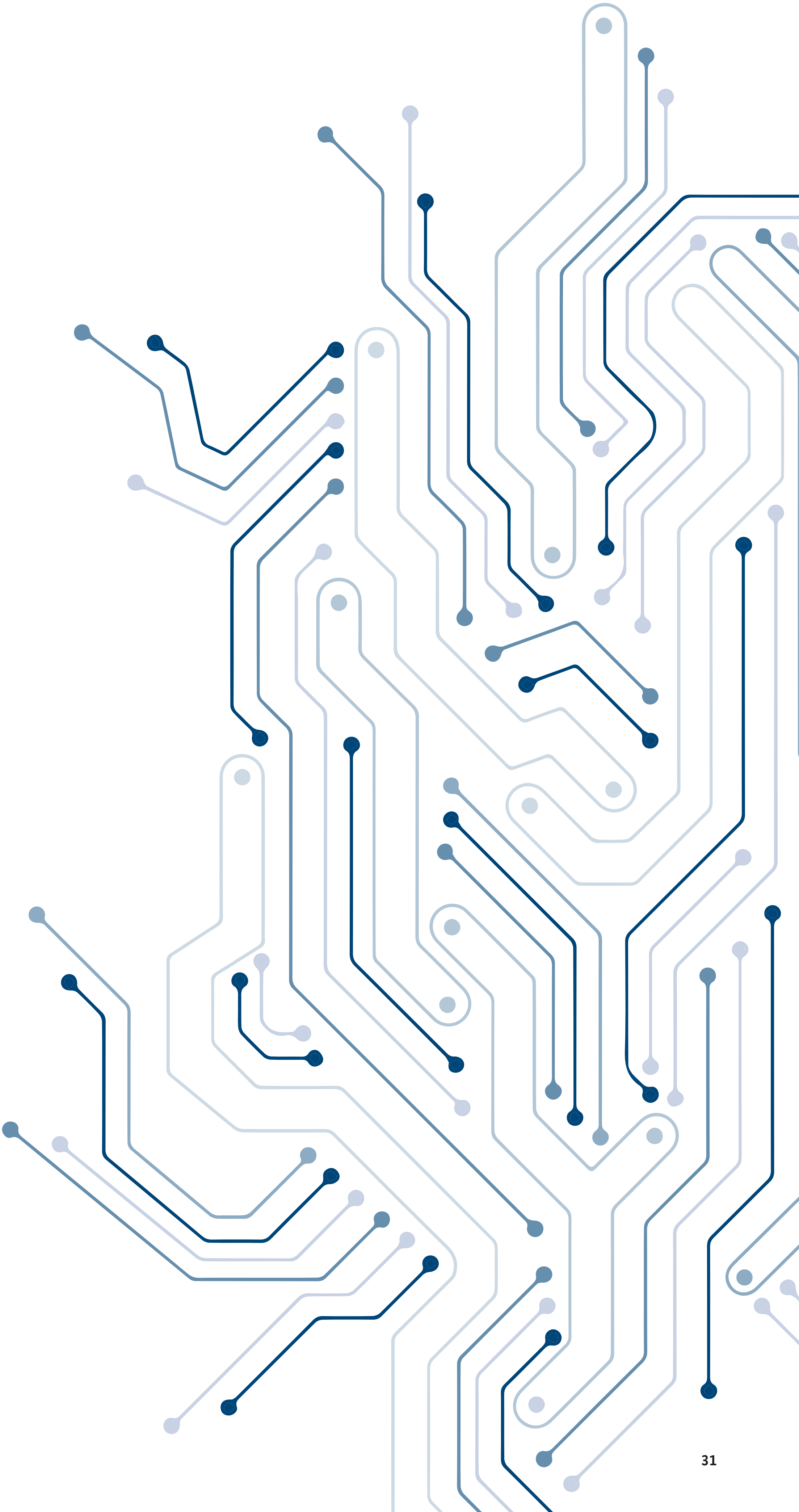
Cybersecurity is now a serious, enterprise-level risk and strategy challenge. Several characteristics make the nature of the threat especially formidable: its complexity and speed of evolution; the potential for significant financial, competitive, and reputational damage; and the fact that complete protection is an unrealistic objective. In the face of these threats, and despite dramatic increases in private-sector cybersecurity spending, the economics of cybersecurity still favor the attackers. Moreover, many technological innovations can increase vulnerability to cyber threats.

Boards need to continuously assess their effectiveness to address cybersecurity, both in terms of their own fiduciary responsibility as well as their oversight of management's activities. While the approaches taken by individual boards will vary, the principles in this handbook offer a helpful blueprint and timely guidance.

This is precisely the aim of this book: to support this target group in this mission and make cybersecurity a matter for the top management. However, in order to achieve this, a basic understanding of the risks in the field of information security is key. Only then, boards of directors and supervisory boards can make informed assessments of the potential economic cyber incidents and decide on the validity of IT security strategies.

Ultimately, as one director put it, "Cybersecurity is a human issue."[36] The board's role is to bring its judgment to bear and provide effective guidance to management, in order to ensure the cybersecurity program is appropriately designed and sufficiently resilient given their company's strategic imperatives and the realities of the business ecosystem in which it operates.

[36] National Association of Corporate Directors, et al. (2014). Cybersecurity: Boardroom Implications. Washington DC: NACD, p. 7.



www.allianz-fuer-cybersicherheit.de
https://isalliance.org/