INTERNATIONAL BOARD FOUNDATION

GLOBAL GUIDELINES ON THE CORPORATE GOVERNANCE OF CYBERSECURITY

Developed by Dr. Maya Bundt and Prof. Dr. Laura Georg Schaffner

It is important for board members to realize that digitalization and new technology may generate incredible opportunities for companies, but at the same time may pose significant risks. The board's role is to weigh the risks and opportunities and to follow a risk-based approach. Security can then even become an enabler and an opportunity in itself.

INTERNATIONAL BOARD FOUNDATION

01 Purpose

The IBF Global Guidelines on the Corporate Governance of Cybersecurity, or national guidelines issued by the respective directors' association, provide the Board of Directors (BoD) with guidance on how to improve governance of cybersecurity, and how to weigh the opportunities that digitalization and technology may bring to companies against the risks involved.

02 Scope

The guidelines are written for larger companies with professional and independent boards, but can be applied by any organization and their oversight body. The guidelines include rules for the BoD and oversight process itself, as well as practical guidance for the organization that is overseen.

03 Development

The guidelines were developed by IBF members, and went through an extensive reviewing and feedback process. Thus, the guidelines represent a collaborative and global effort. Given the fast-paced developments both in the cyber threat landscape as well as in cybersecurity and technology, the guidelines will be reviewed and updated in a timely manner by the IBF policy committee.

04 Core Guidelines

1. **The board should increase its cyber literacy.**

   Each board member should become familiar with the risks of the digital age in general, and with cyber risks affecting their company specifically. This can be achieved through focused training, individual study or exchanges with internal or external specialists. The board as a body can ensure cyber expertise either through deeply knowledgeable board members, or they may 'buy in' that knowledge from internal or external experts.

2. **The board should be familiar with the managers responsible for cyber security within the organization.**

   The board should consider meeting with the executives responsible for cyber security in a regular and timely manner. This could be yearly or even on an ad-hoc basis, depending on the nature of the company and its organization. Pull and push factors of communicating with the responsible should be defined in the organization's governance

3. **The board should ensure the segregation of duties within the organization between the strategy for cybersecurity and its execution.**

   In any organization, the executive and legislative should not be unified in one function. Hence, the executive function of the CIO should not be combined with the more legislative tasks of the CISO function.

4. **The board should request that all employees receive cybersecurity training at regular intervals.**

   Oversight of corporate talent is part of the board's responsibility and the board should thus ensure sufficient cyber security and awareness training for all employees. The objective is to bring the overall organization to a required level of maturity and hence to prevent potential future incidents. This is specifically important since most of the reported cyber incidents have an insider (involve either maliciously or by accident) at their heart

5. **The board should ensure they have adequate time in their agenda to discuss the opportunities and risks of digitalization and the companies' resilience in that respect.**

   Cyber risk and cyber security should have adequate priority, room and discussion time on the board's meeting agenda, thus becoming a topic that the whole board focuses on regularly.

6. **The board should set the risk management framework in a way that ensures adequate controls against cyber risks and which prepares for the worst-case scenarios.**

   The board is typically responsible for the oversight of the organization's internal control environment. Boards need to inform themselves of specific operational, reporting, and compliance aspects of cybersecurity (including legal and regulatory requirements), using and adapting or supplementing as needed at least one recognized framework to do so. Any oversight process should include both defense and response, to ensure business continuity and resilience.

7. **The board should ask for the appropriate metrics that will allow them to understand the company's overall cyber maturity and resilience as well as the level of threat.**

   Frameworks and standards assist the board in assuring a completeness of relevant security metrics reported (see long-paper version for a detailed list of framework and standards). However, boards should be mindful of two potential failures according to the old - but still valid - motto: Do the right things and do things right. The business model and operations of a company define the focus areas for risk-adequate reporting. Boards must ensure they report on the riskiest areas of operations, and do not select simply the metrics that are readily available or easy to collect.

8. **The board should define the role that digitalization and technology plays in their organization's current and future business model, including the identification of opportunities and risks.**

   The company's technology strategy and the role of technology and digitalization in future business models must be an area of strategic focus and oversight by the board, including both the review of future opportunities and of potential risks. In this context, it is important to note that security may even be an asset and potential positioning point for the company.

9. The board should allocate adequate resources to managing technology and cyber risks.

It is important that adequate funding and organizational capabilities are made available for cyber security, and thus the board should ensure that sufficient budgets for technology and security investments and operations are made available. Note that the funding does not only need to cover the technology itself (e.g., software, hardware), but that investments in people and skills, security and resilience processes, and data management are equally important.

10. The board needs to be aware of the laws and regulations regarding data and cybersecurity in all jurisdictions where the company has operations or customers.

The board needs to be knowledgeable about laws and regulations that apply to the operations of their company. This relates for example, but not exclusively, to data protection laws. These laws are very specific for different jurisdictions and impact both technology or business strategy. Also, particular sectors (e.g., financial services, critical infrastructure) often have specific data and cyber security regulations that must be adhered to. Additional data-related regulations may be purely country-specific, for example data localization laws.

11. The board should ask for a sensible data management framework that classifies data, measures its value and allows for a risk-adequate handling of those assets.

The value of data increases the more organizations rely on it during value creation. Boards must apply special emphasis to overseeing the categorization and safeguarding of these assets, and should request the implementation of a practical data management framework, following the GNDI Guidelines on the Corporate Governance of Data (see dataguidelines.com), listing and classifying any data assets that the organization either owns or processes. This data classification can then be used to guide specific protection measures for sensitive data, and to set up the appropriate processes to be performed in order to comply with- for example- data protection laws and regulations.

05 Application

The guidelines provide a global cross-sectoral perspective and serve as a basis for adaptation based on industry, organization type, and jurisdiction.

GLOSSARY

Board of Directors (BoD)

Group of individuals, appointed or/and elected by shareholders and mandated to direct and oversee the company, establish policies for corporate management, appoint and oversee the executive management and to make decision on major company issues.

Cyber maturity

An organization's capabilities with respect to cybersecurity vs. others and/or self-stated targets.

Cyber resilience

An organization's ability to sustainably deliver intended business outcomes despite adverse cyber events. Organizational practices to achieve and maintain cyber resilience must be comprehensive and customized to the whole organization (i.e. including the supply chain). They need to include a formal and properly resourced information security program, team and governance that are effectively integrated with the organization's risk, crisis, business continuity, and education programs.

Digitalization

Process of moving from an analogue to a digital business approach. This guideline also includes 'digital transformation', the pro-active change of business and organizational activities, processes, competencies and models to fully address and leverage the changes and opportunities of relevant digital technologies.

Cyber security

Preservation of confidentiality, integrity and availability of information in cyberspace.

INTERNATIONAL BOARD FOUNDATION

Guiding Principles for Cybersecurity Oversight

Dr. Laura Georg-Schaffner
Dr. Maya Bundt

These 12 key principles are derived from the discussion of the board's internal governance and the board's responsibilities to the organization as outlined in this guideline paper. It is important for board members to understand that technology transformation and digitization generate incredible opportunities for companies, but at the same time pose significant risks. The board's role is to weigh risks and opportunities and take a risk-based approach. Then security can become an enabler and an opportunity in itself.

Summary of the 12 key principles

1. **The board should increase its cyber literacy.**
2. **The board should be familiar with the managers responsible for cyber security within the organization.**
3. **The board should ensure the segregation of duties within the organization between the strategy for cybersecurity and its execution.**
4. **The board should request that all employees receive cybersecurity training at regular intervals.**
5. **The board should ensure they have adequate time in their agenda to discuss the opportunities and risks of digitalization and the company's resilience in that respect.**
6. **The board should set the risk management framework in a way that ensures adequate controls against cyber risks and which prepares for the worst-case scenarios.**
7. **The board should define the risk appetite of the organization and direct risk management actions accordingly.**
8. **The board should ask for the appropriate metrics that will allow them to understand the company's overall cyber maturity and resilience as well as the level of threat.**
9. **The board should define the role that digitalization and technology plays in their organization's current and future business model, including the identification of opportunities and risks.**
10. **The board should allocate adequate resources to managing technology and cyber risks.**
11. **The board needs to be aware of the laws and regulations regarding data and cybersecurity in all jurisdictions where the company has operations or customers.**
12. **The board should ask for a sensible data management framework that classifies data, measures its value and allows for a risk-adequate handling of those assets.**

5 March 2020

GNDI Guidelines for Cybersecurity

Update 2019 to the 2015 Perspective Paper on Cybersecurity

The Global Network of Director Institutes (GNDI), founded in 2012, brings together member-based director associations from around the world with the aim of furthering good corporate governance. Together, the member institutes comprising GNDI represent more than 100,000 directors from a wide range of organizations. This paper describes the global perspective of GNDI on the role of the board in cybersecurity oversight.

1. A Global Issue Calling for Global Solutions

With the digitalization of the economy, an increasing number of companies in a wide range of industries are relying on information and communication technology (ICT) for their day-to-day operations. From airlines to manufacturers to retailers, organizations that never thought of themselves as "digital" or "data-centric" companies are learning the promise and perils of the digital world. Of all perils, the greatest may well be those of cybersecurity: the non-availability, alteration or disclosure of information.

Attacks on information assets of companies are occurring on a widespread and massive scale today, often crossing national borders or even resulting in physical damages. Worldwide, recovery from hacks and other internet crimes are costing the economy more than USD 600 billion per year, estimates McAfee.[1] Furthermore, in addition to the cost of recovery, there are the costs of prevention: the technology research firm Gartner predicts a total of $114 billion in business cybersecurity spending for 2018 alone[2].

Not surprisingly, a number of international and public organizations have tackled the problem of cybersecurity to the economy. These include for example:

- the Organisation for Economic Cooperation and Development (OECD)[3],
- the United Nations General Assembly (UN) with the Internet Governance Forum
- the International Telecommunications Union, with the World Summit on the Information Society,
- the World Economic Forum[4] and
- the NATO Cooperative Cyber Defense Centre of Excellence, which has gathered a comprehensive collection of cybersecurity guidance from over 120 national sources offering insights into national cyber strategy solutions.[5]

[1] https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

[2] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

[3] See for example several OECD publications with respect to security and privacy under the Directorate for Science, Technology, and Innovation: http://www.oecd.org/sti/ieconomy/information-security-and-privacy.htm

[4] The WEF runs cybersecurity as a topical focus, see for example: https://www.weforum.org/agenda/archive/cyber-security/ and has opened the WEF Cybersecurity Center in Geneva in 2018 https://www.weforum.org/centre-for-cybersecurity. There are also specific Board-related thought leadership pieces published by The Global Future Council for Cybersecurity, for example: https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards

[5] https://ccdcoe.org/

In recognition of the global dimension of cyber risks, GNDI hosted a Cybersecurity Summit in 2015[6], setting off a board-level global dialogue from which resulted a first version of this perspective paper. The current version is an update of this first release.

2. What Can the Board Do?

With respect to cybersecurity there is no 100% security. Boards need to ensure the most appropriate level of security and preparedness for their companies as they oversee them—but the question is how? The ultimate goal of any board's oversight should be to reflect and implement the level of risk acceptable to the organization's stakeholder i.e., investors, employees, and regulators, and translate these into concrete actions and optimal investments for the enterprise.[7]
Building on GNDI's first release, this paper seeks to further develop recognized principles for cybersecurity oversight. In the annex of this paper, regional, national and international institutions in charge of developing cybersecurity guidelines are identified, as are additional useful information sources.

2.1 General Guidance

The role of a corporate board in any domain outside their own operations is rightly described as "oversight." This occurs when a body vested with authority controls (or "oversees") the activities of an organization and makes judgments on their adequacy, taking action to ensure any improvements needed. It is worth underscoring the fact that oversight does not mean management: it is unnecessary for directors to delve into in-depth details or technical aspects that are more relevant to executives and operational-level personnel. Nonetheless, directors need to be familiar with the general adequacy and effectiveness of people, processes, technology, and data within the entities entrusted to their care. The board of directors needs to understand the big picture – the essential components of the entity they are overseeing and how they can oversee it effectively.
Fundamentally, the board's approach to cyber risks should not be different to any other area of potential or actual risk:

- risk appetite/tolerance must be determined,
- specific risks must be identified and
- finally, actions must be taken to avoid, mitigate, accept, or transfer risks (e.g., through insurance).

Moreover, as in the case of risk in general, cyber risks need to be overseen by the full board, with support from appropriate committees as the board may assign. The important point is that directors and boards need to treat cyber risks as an integrated component of enterprise-wide risk-management.

The above stated, is a key theme in the National Alliance of Corporate Directors Handbook on Cybersecurity, which has recently been updated for a few selected European markets[8]. The key principles of this handbook are:

---

[6] https://blog.nacdonline.org/posts/global-cyber-summit-sends-message-to-boardrooms

[7] See GNDI perspective paper on Building Principles of Good Governance: "Effective governance structures allow organizations to manage their affairs with proper *oversight* and *accountability*, to *create value* over the short, medium and long term through sound investment and innovation, and provide *accountability and control systems* commensurate with the risks involved." To view this paper, go to gndi.org and click on Papers.

[8] Management von Cyber-Risiken. Handbuch für Unternehmensvorstände und Aufsichtsräte- Deutsche Ausgabe: https://isalliance.org/wp-content/uploads/2018/04/CyberRisk-DSHandbook_Germany-German_Final.pdf and Managing Cyber Risk: A Handbook for UK Boards of Directors. https://isalliance.org/wp-content/uploads/2018/04/CyberRisk-DSHandbook_UK_Final.pdf.

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

When directors are making decisions regarding the safeguarding of their respective companies, they must take the following four dimensions into account.

Each dimension is divided into guidelines that boards should consider regarding their board internal governance, as well as guidelines that directors need to employ to oversee and steer their organization.

2.2 People, Processes, Technology - and Data

In the recent past, the 'golden triangle' of people-processes-technology has been further developed to include data. Since cybersecurity has data at its core, it was an easy decision to add this category to the revision of the paper.[9]

2.2.1 People

The category "people" includes considerations about the adequacy of the organizational setup as well as the number and skills of the people involved.

Board of Directors Internal View

Lately, there has been much discussion in Governance journals and articles about whether there should be at least one member on each Board with specific cyber risk and cyber security expertise and experience. An ongoing international survey shows that 23.3% of all participating boards have such a single expert sitting on their board.[10] Having board members with specific and deep cyber knowledge is desirable but should not lead to a situation where all questions regarding cyber risks are only addressed to this individual.

GNDI proposes that each board member becomes familiar with the risks of the digital age in general and cyber risks affecting their company specifically, much in the same way as directors need to be aware of other risks facing their industry, business model or specific company. One approach that boards should consider is to develop their overall expertise and literacy in the area of digitalization and cybersecurity, offering training to board members in form of life-long learning. In 2019, an average of 49.1% of board members received such in the past two years.[11] Other measures can include, but are not limited to, exchanges with external cyber security specialists, and individual study on

[9] See the results of GNDI Global Director Survey Report and GNDI Guidelines for Data Governance. http://gndi.org/
[10] https://emstrasbourg.eu.qualtrics.com/jfe/form/SV_3vNrA2HcrJ9sB13 (Status February 2020)
[11] https://emstrasbourg.eu.qualtrics.com/jfe/form/SV_3vNrA2HcrJ9sB13 (Status February 2020)

new technology and the associated risks thereof. The idea is to improve the boards' overall cyber literacy in order to have the right discussions and enhance the board's ability to oversee and steer their company.

Organizational View
The board's oversight focuses on the people reporting to the board directly. GNDI saw in 2015 the necessity that cybersecurity needs to be assigned as a specific accountability of one of the officers. We *now want to argue further that security should be a constant variable in every organization's risk management and hence be presented by the respective executive continuously*. The executive having this accountability would ideally report directly to the CEO or to someone on the executive board. In addition, the board should consider meeting with the executives responsible for cybersecurity at the next level or levels down at regular intervals. This could be yearly or on an ad-hoc basis, depending on the nature of the company and organization. Pull and push factors of communicating with the responsible managers should be defined in the organization's governance. Thus, the organization needs to define if, and under which circumstances, the responsible manager will receive the opportunity to speak to the board. Alternatively, the board may define specific topics that must be regularly reported to them, and so it is not left up to the responsible manager to decide on their relevance to the board.

In any organization, the legislative and executive should not be unified in one function. Hence, the executive, often in the form of the CIO, should not be joined with the CISO function, who has rather legislative tasks, i.e. development of a security strategy, policies etc.

More broadly, boards oversee the entire pool of corporate talent and can therefore ensure sufficient cybersecurity and security awareness training for all employees. The objective is to bring the overall organization to a required level of maturity and hence to prevent potential future incidents and to prepare for the case of emergency. This is specifically important since the majority of the reported cyber incidents have an insider (either malicious or by accident) at their heart.[12]

2.2.2 Processes

Board of Directors Internal View
Only 2% of board members say that security was a fixed topic on the board's agenda, while in 17.2% of all enterprises it was never discussed.[13] However, within the Board processes and agenda, cyber risk and cyber security should have adequate room and discussion time. This is especially important since the ongoing digitalization opens up new business models and revenue streams, but also introduces new risks that need to be taken into account and understood by the board.

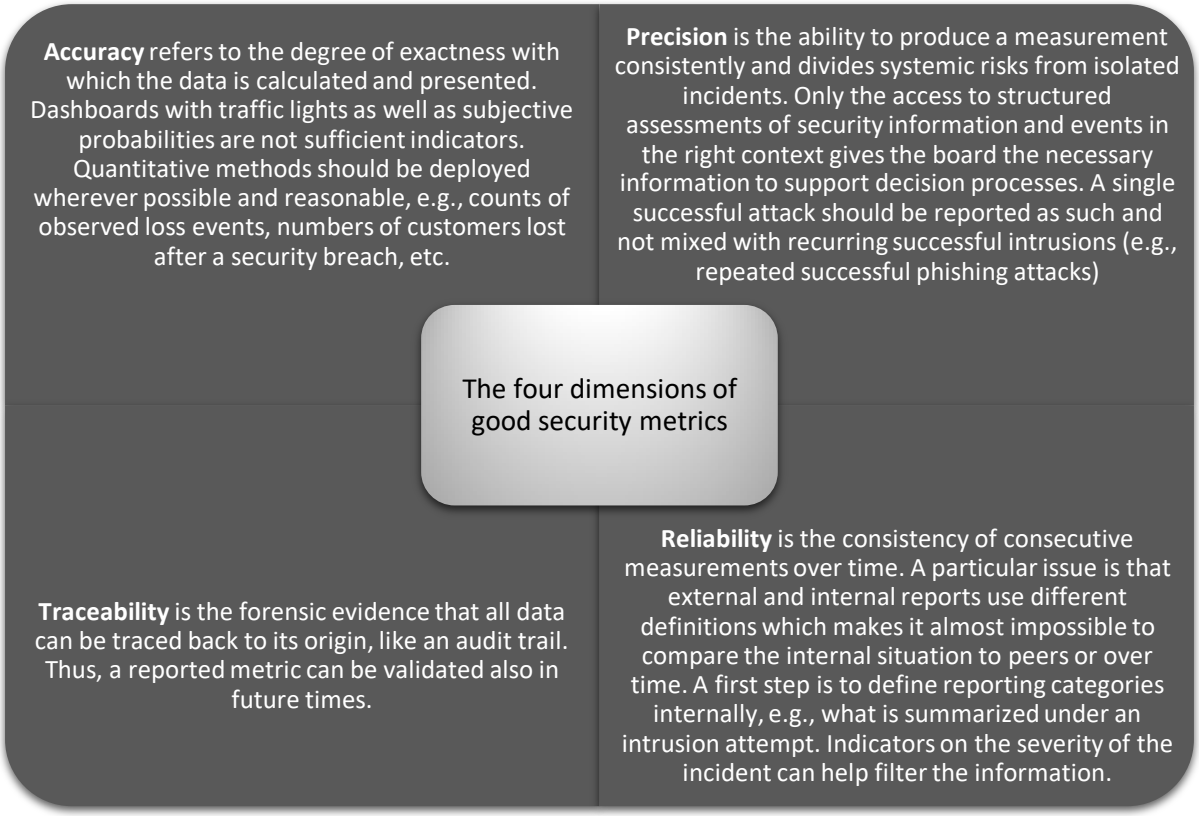
Organizational View
With respect to processes, the board is typically responsible for the oversight of the organization's internal control environment. The well-established COSO initiative defines this as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of

[12] See cyber claim reports including root causes from Ponemon, Netdiligence, or Bitkom.
[13] https://emstrasbourg.eu.qualtrics.com/jfe/form/SV_3vNrA2HcrJ9sB13 (Status February 2020)

objectives in …operations… reporting, [and] compliance…"[14]. Extending this definition to cybersecurity, GNDI suggests that boards inform themselves of specific operational, reporting, and compliance aspects of cybersecurity (including legal and regulatory requirements), using and adapting or supplementing as needed at least one recognized framework to do so. For a list of international recognized frameworks please see Annex A.

Frameworks and standards assist the board in assuring a completeness of relevant security issues reported. However, boards should be mindful of two potential failures according to the old - but still valid - motto: Do the right things and do things right. The business model and operations of a company define the focus areas for a risk-appropriate reporting, and boards need to make sure they report on the riskiest areas of operations and do not select simply the metrics that are readily available or easy to collect.

At the same time, the quality of the reporting is an equally important factor. Dimensional metrology knows four dimensions that characterize good metrics.[15]



For a complete overview, external data should be taken into account for the reports, as well as industry benchmarking, progress reporting on cyber security programs, training measures, etc.

Any oversight process should include both defense and response to ensure business continuity and resilience. While in 2015, enterprises were to a large degree independent

[14] Internal Control: Integrated Framework (2013). http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf

[15] See Georg Schaffner, L. (2017), Mastering Cyber-Resilience, in "Governance of Digitization: The Role of Boards of Directors and Top Management Teams in Digital Value Creation", Editor Michael Hilb, Haupt Verlag.

to choose an appropriate response to cybersecurity incidents, the European Commission in the EU and the SEC in the US launched in 2016[16] and 2018[17] concrete requirements on what data needs to be reported. These reports do not merely serve to improve the information flow but notably shall help overcome information asymmetry between corporate insiders and outsiders. The protection of investors and other external stakeholders requires transparency of the status of cybersecurity.

The risk appetite is an important factor in the risk management framework that each board needs to define. It guides the overall risk management strategies and influences decisions around risk avoidance, mitigation, transfer, or acceptance. Currently, mostly scenario-based impact assessments are used in the quantification process. In general, the risk management method for cyber risks should be aligned with methods in other risk areas to assess the cyber risks for the organization, benchmark them against other risks but also against other organizations. This process helps to define the risk appetite, and continuously improve the risk management strategy.

2.2.3 Technology

Board of Directors Internal View

With respect to *technology*, there is little standard guidance on the nature of board oversight. As discussed already under 2.2.1 'People', and to help enable oversight of the challenges of information and communication technology, GNDI recommends that boards consider knowledge of information and communication technology to be an important skill for the board to possess. Not all directors need in-depth knowledge and experience but understanding of technology - including digitization and cybersecurity - must be covered. This is particularly important for boards of companies where ICT is a core competence.

Organizational View

Areas of strategic focus and oversight should be the technology strategy and the role of technology for further business models, including the review of future opportunities and potential risks. In this context it is important to note that security might even be seen as an asset and potential positioning point.

At the same time, boards should keep an eye on current operations with respect to - for example - simplifying the information technology landscape and decommissioning old applications, as well as product strategies and the use of technology there. In this context, it is important for boards to stay on an oversight and steering level, and not to become operational.

To build a real-time response - a requirement for efficient security management - technology should be built into the DNA of business operations and thus become part of directors' assessment of enterprise risk.

One of the most difficult decisions in this respect is the question of the adequate level of resources and investments in security, security technology and resilience. Nevertheless, this is a decision the board needs to take in order to allow the organization to implement the agreed risk management measures, and invest into technology, people and preparedness. Internal and external benchmarks can help board members to take decisions in an extremely complex and fast-moving area.

[16] See https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[17] See https://www.sec.gov/rules/interp/2018/33-10459.pdf

2.2.4 Data[18]

Board of Directors Internal View

The board needs to be knowledgeable about laws and regulations that apply to the operations of their company. This relates for example but not exclusively to data protection laws. These laws are very specific for different countries and impact both technology or business strategy. Also, particular sectors (e.g., financial services, critical infrastructure) often have specific data and cyber security regulations that must be adhered to. Additional data-related regulations may be purely country-specific, for example data localization laws. The regulatory environment also defines the level of risk with respect to regulatory fines and penalties, whereas the legal environment largely influences liabilities towards other stakeholders.

Organizational View

More than half of the global enterprise value consists of intangible assets today.[19] The value of data increases the more organizations rely on it during value creation. Boards must put special emphasis on overseeing the categorization and safeguarding of these assets.

Only one out of two board members knows the value of data through the identification of its 'crown jewels', i.e., the information that is most valuable to an organization's operations and market success.[20] Furthermore, boards should request to implement a practical data management framework, following the GNDI Guidelines on the Corporate Governance of Data[21], listing and classifying any data assets that the organization either owns or processes. This ranges from data on intellectual property (e.g. a patent) to data of strategic nature (e.g. data on production costs) to sensitive data subjected to specific regulation (e.g. personally identifiable information). This data classification can then be used to guide specific protection measures for sensitive data, and to establish the appropriate processes that must be performed in order to comply with - for example - data protection laws and regulations. The loss or non-availability of data is the logical risk that cybersecurity measures help to protect.

Furthermore, specific emphasis needs to be placed on data relating to due diligence in any Merger & Acquisition scenarios or similar processes.

3. Conclusion & Outlook

Overseeing cybersecurity is a governance challenge in its own right for boards. This is due to the ubiquitous use of information and communication technology in an organization's operations and value creation, as well as the rapid technology change and development of external factors. The externalities include a so far unimagined computing capacity through Quantum Computing, an increasingly automated opponent using Artificial Intelligence that in return requires less and less knowledge on the part of the attacker himself, as well as new governance mechanisms where states increasingly take control of the internet entering, not only in a defensive, but also responsive mode,

[18] Data and information should be distinct: Information is what has been shaped into a form that is meaningful and useful to human beings. Data, in contrast, are streams of raw facts representing events occurring in organizations or the physical environment before they have been organized and arranged. We decided to use data as boards are required to provide meaning to it. See also GNDI paper on Data Governance from 2018.

[19] See Global Intangible Finance Tracker 2018, Brand Finance Institute, https://brandfinance.com/knowledge-centre/whitepapers/global-intangible-finance-tracker-gift-2018/

[20] https://emstrasbourg.eu.qualtrics.com/jfe/form/SV_3vNrA2HcrJ9sB13 (Status February 2020)

[21] http://gndi.org/ GNDI Guidelines on the Corporate Governance of Data

using Proactive Defense Mechanisms. The latter has an impact on the data and information that governments increasingly request enterprises to furnish, together with the cooperation expected in order to secure cyber market space. A good cybersecurity governance therefore will facilitate this interaction.

Additionally, the board faces another well-known challenge, the problem of the common grounds. Individual organizations tend to rely on others to raise the overall security of the market place. However, the overall industry is suffering from negative externalities such as insecurity and lack of trust. Thus, connecting with and learning from global partners is one good way to maintain currency in this dynamic field.

One important aspect of cyber resilience is to avoid getting locked into any single approach. As such, these global principles for cybersecurity oversight are not intended to be prescriptive. Factors that may influence cybersecurity oversight include the organization's industry, business model, strategy, locations, regulatory environment, and culture. Nor are these principles a substitute for the relevant laws, regulations and standards with which organizations must comply.
GNDI recommends that the board stays up to date with emerging advice from a variety of sources such as those cited in the annex.

Acknowledgements:
The authors would like to thank David Petersen for his editorial support.

Annex A

International Security Frameworks:[22]

- Control Objectives for Information and Related Technology (COBIT) from ISACA,
- ISO 27000 standards from the International Organisation for Standardisation (based in Geneva, Switzerland),
- Framework for Improving Critical Infrastructure Cybersecurity from the National Institute of Standards and Technology (NIST), under the U.S. Department of Commerce,
- Information Technology Infrastructure Library (ITIL), developed and owned by AXELOS in the United Kingdom and
- Information Security Forum (ISF)[23] Standard of Good Practice for Information Security.
- BSI Grundschutz Catalogue from the German Bundesamt für Sicherheit in der Informationstechnik

In addition to these general standards and regulation, there are specific industry standards for cybersecurity, notably:

- HIPAA or HITRUST (for health-care industry in the US)
- PCI-DSS for credit card acceptance (retail industry, finance industry)
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP)[24]
- U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities[25]

Cybersecurity and Data Protection laws and regulations are in constant change. 2018 saw for example the implementation of the EU General Data Protection Regulation GDPR, as well as a new Data Privacy Law in California, whereas in 2017 one of the main developments was the implementation of China's Internet Security Law.
Many law firms and other private companies keep track of these developments and some of the collections and comparisons are available to the public.

For a current overview of global cybersecurity laws and regulations see for example the following resource:

- https://iclg.com/practice-areas/cybersecurity-laws-and-regulations

For Data Protection laws and regulations, you might want to access one of the following resources:

- https://www.dlapiperdataprotection.com/index.html
- https://globaltmt.bakermckenzie.com/global-privacy-matrix

[22] For a comparison of these standards, see http://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf
[23] https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/
[24] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[25] https://scp.nrc.gov/slo/regguide571.pdf