WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

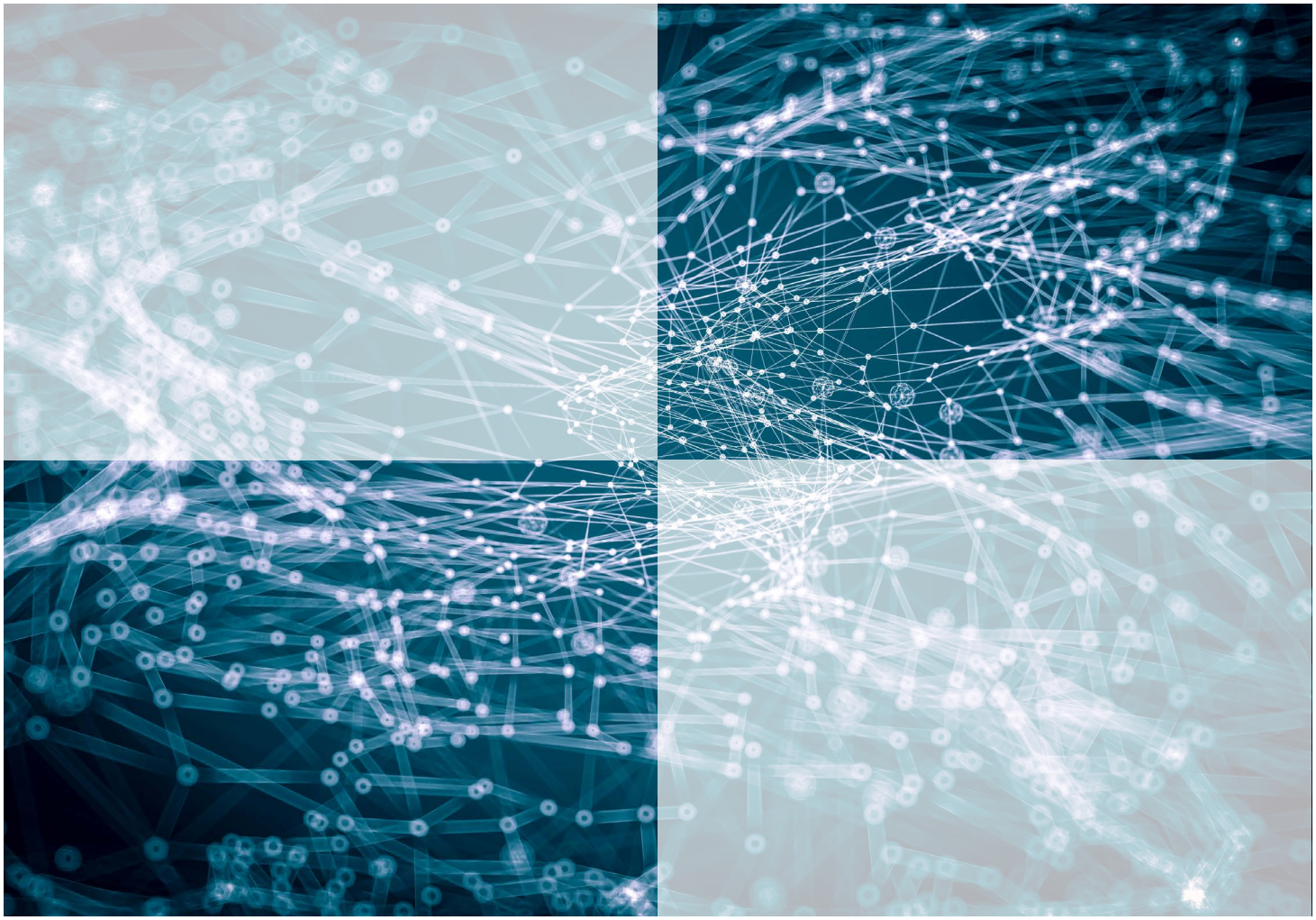
Future of Digital Economy and Society System Initiative

Advancing Cyber Resilience

Principles and Tools for Boards

In collaboration with The Boston Consulting Group and Hewlett Packard Enterprise

January 2017



Contents

World Economic Forum®

REF 110117

Preface

Cyber resilience and cyber risk management are critical challenges for most organizations today. Leaders increasingly recognize that the profound reputational and existential nature of these risks mean that responsibility for managing them sits at the board and top level executive teams.

Many organizations, however, do not feel that they are equipped with the tools to manage cyber risks with the same level of confidence that they manage other risks. Emerging leading practices have not yet become part of the standard set of board competencies.

Beyond individual organizations, cyber risk is a systemic challenge and cyber resilience a public good. Every organization acts as a steward of information they manage on behalf of others. And every organization contributes to the resilience of not just their immediate customers, partners and suppliers but also the overall shared digital environment.

Furthermore, continued technological adoption creates an urgency that cannot be ignored. In the coming years, several billions of everyday devices will be connected. As our virtual and physical worlds merge, the stakes are increased. This will require two things: 1) a significantly increased number of organizations adopting, sharing and iterating current leading practices; and 2) cross-sectoral collaboration to develop the new practices that will be required to deal with the unique attributes of managing cyber risks of physical assets. The second will be difficult without an informed body of leaders leveraging common tools and language.

For these reason, as part of the World Economic Forum's System Initiative on the Digital Economy and Society, the Forum has partnered with The Boston Consulting Group and Hewlett Packard Enterprise to develop an important new resource, *Advancing Cyber Resilience: Principles and Tools for Boards*. This report, which is the product of an extensive process of co-collaboration and consultation, has distilled leading practice into a framework and set of tools that boards of directors can use to smoothly integrate cyber risk and resilience into business strategy so that their companies can innovate and grow securely and sustainably. The Forum would like to thank The Boston Consulting Group and Hewlett Packard Enterprise for their leadership, the Expert Working Group for their contributions and all of the board members, chairs and CEOs who helped shape and adjust our efforts as we went along. This was truly a community effort, and we remain in debt for the energy and commitment of each member.

We hope that you will join us in using these tools to help advance our shared cyber resilience.

Rick Samans
Member of the Managing Board

1. Introduction

Cybersecurity features high on the agenda of leaders across all sectors, with business, governments and individuals rapidly taking advantage of faster, cheaper digital technologies to deliver an unprecedented array of social and economic benefits. The process of digitizing and connecting, however, introduces a range of new challenges.

The World Economic Forum's work on cybersecurity since 2011,[1] along with global interest in cybersecurity issues, has gone a long way towards ensuring that businesses and leaders are aware of the risks inherent in the hyperconnected world. For this awareness to lead to understanding and action, the Forum has engaged with a diversity of stakeholders to develop new ways to empower oversight boards to ensure that their organizations can thrive in this new era.

Two ideas have served as touchstones of our approach since the beginning of the World Economic Forum's engagement on the topic of cybersecurity and resilience. First, leadership has a vital role to play in securing resilience.[2] Second, that in order to effectively deal with cyber challenges, organizational leaders need a mindset that goes beyond cybersecurity to build a more effective cyber strategy and incorporate it into overall strategic thinking.

Cyber resilience is a leadership issue

Those at the forefront of digital security thinking share the Forum's view that cyber resilience is more a matter of strategy and culture than tactics.[3] Being resilient requires those at the highest levels of a company, organization or government to recognize the importance of avoiding and proactively mitigating risks. While it is everyone's responsibility to cooperate in order to ensure greater cyber resilience, leaders who set the strategy for an organization are ultimately responsible, and have increasingly been held accountable for including cyber resilience in organizational strategy.[4] For businesses, this means that cyber strategy must be determined at the oversight board level.

Going beyond cyber security

Speaking only about cybersecurity is insufficient if the challenges of digitalization are to be effectively met. Protection is important, but organizations must also develop strategies to ensure durable networks and take advantage of the opportunities that digitalization can bring. While there are many broader definitions of cybersecurity,[5] there is a difference between cybersecurity and the more strategic, long-term thinking cyber resilience should evoke. Additionally, since vulnerability in one area can compromise the entire network, resilience requires a conversation focused on systems rather than individual organizations.[6]

The Forum recognizes that integrating cyber strategy into business or organizational strategy is a significant challenge for any organization. The best way to combat the fear and uncertainty in this space is through tools and partnerships designed to develop understanding, create transparency, and find certainty in order to support much-needed action in this space. In our aim to normalize cyber risk, the Forum endeavours to make these risks as familiar to board members as any of the others risks they deal with on a regular basis.

This document provides the first in a continuing series of tools that leaders have called for in order to support their efforts at integrating cyber resilience into overall business strategy.

The challenge of cyber resilience

Countering cyber risk presents a significant strategic challenge to leaders across industries and sectors but one that they must surmount in order to take advantage of the opportunities presented by the vast technological advances in networked technology that are currently in their early stages. Over the past decade, we have significantly expanded our understanding of how to build secure and resilient digital networks and connected devices. However, board-level capabilities for strategic thinking and governance in this area have failed to keep pace with both the technological risks and the solutions that new innovations provide.

We have recognized a clear desire on the part of forward-thinking and visionary leaders to improve capabilities in this important aspect of strategy and governance. As recent events and predictions for the future show, now is the time to fill capability gaps with regard to cybersecurity and resilience at the highest level of any organization. The rapid pace of innovation and network connectivity will only increase in the coming years, making board-level action on this topic absolutely urgent. In the next few years, billions of new devices will connect to the internet as well as to corporate and government networks. These networked devices bring with them the threat of new risks to the enterprise and, more importantly, to networked systems that affect millions of lives.

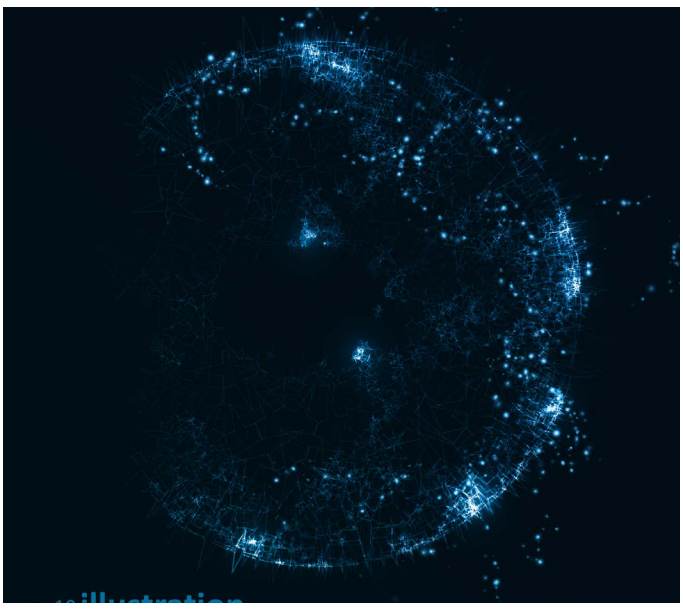
The systematic nature of these threats requires a different set of responses from policy-makers and business leaders. It is no longer sufficient to subject network security to a trial-and-error or low-oversight approach, as has generally been the default for many organizations.

Consider a well-publicized cyber-attack that occurred just as this report was in the drafting process. In the early morning of 21 October 2016, Dyn, a company that acts as a kind of switch-board operator for the internet as part of the Domain Name System (DNS), reported that many websites were inaccessible. Over the course of the day, users experienced the inability to access some of the most popular sites on the internet, including nytimes.com and Twitter. The reason for the outage was that Dyn's servers were undergoing a massive Dedicated Denial of Service (DDoS) attack – that is an attack that uses up all available connections to a website, thereby rendering it inaccessible to legitimate users – instigated by actors who had taken control of thousands of internet-enabled devices, including webcams and DVRs. [7]

Attackers in the Dyn DDoS attack took advantage of strategic choices that a variety of companies made in order to succeed. On the hardware side, manufacturers adopted a speed-to-market strategy rather than a security-by-design strategy, releasing a significant number of vulnerable devices that hackers could co-opt for DDoS attacks. Companies running websites made the strategic decision to concentrate their resources on one or a few DNS servers rather than spreading the load across several, which has implications for a site's resilience.[8] Considering practices across industries, it is likely that these decisions were made by default at a junior management level rather than after a thorough examination of their security and resilience implications at the senior management or board level.

If strategic guidance for decisions like the ones above is not set at the governance level, then an enterprise cannot ensure its own cybersecurity or resilience. Rather than implementing post hoc solutions to problems after they occur, boards and leaders must rapidly develop known capabilities to provide a sound baseline to surmount the challenges ahead.

The tools included in this report are meant to help strategic decision-makers at the board of director and CEO levels to effectively guide the security resources within their own organizations so as to effectively and resiliently pursue the enterprise's goals and ensure accountability for cybersecurity and resilience throughout the organization. These tools further recognize that resilience as a focus of strategy includes the actions an enterprise takes before, during and after an incident, thereby more fully mitigating potential threats.[9]



2. How to Use These Tools

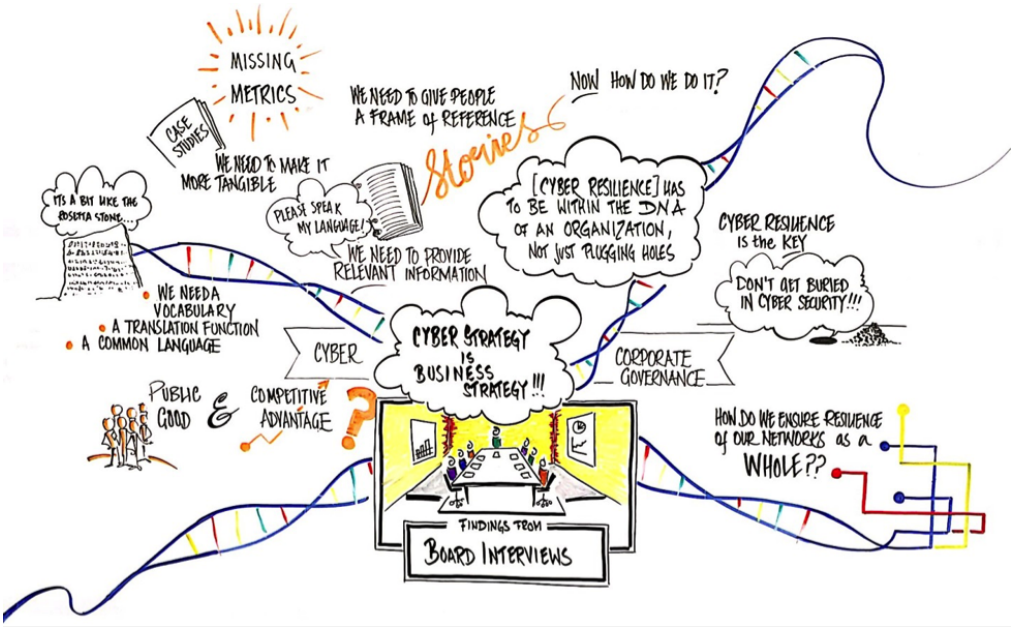
2.1 Board Governance and Cyber Resilience

The tools offered by the World Economic Forum are aimed at strategy and governance rather than at tactics or standards and management. Boards have a vital governance function, determining overall company behaviour and setting a company's risk appetite. For boards, action means effectively exercising oversight by asking managers the right questions to ensure that the boards' strategic objectives are met.[10] This function is no different in the area of cyber resilience.[11] By offering the following principles and tools, the Forum hopes to facilitate useful dialogue between boards and the managers they entrust with the operation of the companies to which they owe their fiduciary obligations.

Demand for board-level cyber resilience tools
Because of the seemingly novel challenges that cybersecurity and cyber resilience present to organizations, there has been a great demand for tools for leaders, especially senior executives and board members, in this area. The lack of a conceptual framework for boards of directors, especially, has been well noted in business scholarship[12] and by the World Economic Forum's own Community of Chairmen.

The Forum's Advancing Cyber Resilience project examines the gaps in cyber resilience tools by conducting a series of interviews with members of boards of directors from leading companies across several industries and continents. The results reveal that boards of directors consistently and increasingly see themselves as responsible for the overall cyber resilience of their companies. Board members, especially, are seeking tools to help them fulfil what they see as their fiduciary responsibilities relating to cyber resilience.

According to the results, 84% of board members surveyed agreed that better cyber resilience tools and guidelines are needed to support their oversight work.[13]



A brainstorming session on board principles with the World Economic Forum Working Group on Cyber Resilience

2.2 Using the Principles and Tools

The tools developed by the Forum are meant to help guide board action with regard to cyber resilience. This report contains three distinct, yet interrelated, documents all tied to the Board Principles for Cyber Resilience: Cyber Principle Toolkits; Board Cyber Risk Framework; and Board Insights on Emerging Technology Risks. It is recommended that board members and senior executives review the Board Principles for Cyber Resilience first in order to set governance expectations around cyber resilience. Boards should then use the Cyber Principle Toolkits to engage with management on the topic and validate the management's responses, as appropriate, with the Board Cyber Risk Framework and/or the Board Insights on Emerging Technology Risks.

Board Principles for Cyber Resilience – While supervisory boards developed a high awareness for cyber risk in recent years, they lack a common set of principles on how to act and how to push cyber resilience in their organizations. This framework of 10 principles is meant to enable board action and to aid in board recognition of their vital role.

Cyber Principle Toolkits – Each of the 10 Board Principles for Cyber Resilience is supported by a set of questions developed to foster constructive dialogue between the board and senior management on the topic of cyber resilience. These questions will aid the board in exercising their oversight role.

Board Cyber Risk Framework – Board Principle number six suggests that boards review their organization's cyber risks on a regular basis and ensure they are integrated in the review of other business risks. This Board Cyber Risk Framework contributes to the overall cybersecurity programme by providing the required informational basis to prioritize risk management actions within the programme.

Board Insights on Emerging Technology Risks – This document lays out guidelines and insights applicable to any organization dealing with business model shifts due to innovations related to the inevitable change in technology and risk. These insights and guidelines are meant to facilitate discussions between board-level stakeholders and executive teams, and help boards develop strategy for evaluating new technologies.

3. Cyber Resilience Principles and Tools for Boards

3.1 Board Principles for Cyber Resilience

Principle 1

Responsibility for cyber resilience. The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. risk committee) or new committee (e.g. cyber resilience committee).

Principle 2

Command of the subject. Board members receive cyber resilience orientation upon joining the board and are regularly updated on recent threats and trends – with advice and assistance from independent external experts being available as requested.

Principle 3

Accountable officer. The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

Principle 4

Integration of cyber resilience. The board ensures that management integrates cyber resilience and cyber risk assessment into overall business strategy and into enterprise-wide risk management, as well as budgeting and resource allocation.

Principle 5

Risk appetite. The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Principle 6

Risk assessment and reporting. The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber Risk Framework.

Principle 7

Resilience plans. The board ensures that management supports the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

Principle 8

Community. The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.

Principle 9

Review. The board ensures that a formal, independent cyber resilience review of the organization is carried out annually.

Principle 10

Effectiveness. The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

3.2 Cyber Principle Toolkits

Each of the Board Principles for Cyber Resilience below is accompanied by questions that allow for stringent self-assessment by the board and examples aimed at facilitating discussion with executive teams. This toolkit has been developed in order to allow board members to better exercise their oversight responsibilities.

Principle 1: Responsibility for cyber resilience

The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. audit committee or risk committee) or a new committee (e.g. cyber resilience committee).

The board should discuss their scope and responsibilities and the manner in which those responsibilities should be performed, including the structure and process of reviewing the management of cyber resilience. The board should determine whether it should take on cyber resilience responsibilities as a whole, or if oversight through an existing or new committee is preferable.

Questions for the board

1. Determine whether the board should retain primary responsibility or designate a committee.
   - Is the board able to devote the time to consistently discuss cyber resilience matters, or do time constraints only permit for periodic updates?
   - Does the board prefer to have discussions with management with respect to cyber resilience more frequently than regular scheduled board meetings?
   - Does the company's industry warrant special attention to cyber resilience matters, and do industry practices or peer companies suggest use of specific governance structures? Does a regulatory or other oversight body or obligation currently exist?
   - Would having a designated committee of specialized or interested members be beneficial to the review of the company's cybersecurity/ resilience strategy and the review of its management?

2. If a primary oversight by committee is preferable, determine whether an existing committee or new committee is appropriate and identify its responsibilities.
   - Does an existing committee have the capacity to manage the increase in workload necessary to effectively oversee cyber resilience?
   - Are there guidelines applicable to the committee and its primary responsibilities (consider formalizing through terms of reference or by adding to existing terms of reference)?
   - What performance measures are necessary for the committee to assist the board in its evaluation of the performance and benefits of the committee?
   - Can you identify individual board members who are qualified to become members of the committee?

3. Evaluate whether existing board members have the requisite skills and experience to effectively oversee cyber resilience and whether knowledge gaps warrant recruiting new members to the board.
   - What criteria for skills and attributes would be helpful for understanding cyber resilience?
   - How can the board include knowledge of emerging cyber resilience best practices, trends and regulations as criteria for evaluating future board members?

Principle 2: Command of the subject

Board Members receive cyber resilience orientation on joining the board and are regularly updated on recent threats and trends, with advice and assistance from independent external experts being available as requested.

Questions for the board

1. Board members should have a good understanding of cyber resilience and should be provided with cyber resilience orientation when they first join the board. Board members need a good level of general understanding about cybersecurity in order to understand and challenge the organization's specific approach.
   - Do new board members receive cyber resilience general orientation? (This should include a general training of the subject matter in order to have a foundational understanding of the subject matter and their oversight responsibilities over the subject matter.)
   - Are regular updates on general cyber resilience given? (The board should receive periodic training, e.g. annually, on cyber resilience and when significant threats or risks are identified that are industry specific in order for the members to have a good command of the subject matter. This regular/annual update may be accomplished by leveraging the enterprise's current awareness programme.)

2. Board members should receive orientation on the organization's cyber resilience and technology risk stance.
   - Are new board members given organization-specific cyber resilience orientation? (New board members should be brought up to speed on the organization's current approach with regards to cyber resiliency.)
   - Are board members provided with regular updates on the organization's cyber resiliency, risk exposure and risk stance? (Board members should receive updates as the risk stance changes or the threat environment changes.)

3. External experts should provide independent assessment of the organization's cyber resilience approach and benchmark the organization's capabilities.
   - Does the board sanction independent third-party assessments? (The board should be able to sanction third-party assessments and benchmark the organization's capabilities and maturity in order to gauge the organization's overall risk exposure and risk reduction strategy and plans.)
   - Does the board have advice from outside experts on cyber resilience? (Board members should request expert insight on the subject matter so that independent third-party perspectives are highlighted.)

Principle 3: Accountable officer

The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

Questions for the board

1. Roles and responsibilities should be clearly defined.
   - Is there a clearly assigned corporate officer in charge of cyber resilience? (The accountable officer should be clearly identified by management and accepted by the board; the accountable officer should have a strong command of the subject matter, and should have direct access to the CEO and board when needed.)
   - Does the accountable officer have sufficient independence from IT to provide oversight reporting on overall matters of technology and cyber risk? (Cyber resilience is a component of both business and technology risk. As such, the accountable officer has a direct reporting relationship with business and IT leadership and the board. This will ensure that risks are reported in a timely manner and appropriately. This also ensures that the cyber resilience and risk management strategies are aligned with, and in support of, the business strategy and direction.)
   - Is there a need for multiple lines of review and audit? (Should there be other means of oversight of the organization's cyber risk, such as internal audit, external audit, etc.?)
2. The accountable officer should have sufficient authority and influence.
   - To whom does the accountable officer in charge of cyber risk management report? What is the seniority of this officer? (Most organizations have identified cyber risk as one of their top risks. Because priorities may differ between IT departments' objectives to run IT cheaply and cyber risk management objectives to increase technology costs to manage risk more effectively, many organizations have established an accountable officer that has a sufficient separation from IT, can act independent of IT, but works collaboratively with IT to address the risk)
   - Are there clear communication and escalation pathways, processes and thresholds for resolution of conflict? (The accountable officer needs to have the capability to communicate and escalate to business leadership in matters that compromise the organization's cyber resiliency.)
   - Does the accountable officer have sufficient authority to drive a business and IT culture that builds suitable controls into the business and IT processes?
   - Who makes decisions on sourcing of cyber resilience activities/resources? (Business leadership should have oversight over cyber resilience activities and resources. The accountable officer should have direct line authority to execute. This ensures alignment between business goals and cyber resilience.)
3. The accountable officer should have sufficient resources
   - What percentage of the annual operating expenditure is spent on cyber resilience and how does this compare with industry norms? (Industries vary in the amount of operating expenditure dedicated to cyber resilience.)
   - Is there a dedicated cyber resilience budget and who owns it? (Cyber resilience should be considered as part of the overall risk profile of the organization. As such, cyber resilience budgets should be under the direct control of the accountable officer, with final authority from executive leadership, i.e. CEO, in order to address the organization's risk exposure and not compete with other support functions.)

- Are there other budgets contributing to cyber resilience, such as for IT or risk? (The challenge of having cyber resilience budgets spread across various departments is that competing priorities may reprioritize such budgets, and the true cost of cyber resilience may not be obtainable.)
- Are metrics regularly benchmarked against peers within the organization's own industry and beyond its industry? Such metrics might include:
  - The percentage of the organization's annual revenue that is spent on cyber resilience
  - The size of the cyber resilience team? (e.g. number of cyber resilience full-time equivalent (FTE) per 1,000 employees or per 1,000 IT employees)
  - The % growth in the cyber resilience budget/resource over the past three years
  - The planned % growth in the cyber resilience budget/resource for the next three years
  - Maturity of control operations

Principle 4: Integration of cyber resilience

The board ensures that management integrates cyber resilience and cyber risk assessment into overall business strategy, into enterprise-wide risk management, as well as budgeting and resource allocation.

Questions for the board

1. Are cyber risks and cyber resilience evaluated by management using the same risk framework as other risks?

2. How does the organization govern cyber risks?
   - Is there a senior management-led risk committee that evaluates cyber risk?
   - Is there a board-level risk committee that evaluates risks across the organization, including IT risk, cyber and third-party risk?
   - Is cyber risk a standing agenda item for board meetings with briefings from the chief information security officer (CISO)?

3. How involved is the board in reviewing and approving enterprise resilience strategy and associated risks?
   - Does the board review annually the organization's strategic plan? As part of this plan, does the board also approve the operating budget for cybersecurity and key cybersecurity strategic priorities?
   - Is the board briefed periodically on how the organization is meeting its business strategy, including around key cybersecurity priorities?

4. Is cyber resilience awareness incorporated at all levels and operational elements across the enterprise?
   - How are resources allocated to make this possible?

5. Has the board reviewed the cyber resilience strategy, including whether key cybersecurity-related risks have been adequately assessed, prioritized and mitigated, and whether the board or committee has evaluated the organization's cyber insurance coverage?

Principle 5: Risk appetite

The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Questions for the board

1. Has the board been given the opportunity to understand the context of cybersecurity risk appetite and how appetite may be different for different company objectives when balancing risk and the operational cost/impact of cybersecurity measures?

2. Does the board have visibility of how the stated risk appetite is being applied in business decision-making?

3. Where risk tolerances differing from risk appetite have been accepted because of necessity, are these presented back to the board on an annual basis?

4. Is risk examined on a case-by-case or business line basis as well as in the aggregate to ensure understanding of enterprise-wide risk?

5. Is the board given the necessary shareholder, regulatory, customer and other societal external perspectives to allow them to set the cyber risk appetite?

6. Does the board understand the real impact of cyber risk in business terms such as business disruption or impact on product/service quality or reputation?

7. Where their business supports critical national infrastructure or other national interests, does the board have a strategy to deal with broader governmental and societal stakeholder expectations?

8. Does the board hold the accountable officer responsible for understanding the cyber risk in advance of undertaking new business ventures (e.g. mergers, acquisitions, joint ventures and divestments) or new products or technologies?

9. Does the accountable officer brief the board on changes in customer, staff or regulatory expectations or other external factors such as incidents or the views of society as a whole which may change the risk appetite?

(See Appendix 3 below for an illustration of how this principle may be put into practice. For more information on determining cyber risk appetite, please see the accompanying document Board Cyber Risk Framework on page 15.)

Principle 6: Risk assessment and reporting

The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber Risk Framework.

Questions for the board

1. Is the risk reporting to the board balanced and does it reflect the present and potential future situation?

2. Is the board briefed on strategic and operational actions not taken (past or contemplated) because they exceeded the business cyber risk tolerance?

3. Is there an evaluation of cybersecurity culture and awareness among employees and are resulting action plans communicated to the board?

4. Does management highlight to the board the differences in security between the digital systems that are involved in the operational aspects of the business (e.g. financial transactions in a bank, manufacturing control systems, medical devices in a hospital, etc.) as opposed to the classical IT systems that are used for word processing, accounting, inventory control, employee management, etc., and are any differences and overlap in the approach to securing these systems reported to the board?

5. Does management communicate potential physical, operational, human life, legal and reputational damage that may accompany a cyber incident to the board?

6. Does management communicate current industry specific threats/threat patterns/trends to the board, including risks relating to associated third parties (e.g. vendors)?

7. Is the board comfortable that the organization is able effectively to manage any cybersecurity vulnerabilities and required updates that may arise as a result of planned changes to its business or technology?

Principle 7: Resilience plans

The board ensures that management support the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

Questions for the board

1. Does the organization have a basic set of cyber resilience plans in place, including business continuity, communications, disaster recovery and incident response plans?
   - Is primary accountability for these plans placed sufficiently high in the organization to reasonably ensure appropriate executive level attention and influence?
   - Do the plans incorporate cross-functional management representation to reasonably ensure that key perspectives and needs are incorporated (e.g. legal, sales and marketing, media relations, government relations, investor relations, facilities management, corporate security, etc.)?
   - Who in management is accountable for understanding legal and regulatory requirements in jurisdictions where the company operates globally, and how are these requirements incorporated in the cyber resilience plans?
   - Is the board satisfied with the frequency of update of the plans?
   - Is the board satisfied that plans have been tested frequently enough using table-top exercises or some other systematic simulation and that any lessons learned from testing been actioned?
   - Is the board satisfied by the organization's response during an actual incident or event and that any lessons learned have been incorporated into the plans? How has management incorporated lessons from other organizations that have faced cyber events into its own plans?
   - What is the policy regarding the board's role relative to cyber resilience plans, and how has this been communicated to the board and to executive management? Is the board's role explicitly incorporated into the overall response plans?

2. Are KPIs used to measure the effectiveness of existing cyber controls and any improvement?

3. Does the board ensure that management has adopted an appropriate approach to cyber resilience (e.g. detect and respond)?

Principle 8: Community

The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.

Questions for the board

1. Has the accountable officer identified which organizations the business should collaborate with externally?
   - Who are those entities (e.g. suppliers, law enforcement, regulators, policy/standard bodies)?
   - How were they selected?
   - How does management ensure sensitive information is appropriately shared with trusted individuals/organization and protected?
   - Have agreements been established in advance for sharing between organizations (e.g. non-disclosure agreements)?

2. Has the accountable officer identified how others in the industry are collaborating?
   - Have industry best practices been identified?
   - Have industry sharing forums been identified?

3. Has the accountable officer identified the potential benefits of collaborating, for example:
   - Benchmarking to identify best practices and gaps in security compared to others?
   - Sharing of indicators of compromise to enable better identification and prevention of attacks?
   - Sharing of information about attackers' tools, techniques and practices to allow for better protection and defense?
   - Sharing of industry incident trends to allow for improvements in control?
   - Sharing investment costs and innovation to build new controls?

4. Have potential liabilities resulting from each collaboration been identified and managed?
   - How does collaboration align with the goals and values of the organization?
   - What are the risks associated with collaboration?
   - What is the monetary cost of collaboration?
   - What elements of collaboration will the organization need to make public?

5. Has the accountable officer ensured that appropriate parts of the organization collaborate internally (e.g. with other business units) to assess whether similar threats have been detected by them and to coordinate the response or implement a common set of controls to centrally address and manage the risk?

Principle 9: Reviews

The board ensures that a formal independent cyber resilience review of the organization is carried out annually.

Questions for the board

1. How are independent reviewers selected?
   - Is there a definition surrounding what constitutes an independent reviewer?
   - How are the independent reviewers audited to ensure they are qualified for the review?
   - How often does the board select an independent reviewer?
   - How long does the review take?
   - What is the cost of the review and implementation of any changes?
   - What are the risks associated with participating in the review and how are they mitigated?

2. Has the accountable officer appropriately scoped the review in conjunction with the head of technology and the CISO? For example, it should include:
   - A focus on top IT and security risks, not all risks
   - An update on other IT risks, including third-party risks like privacy and IP protection, as well as risk from components
   - Key risk assumptions and controls to mitigate risks
   - Key results from testing activities (controls, penetration, vulnerability, etc.)

3. Has the board reviewed the process and plan to implement any changes following the review results?
   - Are these changes properly documented and reviewed throughout the year?
   - Are changes made throughout the year?
   - How are executives in the organization held accountable for the correct implementation of the changes needed?

4. Does the organization have a process in place to evaluate cyber resilience with third parties that may control information or technology assets?
   - Does the organization have a good understanding of the assets and offerings that they do not control?
   - Does the organization have strong contacts at each third party in place to ensure issues are resolved quickly?
   - What auditing capabilities does the organization have in place with third-party partners?

5. Are internal and external audits of the organization's cyber preparedness performed periodically and independently reported to the board?

Principle 10: Effectiveness

The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement

Questions for the board

1. Does the board periodically review its own composition, including:
   - Experience and skills of its members in the cyber resilience area?
   - Overall size and whether the addition of a cyber resilience expert would significantly improve cyber resilience oversight and the meeting of the board's fiduciary duties?
   - Whether cyber resilience is sufficiently part of the process for identifying and selecting new board candidates?

2. If the board has delegated responsibility for oversight of the risk to a committee, has the board reviewed the:
   - Process by which the board delegates work to the committee?
   - Size and composition of the committee?
   - Quality and frequency of communication between the committee and the full board?

3. Has the board evaluated its independence from management, including:
   - Evaluation based on regulatory requirements?
   - Evaluation of the practice and philosophy of the board/applicable committee in appropriately balancing, supporting and, at the right times, challenging management?

4. Has the board reviewed the timeliness and quality of the information provided to it, including:
   - Access to management at different levels, external advisors, reports and presentations that are relevant and focused at the right level of detail?
   - Management's responsiveness to appropriate requests for information?

3.3 Board Cyber Risk Framework

As laid out in the Cyber Resilience Board Principles, principle six suggests that boards review their organization's cyber risks on a regular basis and ensure they are integrated in the review of other business risks. The assessment of cyber risk contributes to the overall cyber security programme by providing the required informational basis to prioritize risk management actions within the programme.

To be more specific, boards need to understand and evaluate:

- The current risk tolerance/appetite of the organization in the context of the organization's cyber risks and business strategy
- Cyber risks that the organization faces – not taking into account any risk management or mitigation actions at this point in time
- Risk management or mitigation actions suggested by the executive team and associated costs
- The residual cyber risk portfolio after risk management or mitigation actions and how it compares to the risk tolerance/appetite

These steps are described in the subsections below: analysis of the cyber risk portfolio; guidance on the application of this framework; and an outlook on risk benchmarking. This piece of work is augmented by the Board Insights on Emerging Technology Risks, which addresses the issue of risk arising from new technology (e.g. the Internet of Things).

Cyber risk review by the board

To establish the review of cyber risk as a regular activity, the ultimate goal needs to be an integration of the cyber risk discussion into the discussion of overall operational risk. Today, though, cyber risk still is a relatively new risk and the level of knowledge on cyber risk is low

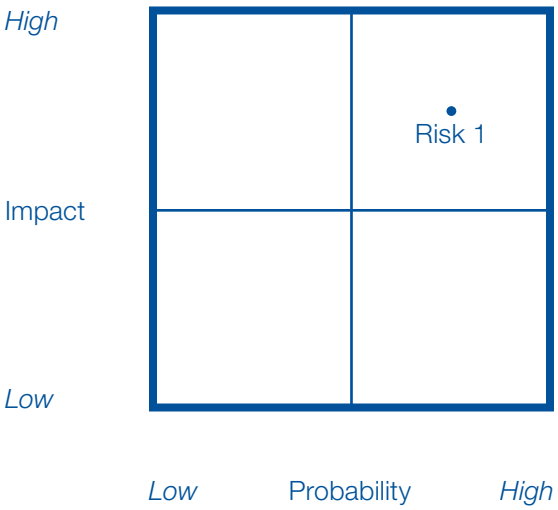
compared to other operational risks. In order to increase the understanding of cyber risk, an explicit discussion on the board level is desirable for the near future, prior to combining it with other, better understood operational risks.

The four issues discussed below should be of particular interest to the board when it reviews the cyber risks applicable to an organization:

1. Cyber risk tolerance level/risk appetite
The board needs to align the overall risk tolerance level with the executive team. Defining it requires a joint effort by the board and the executive team with the board representing the long-term sustainability needs of the shareholders it represents. This discussion will take into account future strategic events, the expected market environment, as well as the competitive position of the organization. It needs to consider the organization's ability to absorb materialized risks and will balance the value of tolerated risk and the potential business upside that comes with it. This accepted risk of doing business includes all different risk types, traditional risk types like credit risk and new risk types like cyber risk. Subsequently, the risk tolerance level for each type of risk, and cyber risk in particular, needs to be determined.

2. Cyber risk identification prior to management actions
The identification of an organization's cyber risk portfolio will be provided to the board by the executive team. The portfolio should take legal, operational, financial, reputational and strategic considerations into account. It will usually consist of a meaningful aggregation of cyber risks along the two dimensions of risk probability and risk impact with each dimension ranging from high to low levels. Any particular risk may thus be represented as a point on a traditional 2x2 matrix, as illustrated by Risk 1 in the figure below.

Figure: 2x2 matrix to depict results of risk assessment



Typical questions boards need to ask include:
- Have all relevant cyber risks been identified? The board might wish to conduct its own risk assessment to answer this question. It might rely on the framework provided in subsection 3 and engage independent advisers to assist them. See also Board Principles 5 and 6, above.
- Based on the board's experience and relevant information, does it believe the assessment of risks is accurate? Are estimates of probability and impact in line with the board's perspective?
- Does the assessment of a risk include a perspective on the organization's capability to recover from that risk should it materialize? How long would it take to recover and at which cost is associated with recovery? See also Board Principle 7, above.

3. Risk management actions
After reviewing the cyber risks presented and aligning on their probability and impact, the board needs to evaluate the risk management actions proposed. Risk management actions are bundled in the organization's cybersecurity programme. Possible types of management actions include:

- *Mitigation actions* – Risks can be mitigated by technical, administrative, physical, and organizational controls or capabilities. Examples include:
  - Risk controls targeting people and culture, such as employee training, or awareness campaigns
  - Organizational/procedural risk controls, such as contractual provisions, policies, governance, legislation and sharing of intelligence across industries, or mutual aid and coordinated responses (this category includes administrative risk controls, such as asset inventories and risk categorization)
  - Technical risk controls, such as firewalls, detection capabilities, respond/recover capabilities and physical access controls (SANS provides a high-level overview of technical mitigation actions in its CIS Critical Security Controls publication)
  - Each mitigation action has an associated cost and expected reduction of risk

- *Transfer actions* – Transfer of risk, for example via insurance contracts in risk markets

- *Acceptance actions* – Risks that are minor or cannot be mitigated in an efficient way can be accepted, i.e. they remain as a cost of doing business and are not addressed by controls.

- *Avoidance actions* – Risks that are outside of the risk tolerance/appetite of the organization should most likely be avoided (e.g. a product being withdrawn from the market)

The board needs to understand which actions are taken and which are consciously not taken. It needs to challenge whether the executive team has set the right priorities and risk thresholds, and whether the risk actions taken are the most efficient choices. This analysis requires consideration of any correlations between risks in the portfolio as well as the sustainability need of shareholders.

Another question that needs to be asked in this context is around resources and budgeting. The board will wish to assess whether the overall resource/budget allocation allows for an optimal treatment of the risk portfolio. Too few resources will result in a significant residual portfolio and therefore in a significantly higher risk exposure post risk controls. On the other hand, if extensive resources are allocated to inefficient risk management actions, i.e. the ratio of resulting risk reduction to cost will fall significantly.

The board will require the executive team to propose a structured set of KPIs/metrics to measure the effectiveness of implemented risk management actions. These KPIs/metrics will be included in a report/dashboard that the executive team presents to the board on a regular basis.

4. Residual risk portfolio
Applying the risk management actions to identified cyber risks will change the actual risk exposure of the organization and result in residual risks. The board needs to ensure that the total value of the residual portfolio – plus the cost of risk mitigation, avoidance and transfer – is lower than the risk tolerance level as outlined above. This residual portfolio is the cost the board accepts as a representative of the shareholders and/or other stakeholders. The board should require management to put the residual cyber risks into the context of the overall (operational) risk portfolio (risk register) of the organization, to update it regularly, and to further drive the normalization of cyber risk and its management.

Board cyber risk assessment framework
The following sections outline a high-level framework to support boards with their own assessment of cyber risk to validate the risk assessment provided by the executive team.

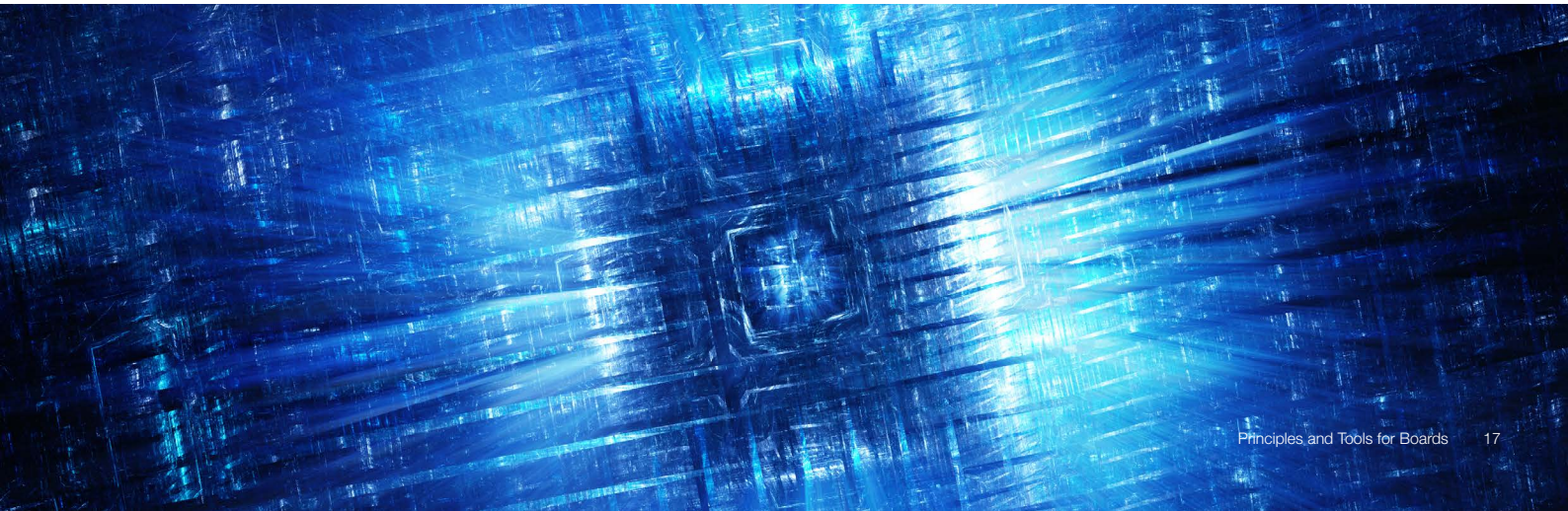
Common cyber risk frameworks
A large variety of frameworks for risk assessment and management exist, many of which with a long history and a track record of success.[14] The majority of these frameworks address the specific needs of executive officers responsible for cyber resilience and those of their operational teams. Many of them are very detailed complicating a quick high-level access to key concepts which would be required for board-level strategic discussions.

Frameworks commonly used by organizations include, but are not limited, to:
- The ISO/IEC 27k series of standards
- Control Objectives for Information and Related Technologies (COBIT) by ISACA
- NIST Special Publication (SP) 800 Series
- Federal Information Processing Standards (FIPS) by NIST
- OCTAVE Allegro
- Payment Card Industry Security Standards Council (PCISSC)

The *Framework for Improving Critical Infrastructure Cybersecurity* by NIST provides an overview for most of them as does ENISA's *Inventory of Risk Management/Risk Assessment Tools*.

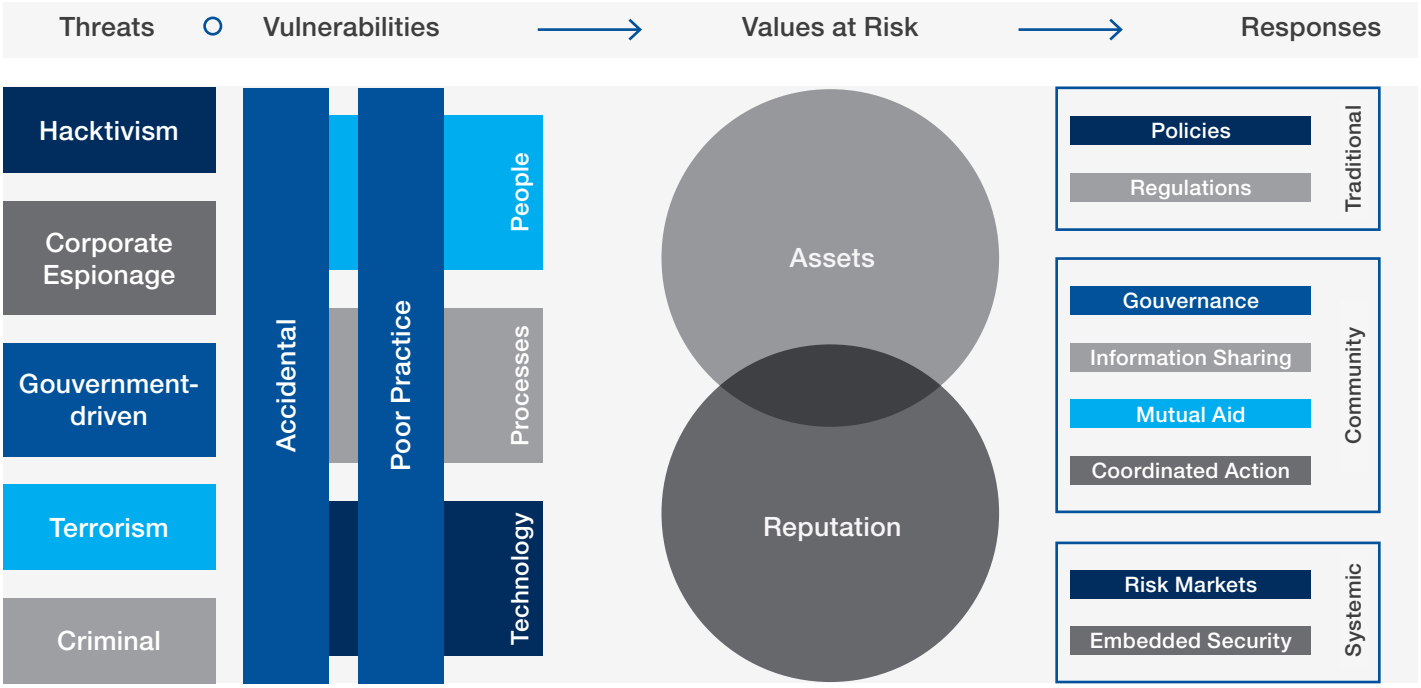
These frameworks use different taxonomies and methodologies for their particular area of application – yet all of them share common elements and approaches. The high-level concepts of these frameworks (see following table for examples) have been considered while updating the Forum's framework and special attention has been paid to the avoidance of conflicting concepts.

	ISO/IEC 27k series of standards[15]	COBIT[16]	NIST SP 800 series[17]	OCTAVE Allegro[18]
Description	De facto standard for risk frameworks	Comprehensive IT risk framework, including governance	US standard cyber risk framework	Mainly used in addition to other frameworks
Key concepts	Context, assessment, treatment, monitoring and review, communication	Risk scenarios, risk map, risk appetite, risk responses, risk action plan	Threat source, threat event, vulnerability, security controls, adverse impact	Risk drivers/ criteria, asset profiles, threats, threat scenarios, risks, response approaches



Previous cyber risk framework by the Forum

The Forum's original Cyber Risk Framework dates back to its 2012 publication *Pathways to Global Cyber Resilience*, which comprises the key elements of threats, vulnerabilities, values at risk and responses. It was intended as a first step towards the quantification of cyber risk.[19] This framework is the foundation of the Forum's current work on board empowerment in cyber resilience.



Updated board cyber risk assessment framework

The following framework builds on the Forum's work, adapting it to state-of-the-art cyber strategies. A later section presents a self-assessment questionnaire that helps with applying the below framework to individual organizations. Instructions on how to apply the framework will follow in a subsequent section.

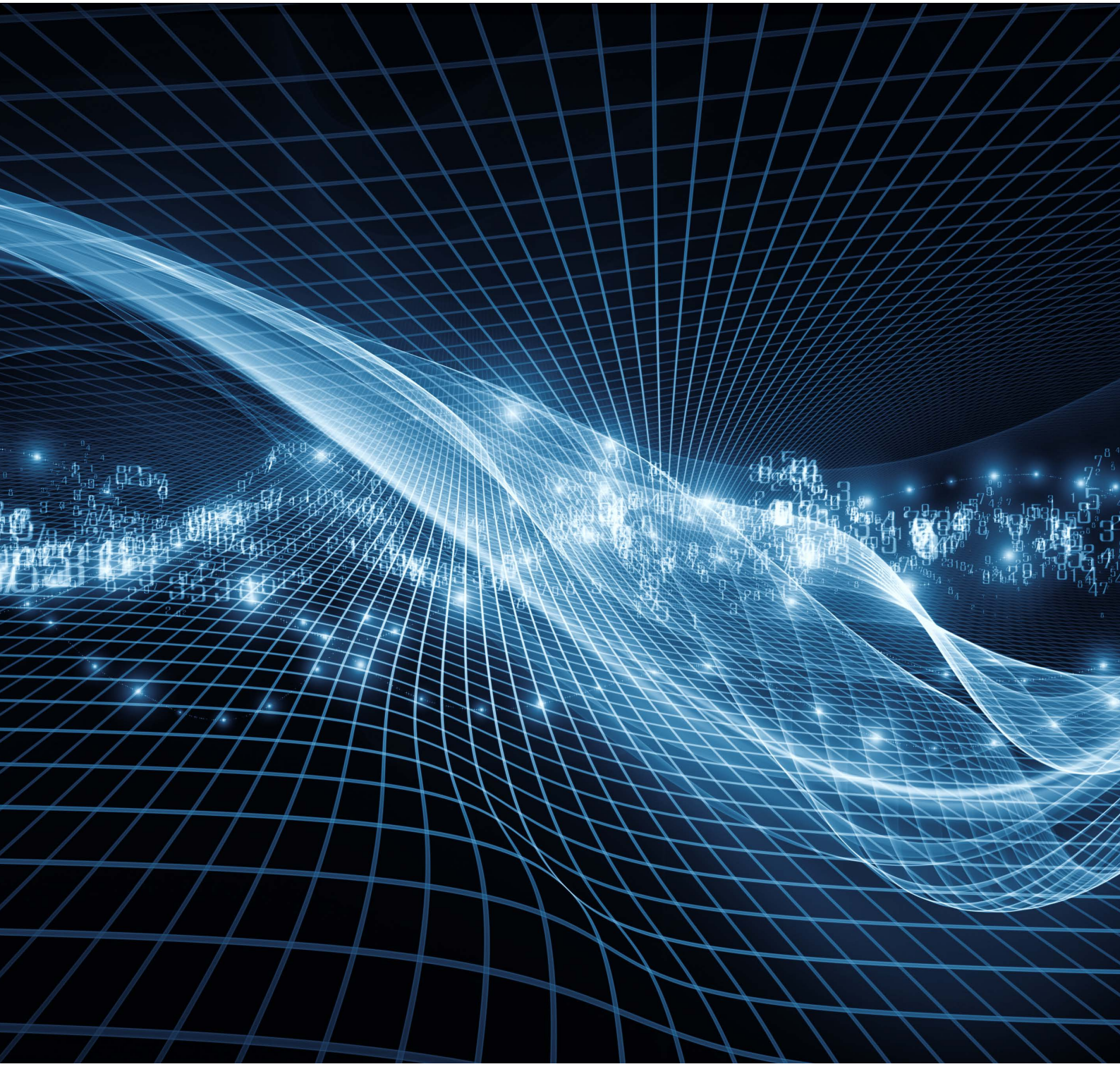
Cyber Risk

Cyber incident impact			X	Cyber incident probability		
Assets at risk[1]	X	Loss of …		Vulnerabilities	X	Threats[2]
Intangible assets — IP — reputation — compliance		confidentiality		People and Culture		Disgruntled Customers Human Error Supply Chain Partner Action
Tangible assets — financial — physical — production systems — infrastructure		integrity and accountability		Processes and Organization		Insider Action Hacktivism Crime Sabotage
Greater good — safety of life and health — civil liberties — individual privacy		availability		Technology and Infrastructure		Corporate Espionage Terrorism State Action Force Majeure

[1] Examples for assets
[2] Selection of examples, sorted in ascending order of available resources

The updated Board Cyber Risk Framework is intended to support structured discussions on cyber risk and to allow the board to periodically apply the framework to validate the risk reported by the executive team. It defines risk as the combination of the probability of an incident within the realm of information systems and the impact of this incident on assets. Cyber risks are a business issue with technical aspects. Cyber risk can impact and can be impacted by all areas of the organization and even beyond by other parts of the value chain.

In the framework above, the impact of a cyber incident results from a loss of one or multiple qualities of an asset – be it a loss of confidentiality, integrity, availability, or accountability. The assessment of vulnerabilities and threats indicates the probability of a cyber incident and should preferably be quantitative – the risk framework can be used for guidance on the quantification. In case this is not feasible, a qualitative assessment using a "low/medium/high" scale can be used to prioritize risk. Subsequent sections will provide a self-assessment tool and support on the application of the framework.



Risk examples

Some examples of risks (and their associated assets, losses, threats and vulnerabilities) include:

Risk	Asset at Risk	Loss of	Threat	Vulnerability	Impact and Quantification
Loss of integrity and accountability of financial data	Financial Information or systems: e.g. transfer orders	Integrity and accountability	Insider crime	Process: Lack of change (dual) control enables employee to manipulate financial systems or data	– Direct financial fraud loss minus insurance recoveries – Direct cost to investigate incident (internal and external resources) – Reputation risk, impact to sales, renewals, market share and share price – Penalty fees and fines
Loss of confidentiality of customer data	Customer data, reputation	Confidentiality	Phishing attack from criminal organization	People: Untrained and unaware employee is contacted and sends out customer data via email	– Direct cost to investigate incident (internal and external resources) – Cost per record for customer communication and identity theft monitoring – Reputation risk, impact to sales, renewals, market share and/or share price – Regulatory penalty fees and fines
Loss of availability of production systems	Production output and potentially revenue from that output	Availability	Distributed Denial of Service Attack (DDoS) due to hacktivism or perpetrated to enable fraud	Technology: Lack of controls to limit the impact of a DDoS attack or recover following such an attack	– Direct cost to investigate incident (internal and external resources) – Cost of production outage; e.g. SLA penalty, loss of revenue (interchange fees) due to lost transactions or fines, penalties or lawsuits due to missed trades – Further impact to reputation and loss of future business – Reputation risk, impact to sales, renewals, market share and/or share price
Loss of confidentiality of intellectual property	Intellectual property, e.g. engineering plans	Confidentiality	Cyber crime	Technology: Security patches are not applied, enabling an external attacker to exploit a known software vulnerability	– Direct cost to investigate incident (internal and external resources) – R&D cost to develop intellectual property to the point of theft and/or future lost market share/sales due to loss of IP – Legal fees related to IP infringement/ litigation
Loss of integrity of control systems	Health and safety Physical and technology assets	Integrity and accountability	Sabotage	Technology: Lack of anti-malware controls allows attackers to deploy command/control malware designed to take control of critical systems	– Direct cost to investigate incident (internal and external resources) – Injuries and/or fatalities – Liability and financial impact of above – Cost of production outage – Cost of fines and penalty fees – Reputation risk, impact to sales, renewals, market share and/or share price

Self-assessment questionnaire for boards
This short self-assessment questionnaire for use by the board is meant to allow for a structured analysis of each of the building blocks of the Board Cyber Risk Assessment Framework. Naturally, it stays at a high level and intentionally focuses on those elements that are of highest strategic importance. Recommendations regarding the application of this questionnaire can be found in a subsequent section of this report.

Step 1: Assets
The board needs to develop a perspective on the organization's most important assets. This inventory typically includes hardware and software systems, networks, infrastructure to operate these systems, information, and people or external resources. It should contain some administrative information, for example, on the age of technology assets and therefore the technical debt. For a board-level assessment, assets will typically be aggregated into asset classes.

Typical questions to ask include:
– Which assets could potentially cause harm to peoples' health or life if they were attacked successfully?
– What are the business objectives in order of priority with respect to value creation?
– Which assets are most critical to our value creation today? In the future? What are the "crown jewels" of our organization?
– Which assets would be likely to create significant losses if unavailable to us or manipulated unnoticed?
– Which assets are of highest value to external parties like competitors, clients, or the general public?
– Which assets are most important for our reputation?
– Which assets are most relevant for our regulatory compliance?

This high-level asset inventory can be compared to the asset inventory presented by the executive team. The latter will naturally be more detailed and comply with best practices such as the asset inventory control required by the ISO/IEC 27001 standard's information security management system.

Step 2: Losses of asset qualities and their impact
In a next step, the potential impact of an incident needs to be assessed. Therefore, each top asset (class) as identified in the previous step is analysed along the three loss dimensions as outlined in the matrix below.

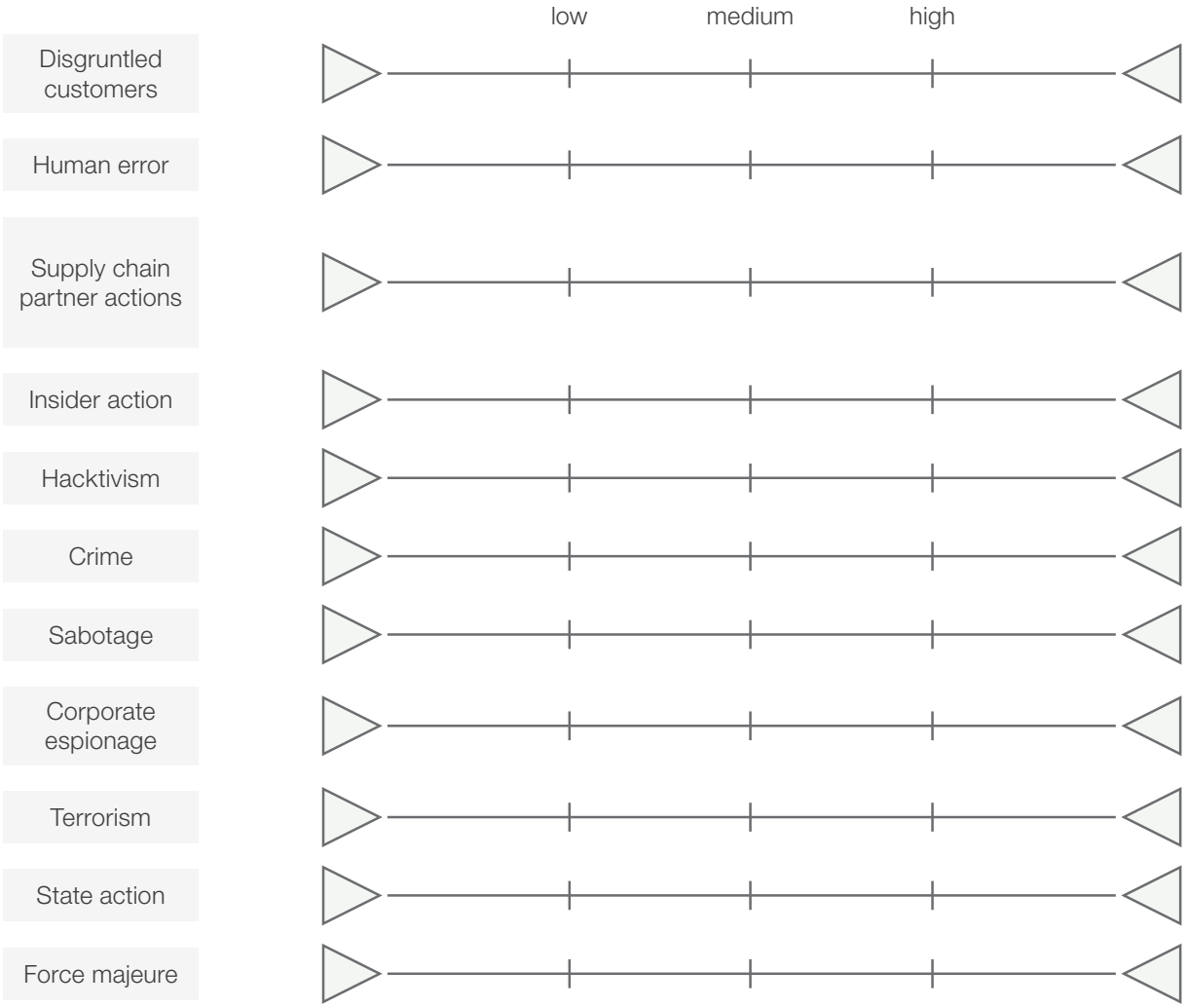
Confidentiality		Loss of…		
		Integrity and Accountability	**Availability**	**Confidentiality**
Asset class	**Customer data**			
	Financial data			
	IP			
	Production and control systems			

For each cell of the matrix, the impact of the particular loss is determined. It is recommended to take all associated cost into account, including:
– Cost directly associated with the incident (e.g. loss in cash due to manipulated transaction data or loss in sales)
– Cost indirectly associated with the incident (e.g. from a damage to the organization's reputation or cascading and tail risk)
– Cost of investigating the incident (e.g. cost of external advisors and reporting the incident in line with regulations)
– Cost of recovery from the incident (cost for establishing regular operations, reinstalling back-ups, repeating research to build IP, fixing vulnerabilities)
– Fines and/or regulatory penalty fees

Now that the potential losses and their impact are determined, the probability of an incident needs to be explored to determine the expected value of the risk portfolio.

Step 3: Threats
The probability of an incident results from a combination of threats and vulnerabilities that can be exploited by these threats. So for each asset/loss combination identified in steps 1 and 2, the threats and vulnerabilities that could lead to this incident need to be identified and their probability needs to be assessed.
In general, it is perceived that boards have a high level of awareness and understanding of the relevance of general and cyber threats to their business. Their sound understanding of their business's strategy, the organization's position towards competitors, and business events with negative public resonance supports this assessment.

The board should consider the threats shown in the figure below in the context of current and future business and rate their relevance to the organization on a scale from low to high. Each grade on the scale shown in the figure can be assigned to a degree of likelihood that a particular threat actor will launch an attack against the organization. This analysis should take into account the expertise or resources known to be available to the threat actors.



On an operational level, the executive team will ensure that the organization has a continuous cyber threat intelligence process that observes threats to the organization, either by leveraging third-party commercial sources, or with processes, technologies and expertise within the enterprise. This information can be validated against the board's high-level perspective.

Step 4: Vulnerabilities
The combination of threat level and vulnerabilities indicates the probability of an incident to materialize. Vulnerabilities come in three categories:
- People and culture
- Processes and organization
- Technology and infrastructure

While for the latter category there are, and should be, automated test tools that are run continuously by operational teams, the first two categories are where the board can and should take a perspective.

People and culture
Typical questions to be raised around this category of vulnerabilities include:
- What is the level of awareness and training of our employees?
- Are our employees assured of what is secure and what is not by making it explicit?
- How easy would it be to exploit them to gain access to information, alter data, or make it unavailable?
- Do we have a cyber resilient culture in which cyber resilience counts as an argument?
- Do we have a no-blame culture which allows to neutrally analyse security in a blame-free and open way?
- Does the executive team lead by example and does it embody our cyber resilience rules and policies?
- How easy would it be for an inside person to willingly or by accident cause an incident?

Processes and organization
Typical questions to be raised around this category of vulnerabilities include:
- Have our primary and secondary processes been reviewed from a cyber resilience perspective?
- Are business process owners and process consultants trained on cyber resilience?
- Do we have a company-wide system in place to authenticate employees, customers, partners and other players in the value chain on all potential communication channels?
- Is there a "four-eye principle" for all cyber resilience processes?
- Do we regularly review elevated privileges assigned to employees and actions performed by these employees?

Once threats and vulnerabilities have been assessed, it is time to circle back and combine all four elements of the risk framework. What are the most important assets as identified in step 1? Which potential losses to these assets come with the highest impact? Which combination of vulnerabilities and threats could lead to a given loss and how likely is this combination to occur?

Using this methodology, risks can be plotted on the two-dimensional risk portfolio along its impact and probability axes. Risks with the highest impact and probability will show up in the upper right quadrant of the framework's output (see page 15).

Application of this guideline
The risk pattern of an organization can change rapidly with change of business models (e.g. introduction of new technologies), new market entries, M&A activities, or new attack approaches. The latter not only because of new established attack technologies, but also if the sentiment of the hacker community suddenly targets an organization as a response to a perceived issue such as lack of "political correctness" in corporate communications.

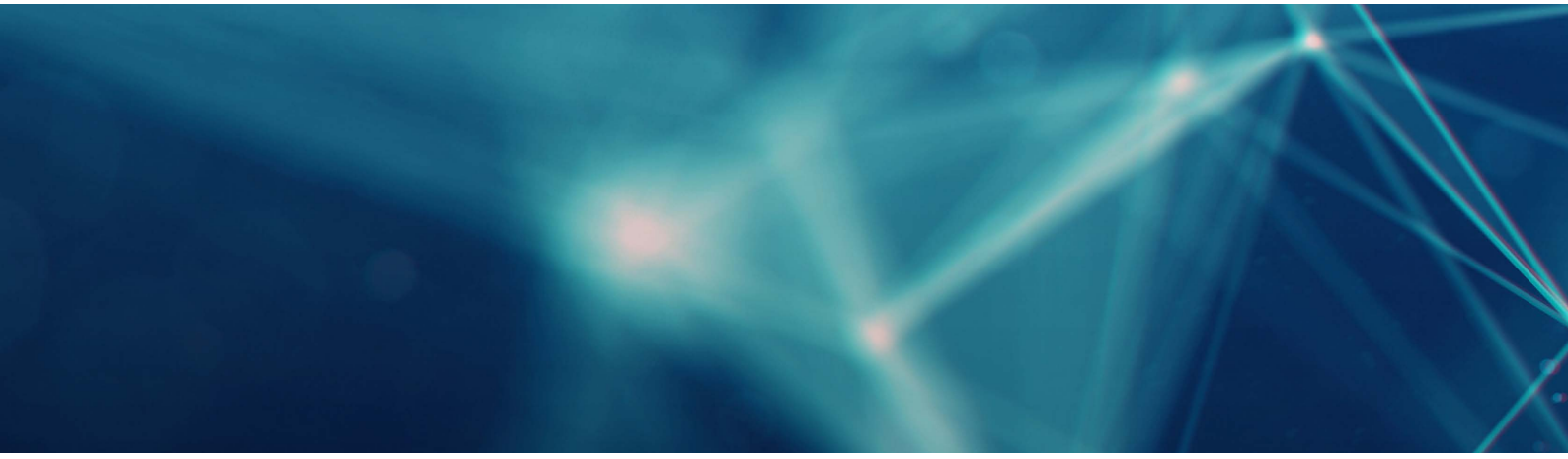
The board should be aware of the fact that the actual cyber risk depends not only on the business model, including the underlying technologies, but also on how much focus hacker groups, such as those that are government-sponsored, have on the organization.

Therefore, the risk pattern of a company may change suddenly and need to be continuously updated by the management; based on changes such as expansion into cybersecurity critical regions or the introduction of new technologies, which may increase opportunities for attack by threat actors. The risk assessment may also change as a result of information from relevant forums, or provided by cyber threat intelligence from within the organization.

Due to their criticality to an organization, cyber risks should be part of the standard agenda of board meetings, and the executive management needs to report changes in the risk pattern, the corresponding risk mitigation measures and the residual risk exposure.

In case of an identified significant change of the cybersecurity risk (e.g. triggered by the cyber threat intelligence), the board needs to be informed immediately by the executive management.

Typically, the following stakeholders are involved during the application of this guideline:
- Business units
- CISO organization
- Legal department
- Communications department
- CERT and/or PSIRT
- Audit organization
- Workers' council



3.4 Board Insights on Emerging Technology Risks

Insight: Guidelines for oversight of emerging technology

The following set of guidelines were developed with the intent of providing board-level stakeholders a set of common risk items that may be present in emerging markets that are based on hyperconnected technologies such as the Internet of Things (IoT) or other innovations. These guidelines are meant to facilitate communication between the board and management and therefore take the position that risks are more effectively managed when the information is harmonized among all levels.

1. *Awareness of emerging technology risk:* The board should be actively involved in understanding and managing the risks associated with emerging technology. Board members should suggest an informed presentation of the risks before business ventures are approved as well as continuously managing risk through periodic assessments using frameworks such as the Board Cyber Risk Framework to new technologies.

2. *Resilience by design:* The board inquires whether cyber resilience is a focus area for all emerging technology initiatives, which are based on hyperconnected cyber physical systems. The board indicates a specific emphasis on ensuring that security is included in the initial phase of any emerging technology endeavour.

3. *Acceptable level of security:* The board recommends an informed and transparent process for adequately managing cyber risks from emerging technologies and balancing them against strategic objectives, risk appetite, go-to-market plans and other business priorities.

4. *Vendor cyber risk management:* For implementation of emerging technologies, the board understands the scale of the new venture and ensures cyber risks associated with vendor selection, vendor partnerships and externally procured technology are adequately managed.

5. *Lifecycle cybersecurity*: The board recommends a comprehensive risk-based lifecycle approach for new technologies, which considers cyber risk for implementation, operations, maintenance, end of life, supply chain, support and liability.

6. *Data privacy:* The board ensures a stringent analysis regarding the privacy implications of, and requirements for, all emerging technology initiatives and encourages a “privacy by design” approach where applicable.

7. *Ethical considerations/public policy*: The board ensures analysis of, and informed decisions relating to, the implications of cyber risk from emerging technology with regard to ethical considerations, social responsibility and public policy.

8. *Continuous improvement of controls*: The board recommends that the responsible cyber risk officer continuously evolves cyber resilience by performing frequent assessment of the controls used to manage risk associated with emerging technologies and by improving the process in accordance with an effective asset protection strategy.

9. *Ability to quickly adapt to change:* The board should be aware of the organization’s cyber resilience capabilities with regards to supporting the business without hindering time-to-market strategies. As market conditions rapidly change and organizations react to these conditions, cyber resilience programmes must have the correct foundations in place to adjust quickly while effectively managing risk.

Insight: The Fourth Industrial Revolution

The proliferation of emerging technologies can currently be seen in every day consumer lives. Physical devices which have internet-enabled connectivity qualify as cyber physical systems. This includes a multitude of examples such as internet-enabled home security cameras, driverless cars, internet-connected pacemakers and other devices. As hardware becomes cheaper to produce and internet connectivity continues to expand throughout the globe, the natural evolution of business is to converge these two ideals into a cyber physical system.[20]

As emerging technologies move from the area of research into production and live implementation, the risks to cyber resilience must be socialized at the board level. This is critical for organizations that are leveraging these technologies due to shifts in business plans and opportunities within these markets. Although the opportunity provided for business is immense, the risks due to the technologies and their scale must be understood*. As the Forum's work in Advancing Cyber Resilience has made clear, it is no longer feasible to embark on business opportunities at the sub-committee or management level without educating the board on the cyber resilience impacts.

While it is unlikely that every risk can be avoided, a clear framework for managing risk will reduce the impact of any incident. Once organizations can effectively manage the risk associated with these technologies, their strategic objectives can be achieved with a greater degree of assurance.

Insight: Current state of emerging technology – Internet of Things

Below is a description of how risk and opportunity collide in one area of emerging technology – the Internet of Things (IoT). Describing this case allows for an illustration of how to consider strategy in light of new and developing risks.

Hyperconnected devices are present in many different business verticals, both private and public. Consumer products are experiencing tremendous growth as new and innovative connected devices are sent to market. This is especially relevant in home or "smart home" systems. These systems include wireless or internet-connected doorbells, cameras, baby monitors, lighting, alarms and other consumer-based products. However, businesses are also expanding their markets to include the next generation of connected devices to aggregate data and change conditions in near real time in order to minimize costs, add value or simply improve operations. Some examples of the current state of IoT include:

- *Transportation:* Telemetry data, traffic routing, platooning, shipping, parking, insurance adjustments
- *Smart cities:* Electrical transmission and distribution, surveillance, predictive analytics, smart grid, waste management, maintenance
- *Healthcare:* Patient care, pacemakers, elderly monitoring, bio-feedback, equipment monitoring, hospital hygiene
- *Buildings:* HVAC monitoring, security, lighting, structural integrity, occupancy, power consumption, emergency alerting

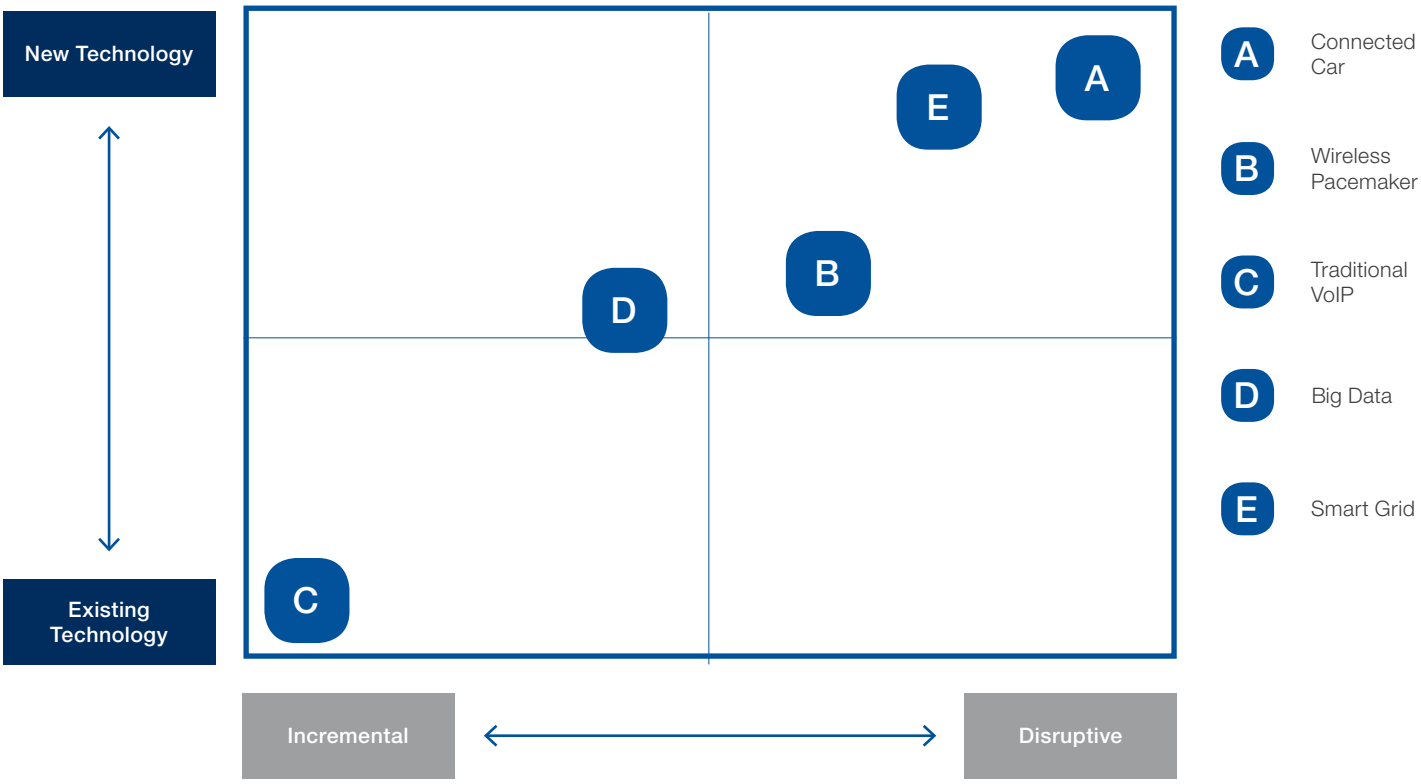
Several opportunities to penetrate new markets and disrupt business models have been major highlights of the prevalence of cyber physical systems. There are many key opportunities for organizations to take advantage of these new models which include, but are not limited, to:

- *Operational efficiency:* Improving uptime and utilization of capital assets and skilled resources
- *Outcome economy:* Shift from products to outcome-based services redefining the basis of competition[21]
- *New markets:* New ecosystems coalescing around shared platforms create new markets and partnerships
- *Integrated digital and human workforce:* Humans collaborating with machines augmenting skills and increasing productivity

As opportunities to converge physical and cyber-related systems grow, organizations are recognizing that they present risks that may be unknown to the business. Executives agree that IoT presents several challenges that must be dealt with in the near future. The Forum conducted an initial survey of market leaders and innovators about the urgency in which IoT must be managed. The survey found:

- 72% believe that the Industrial Internet is disruptive (4-5 on scale of 5)
- 78% say that the disruption will occur within five years
- 88% indicate that businesses are not ready for it now[22]

The following illustrative guide offers a mechanism for contextualizing emerging opportunities and risks for strategic leaders. In the examples provided, business opportunities for new technologies can present higher risk profiles since these technologies are mostly unproven. The rush to market in order to maximize competitive advantage adds to the risk profile incrementally as the business impact increases. Existing and known technologies that have been in use across a large percentage of businesses such as traditional Voice Over Internet Protocol (VOIP) may have a lower risk profile since their threat and vulnerability profiles are well known. However, new technologies such as connected cars, connected medical devices and smart grid can present higher risks since they are disruptive in nature and are driven by innovation, new markets and shifts in business.



Insight: IoT case studies
Cybersecurity experts are seeing a significant amount of research and industry information sharing regarding the risks associated with IoT and its respective technological variants. The concept of IoT has dramatically shifted into new markets due to rapid innovation and building on the model of hyperconnected cyber physical systems.

Tinkerers, hobbyists and researchers have discovered many weaknesses in products that have been rushed to market in the past. There are many lessons to be learned from these case studies. The information within each story highlights the need to socialize the top risks for board-level stakeholders so that an informed discussion can take place between the board and sub-committee stakeholders, executives and other interested parties.

Example 1: Healthcare IoT risk
Norwegian security researcher Marie Moe was able to dissect the wireless security and capabilities of her own pacemaker by downloading manuals and whitepapers. Pacemakers use both short- and long-range wireless capabilities that are susceptible to unauthorized control and command instructions. Moe discovered several insecure lines of code within the pacemaker, which led to physical symptoms of tiredness and lethargy. It was discovered that several software bugs existed in this particular model of pacemaker. This highlights the human safety and product liability concerns related to these devices on a massive scale.[23]

According to a study performed by the University of Massachusetts, some implantable cardiovascular defibrillators are susceptible to short-range wireless attacks. The university released a paper demonstrating that attackers could use software radios via short range to disrupt the devices' capabilities.[24]

Example 2: Transportation industry IoT risk
The trucking industry often utilizes GPS via Telemetry Gateway Units (TGU) to track where their fleets are located at all times. Researchers using publicly available tools found on the internet were able to locate over 700 potentially vulnerability devices. Researcher Jose Carlos Norte discovered several additional weaknesses associated with these devices. Exposing potentially sensitive data about a trucking fleet, destination, estimated time of arrival and possibly the details of its cargo can lead to significant losses if assets are damaged or stolen while in transit. This may also disrupt the supply chain for business partners or customers and lead to damaged reputation.[25]

Example 3: Automotive industry IoT risk
As automakers rush feature enhancements, hyperconnectivity and value propositions to market, researchers are uncovering various ways to take advantage of weaknesses in these newly connected systems. For example, many automobiles have features that can now be controlled through the user's smartphone by an application that connects via the cloud and back to the car itself. However, this presents a potential vulnerability for smartphone applications if security is not at the forefront of the software architecture. Researcher Troy Hunt was able to take advantage of a software vulnerability on a smartphone in order to access some non-life threatening features of the Nissan Leaf. This is also an example of potential product liability and breach of customer trust. Hunt's research underscores the need for vigilant security in the automotive industry as accessibility and connectivity become more pervasive.[26]

Example 4: Critical infrastructure
The protection of cyber assets within the critical infrastructure domain such as oil and gas, power generation and transmission, smart cities and other classifications continue to be a topic of concern for global cybersecurity stakeholders. As more critical cyber assets and SCADA systems are interconnected, the concern for human safety remains at the forefront. Researchers at the University of Michigan demonstrated how weaknesses in wireless radio communications can be exploited in order to take control of several traffic lights in an undisclosed Michigan municipality. This research highlights the risk associated with the wireless connections and the potential for catastrophic consequences if attackers are able to perform similar feats.[27]

4. The Future of Cyber Resilience

The World Economic Forum hopes that the principles and tools above will provide the means by which boards and business leaders can take action on ensuring their organizations adopt cyber resilience strategies. In the coming years, the Forum will continue to provide insights and spur action in this space, including in the following ways:

Continual improvement. These tools are not meant to be the final work on cyber resilience governance and strategy. Rather, by working with partners, the Forum will serve as the platform for continual iteration and improvement of these and other governance and leadership tools. Iteration will continue for these tools, including continued development of the Cyber Risk Framework, described below in Appendix 4.

Partnership. Digital networks cross the globe and connect firms across industries and border. The Forum will continue to work to nurture partnerships in support of cyber resilience among boards and senior executives.

Public-private cooperation. Security in the digital space is a global public good. As such, the Forum will bring together stakeholders to ensure that cybersecurity and resilience are a matter of cooperation between government, business and civil society.

Leadership. The global and cross-sectoral nature of digital networks means that the mechanisms used to foster cyber resilience in the private sector can and should be adapted to serve the public sector and society as a whole. The Forum will continue to develop these tools to support a wide variety of leaders.

Appendix 1: Cyber Resilience Tools at a Glance

Board Principles for Cyber Resilience

Principle 1

Responsibility for cyber resilience. The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. risk committee) or new committee (e.g. cyber resilience committee).

Principle 2

Command of the subject. Board members receive cyber resilience orientation upon joining the board and are regularly updated on recent threats and trends – with advice and assistance from independent external experts being available as requested.

Principle 3

Accountable officer. The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

Principle 4

Integration of cyber resilience. The board ensures that management integrates cyber resilience and cyber risk assessment into overall business strategy and into enterprise-wide risk management, as well as budgeting and resource allocation.

Principle 5

Risk appetite. The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Principle 6

Risk assessment and reporting. The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber Risk Framework.

Principle 7

Resilience plans. The board ensures that management supports the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

Principle 8

Community. The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.

Principle 9

Review. The board ensures that a formal, independent cyber resilience review of the organization is carried out annually.

Principle 10

Effectiveness. The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

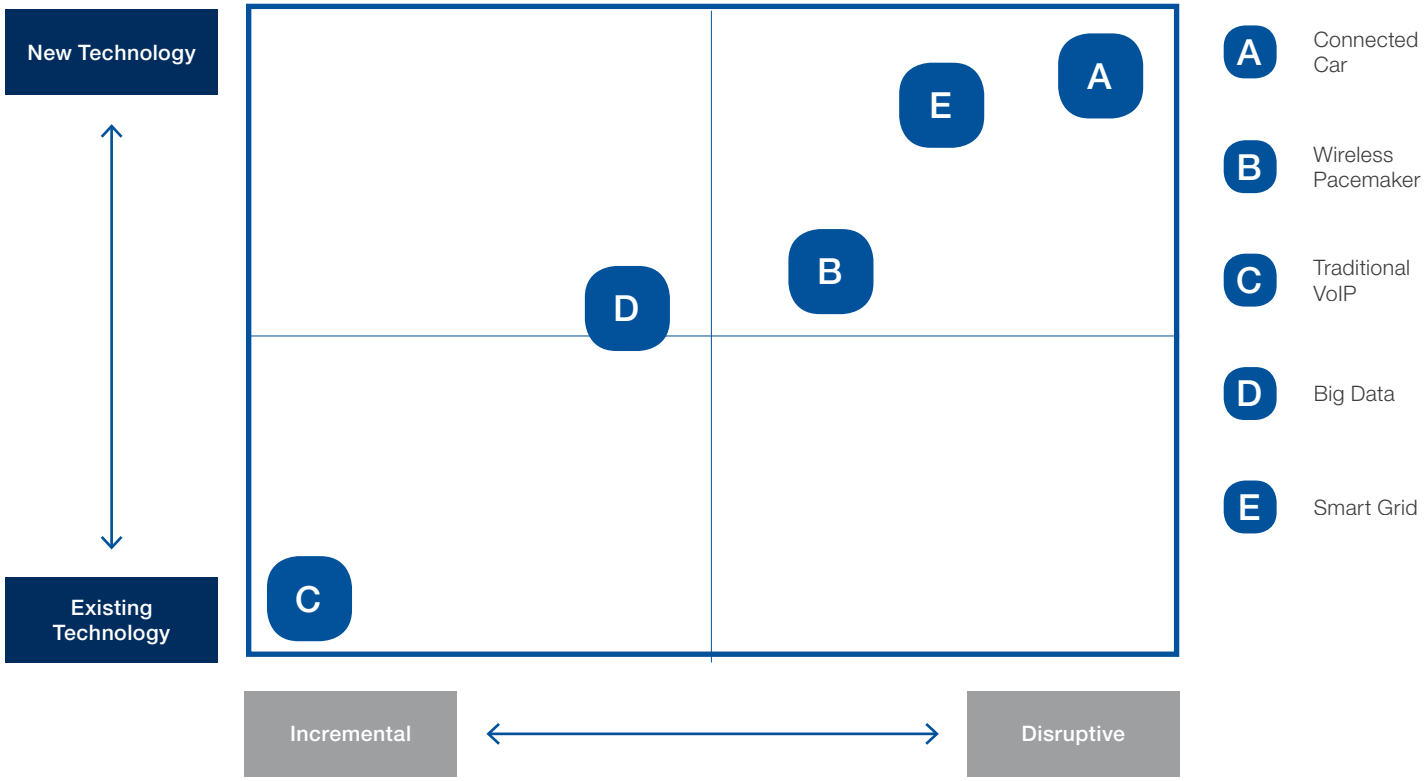
Updated Board Cyber Risk Framework

Cyber Risk

Cyber incident impact				Cyber incident probability		
Assets at risk[1]	X	Loss of …	X	Vulnerabilities	X	Threats[2]
Intangible assets — IP — reputation — compilance		confidentiality		People and Culture		Disgruntled Customers Human Error Supply Chain Partner Action Insider Action Hacktivism Crime Sabotage Corporate Espionage Terrorism State Action Force Majeure
Tangible assets — financial — physical — production systems — infrastructure		integrity and accountability		Processes and Organization		
Greater good — safety of life and health — civil liberties — individual privacy		availability		Technology and Infrastructure		

[1] Examples for assets
[2] Selection of examples, sorted in ascending order of available resources

Risk Context for Emerging Technologies



Appendix 2: Terms and Definitions

Advanced persistent threat	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g. cyber, physical and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, programme, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives
Assurance	Grounds for justified confidence that a claim has been or will be achieved – Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g. security claims, safety claims) and the claims themselves may be interrelated – Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims
Availability	Ensuring timely and reliable access to and use of information – Mission/business resiliency objectives extend the concept of availability to refer to a point-in-time availability (i.e. the system, component, or device is usable when needed) and the continuity of availability (i.e. the system, component, or device remains usable for the duration of the time it is needed)
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Cyber resilience	As an additional dimension of cyber risk management, the ability of systems and organizations to develop and execute long-term strategy to withstand cyber events; practically, it is measured by the combination of mean time to failure and mean time to recovery
Incident	Anomalous or unexpected event, set of events, condition, or situation at any time during the lifecycle of a project, product, service, or system
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
Penetration testing	A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system
Residual risk	Risk remaining after risk treatment
Risk	Effect of uncertainty on objectives
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk management	Coordinated activities to direct and control an organization with regard to risk
Risk appetite	The organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives; risk tolerance can be influenced by legal or regulatory requirements
Risk treatment	Process to modify risk
Security control	A mechanism designed to address needs as specified by a set of security requirements
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

Appendix 3: Principles and Toolkits in Practice

Illustration of Principle 5

Principle 5: Risk appetite
The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Risk Appetite in Practice
The chief information security officer of a manufacturing company ran a cybersecurity risk workshop for the board and company executives in which the risks to different objectives of the business were debated along with the cost/operational implications of typical security measures. The board determined that they had a low appetite for any risk to government business and wished to keep up with, but not exceed, the industry leaders in managing risks to their commercial business (moderate appetite). They considered having a higher risk appetite that might lower operating costs in their start-up consumer business, but concern for strategic damage to reputation lead them to also declare this as moderate appetite.

These risk appetite views were subsequently used by business management, IT and the CISO security team to look at additional special cybersecurity measures for the government business and making sure that the cybersecurity strategy for the other businesses tracked both threats and the upper quartile of the competitive market.

For more resources relating to setting or evaluating an organization's risk appetite, please see the Board Cyber Risk Framework.

Appendix 4: Future of Cyber Resilience – Risk Benchmarking for Boards

Steps towards Risk Benchmarking

There is an interest among board members to benchmark cyber risk on a strategic level between companies. Therefore, the Forum plans to build a platform for the anonymous sharing of a board's risk assessments. Contributing data to this platform will open access to the benchmark data collected from peers. Industry-specific averages will be made available as soon as meaningful data is provided back. Formal standards will ensure data consistency and allow for its evaluation across organizations. Further provisions will safeguard encrypted, anonymous data transfer and storage. Relevant global standards for sharing of risk and threat data will be considered.

The following provides a list of potential items for company benchmarking:

Demographics
- Organization's size (revenue categories)
- Geographic presence
- Primary industry

Risk portfolio
- Total value of cyber risk portfolio prior to risk management actions
- Total value of residual cyber risk portfolio after risk management actions
- Risk appetite
- Total cost of risk management actions

Risk controls/responses/management actions
- Risk controls implemented
- Aspired maturity level
- Actual maturity level
- Implementation status of CISO structure
- Organization structure
- Governance model
- Cyber resilience budgets/spent
- Existence of IT security architecture plan
- Implementation status of CERT and/or PSIRT
- Availability of centralized security monitoring available, such as a security operation centre (SOC)
- Deployment status of incident and vulnerability handling policy
  - Existence of alerting plans and structure
  - Implementation stratus of database
- Existence of IT security audit plan
- Implementation status of encrypted communications
- Existence of concepts to increase employee awareness
- Implementation status of advisory service
- Participation in a community for data sharing and development of standards
- Existence of threat intelligence
- Implementation of scheduled vulnerability assessments

Threats
- Threat level per threat category (insider, crime, etc.)
- Frequency of attacks
- Average duration of an attack/incident (in days)
- Incident ratio (#of incidents/#of attacks)

Acknowledgements

The World Economic Forum's Advancing Cyber Resilience project is a global, multi-industry, multistakeholder endeavour aimed at contributing to a safer and stronger connected society by improving cyber resilience. The project engages stakeholders across multiple industries and governments from around the world.

The governance and strategic direction for this project is provided by the System Initiative on Shaping the Future of Digital Economy and Society and our dedicated Working Group. This report is based on numerous discussions, workshops and research and the combined effort of all involved opinions expressed herein may not necessary correspond with each and every one involved with the project. The project intended to seek consensus among those participating.

Sincere thanks are extended to the industry experts who contributed their unique insights to this report. We are also very grateful for the generous commitment and support of The Boston Consulting Group in its capacity as project strategy adviser and of Hewlett Packard Enterprise in its capacity as project technology adviser.

At the World Economic Forum, the support and commitment of the ICT Industry Community, led by Alan Marcus, the IT Industry Community, led by Danil Kerimi with Roger Zhang and Adam Sherman, have been vital to our success. We would also like to thank the Mobility Industry Community, led by John Moavenzadeh with support from Andrey Berdichevskiy. Finally, this project would not be possible without the leadership and guidance of Derek O'Halloran, Mark Spelman and Fadi Chehadé, Co-Heads of the System Initiative on Shaping the Future of Digital Economy and Society as well as the invaluable input and guidance provided by the Forum's Managing Board, especially Richard Samans and Jim Hagemann Snabe. This report's editor and project lead would like to especially acknowledge Derek O'Halloran, who has led this work at the Forum for many years and continues to be a great champion of cyber resilience.

Daniel Dobrygowski
Project Lead – *Advancing Cyber Resilience* for the project team

Expert Working Group

The Expert Working Group brings together leading academic experts, thinkers and senior executives from across industries. Working Group members dedicated a significant amount of time and other resources to help the project cover the range of functional perspectives that needed to be integrated in this topic, in particular risk, security, technology and legal perspectives.

Paul Wood	Chief Risk & Compliance Officer	Bloomberg	USA
Boaz Gelbord	Chief Information Security Officer	Bloomberg	USA
Friedhelm Pickhard	President	ETAS GmbH	Germany
Phillip Harrington	Senior Managing Director	Brock Capital Group	USA
Les Anderson	Vice-President of Cyber and Chief Security Officer	BT Group	United Kingdom
William H. Saito	Special Adviser	Cabinet Office of Japan	Japan
Don Proctor	Senior Vice-President, Head of Cybersecurity Task Force	Cisco	USA
Michael Nelson	Head of Public Policy	Cloudflare	USA
Paul Dorey	Founder	CSO Confidential	United Kingdom
Andreas Rohr	Chief Technology Officer	DCSO (Deutsche Cyber-Security Organization)	Germany
Greg Montana	Chief Risk Officer	FIS	USA

Robert Taylor	Senior Vice-President, Chief Information Officer	Fluor Corporation	USA
Harry Lightsey	Executive Director, Global Connected Customer, Public Policy	General Motors	USA
Jody Westby	Chief Executive Officer	Global Cyber Risk LLC	USA
Robert Coles	Chief Information Security Officer	GlaxoSmithKline	United Kingdom
Mark Viola	Vice-President, Global Chief Information Security Officer	Henry Schein	USA
Seung Ho Hwang	Executive Vice-President, Auto Intelligence Division	Hyundai Motor Company	Republic of Korea
George DeCesare	Senior Vice-President, Chief Technology Risk Officer	Kaiser Permanente	USA
Paul Nicholas	Senior Director	Microsoft Corporation	USA
Amy Weaver	Executive Vice-President and General Counsel	Salesforce	USA
Kirstjen Nielsen	President	Sunesis Consulting	USA
Sadie Creese	Professor of Cyber Security	University of Oxford	United Kingdom
Debra Farber	Senior Director, Privacy, Data & Risk Policy	Visa Inc.	USA
Martin Hoffman	Chief Information Officer	Volkswagen	Germany
Stefan Pinelli	Head of IT Legal	Volkswagen	Germany
Lori Bailey	Global Head of Special Lines	Zurich Insurance Group	USA

The project team would also like to thank the board members who supported our work by serving as a sounding board and informal validation body as we developed this project and its deliverables: Phillip Harrington (USA), Leonard Schrank (Belgium), Vikas Sehgal (UK), Kevin Kessinger (USA), Noel Gordon (UK), Sheila Stamps (USA), Olga Botero (Colombia), Peter Dehnen (Germany), Carmen Graham (Peru), Jaime Ardila (Brazil), Mel Lagomasino (USA), Jason Hogg (USA), Rene Soltwisch (Germany), Edgar Ashenbrenner (Germany), and Maria Eugenia Giron (Spain).

We would further like to thank Jim Pinter, Senior Security Strategist, Microsoft, and Hala Furst, Cybersecurity and Technology Business Liaison, US Department of Homeland Security, for their invaluable contributions to the development of this project.

Project Strategy Adviser: The Boston Consulting Group

Alexander Tuerk	Project Leader (*Secondee to the Forum)*	USA/Germany
Walter Bohmayr	Senior Partner and Managing Director	Austria
Stefan Deutscher	Principal	Germany

Special thanks to the following Boston Consulting Group experts for their insightful contributions to this project and report: Michael Coden, Associate Director, BCG Platinion; Russ Trpkovski, Principal; Anil Vijayan, Associate Director, BCG Platinion; Bella Powell, Project Leader; Shoaib Yousuf, Project Leader; Nadya Bartol, Manager, BCG Platinion; Alex Asen, Senior Knowledge Analyst.

Project Technology Adviser: Hewlett Packard Enterprise

Andrzej Kawalec	Global CTO, HPE Enterprise Security	United Kingdom
Richard Archdeacon	EMEA CTO HPE Enterprise Security	United Kingdom
Nathan Ouellette	Security Architect	USA

Special thanks to the following Hewlett Packard Enterprise experts for their insightful contributions to this project and report: Chris Leach, AMS CTO, HPE Enterprise Security; Andreas Wuchner, CTO Security Innovation, HPE Enterprise Security; Jeremy Ward, Security Consultant, HPE Enterprise Security; Ann Ewasechko, Senior Manager, Corporate Affairs.

The project team would also like to thank Mike Nefkens, Executive Vice-President and General Manager, Enterprise Services, for his leadership in this work and generosity with his time and energy in engaging Hewlett Packard Enterprise in this project.

Contacts

Derek O'Halloran,
Co-Head, System Initiative on Shaping the Future of Digital Economy and Society
World Economic Forum
derek.ohalloran@weforum.org

Daniel Dobrygowski
Global Leadership Fellow
Project Lead
World Economic Forum
daniel.dobrygowski@weforum.org

Endnotes

1 World Economic Forum, *Partnering for Cyber Resilience*, 2012, http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf; World Economic Forum, *Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience*, 2012, https://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience.

2 World Economic Forum, *Partnering for Cyber Resilience*, 2012, http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

3 Post, Dana, "Cybersecurity in the Boardroom: The New Reality for Directors", *IAPP*, 27 May 2014, https://iapp.org/news/a/cybersecurity-in-the-boardroom-the-new-reality-for-directors.

4 "Cybersecurity and the SEC", *US Securities and Exchange Commission,* https://www.sec.gov/spotlight/cybersecurity.shtml; "Reform of EU data protection rules", *European Commission*, http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

5 Harvard University page on cybersecurity, https://cyber.harvard.edu/cybersecurity/Main_Page.

6 Kaplan, James, Tucker Bailey, Derek O'Halloran, Alan Marcus, Chris Rezek. *Beyond Cybersecurity*. Wiley, 2015.

7 Perlroth, Nicole, "Hackers use new weapons to disrupt major webites across U.S.", The New York Times, 21 October 2016, http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html.

8 Schneier, Bruce, "Lessons From the Dyn DDoS Attack", *Schneier on Security Blog*, 8 November 2016, https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html

9 Dobrygowski, Daniel, "Cyber resilience: everything you (really) need to know", *Forum Blog*, 8 July 2016, https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know.

10 Steinberg, Richard, *Governance, Risk Management, and Compliance*. Wiley, 2011.

11 Calder, Alan & Steve Watkins. *IT Governance*, 6th ed. KoganPage, 2015.

12 Howell, William, "Uncontrollable Risks and the Role of the Board of Directors", *Dissertation of the University of St. Gallen School of Management, Economics, Law, Social Sciences and International Affairs*, 2016, http://www1.unisg.ch/www/edis.nsf/SysLkpByIdentifier/4469/$FILE/dis4469.pdf.

13 World Economic Forum confidential board surveys (July-September 2016).

14 Westby, Jody, "Cybersecurity & Law Firms: A Business Risk", *ABA Law Practice Magazine*, Vol. 49, No. 4, 2013, http://www.americanbar.org/publications/law_practice_magazine/2013/july-august/cybersecurity-law-firms.html.

15 ISO, Information technology -- Security techniques (ISO/IEC 27000:2016), 2016.

16 ISACA, COBIT 5 for Information Security, 2012.

17 National Institute of Standards and Technology (NIST), Framework *for Improving Critical Infrastructure Cybersecurity*, 2014.

18 Caralli, Richard, James F. Stevens, Lisa R. Young, William R. Wilson, Introducing OCTAVE Allegro: Improving the *Information Security Risk Assessment Process*, Software Engineering Institute, 2007.

19 World Economic Forum, *Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience*, 2012, https://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience.

20 Schwab, Klaus, "The Fourth Industrial Revolution: What it means, how to respond", *Forum Blog*, 14 January 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond.

21 World Economic Forum, "Convergence on the outcome economy", http://reports.weforum.org/industrial-internet-of-things/3-convergence-on-the-outcome-economy/3-2-the-emergence-of-the-outcome-economy/?doing_wp_cron=1463567483.8225409984588623046875.

22 World Economic Forum, *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services*, 2015, http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

23 Vallance, Chris, "Could hackers break my heart via my pacemaker?" *BBC*, 3 December 2015, http://www.bbc.com/news/technology-34899713.

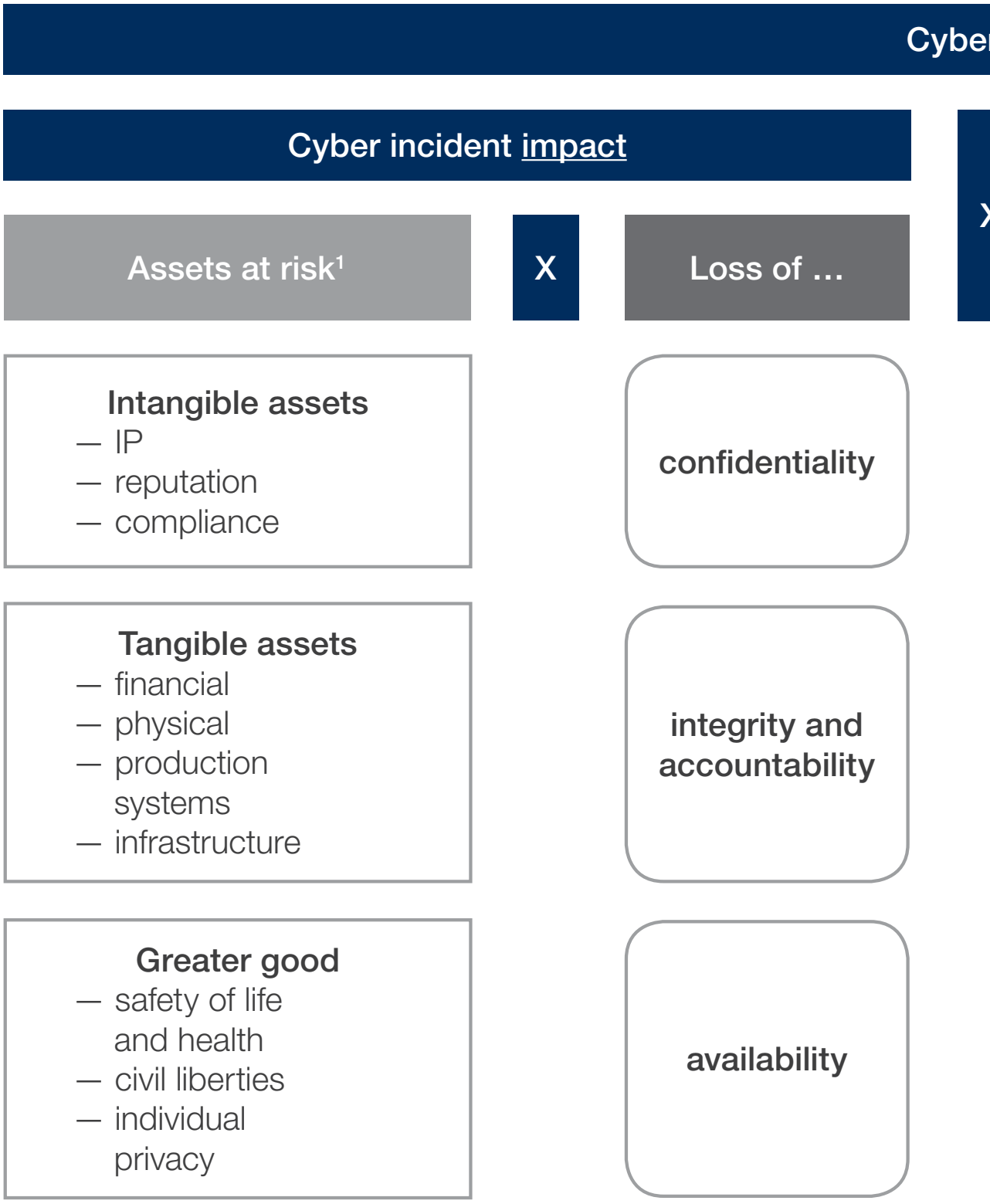
24 "How Much Security Do You Expect From Your Pacemaker?" University of Massachusetts, Amherst, 3 October 2008, https://www.umass.edu/newsoffice/article/how-much-security-do-you-expect-your-pacemaker-umass-amherst-expert-works-provide-cyber.

25 Norte, Jose Carlos, "Hacking Industrial Vehicles From The Internet", 6 March 2016, http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html

26 Kelion, Leon, "Nissan Leaf electric cars hack vulnerability disclosed", *BBC*, 24 February 2016, http://www.bbc.com/news/technology-35642749.

27 Branden Ghena, William Beyer, Allen Hillaker, et al., "Green Lights Forever: Analyzing the Security of Traffic Infrastructure", Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT), http://www.eecs.umich.edu/eecs/about/articles/2014/traffic-woot14.pdf.

Updated Board Cyber Risk Framework



[1] Examples for assets
[2] Selection of examples, sorted in ascending order of available resources

r Risk

X

Cyber incident probability

Vulnerabilities	X	Threats[2]
People and Culture		Disgruntled Customers
		Human Error
		Supply Chain Partner Action
		Insider Action
		Hacktivism
		Crime
		Sabotage
		Corporate Espionage
		Terrorism
		State Action
		Force Majeure
Processes and Organization		
Technology and Infrastructure		

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org

World Economic Forum LLC
3 East 54th Street, 18th Floor,
New York, NY 10022, USA
Tel.: +1 212 703-2300
Fax: +1 212 703-2399
contact@weforum.org
www.weforum.org