# Director's Technology Handbook

## Tips and Strategies for Advising Corporate Directors

**Candace M. Jones, Editor**

ABA
AMERICANBARASSOCIATION
Business Law Section

# Table of Contents


Preface ..... v

Chapter 1: Fiduciary Duties of Corporate Directors ..... 1

Chapter 2: The Lawyer's Role in Communicating with the Board about Technology ..... 5

Chapter 3: Overcoming the Jargon Divide: Shared Lexicon for Business, Technology, and Law ..... 11

Chapter 4 Regulatory Compliance and Compliance Risk ..... 15

Chapter 5 Same, Same, but Different: Uncommon Law(s) When Doing Business in Canada ..... 27

Chapter 6: Contracts ..... 39

Chapter 7: What Is . . . Cloud Computing? ..... 45

Chapter 8: Open Source Software Licenses ..... 49

Chapter 9: Acquiring Technology Assets ..... 57

Chapter 10: What Are . . . Intellectual Property Rights? ..... 65

Chapter 11: Data Management ..... 73

Chapter 12: Privacy—Europe ..... 79

Chapter 13: International Data Privacy Laws ..... 85

Chapter 14: Legal Risks and Mitigation Strategies for Business Use of Social Media ..... 95

Chapter 15: Payments Issues for Directors and the Lawyers Advising Them ..... 105

Chapter 16: Cybersecurity Programs and Organizational Culture ..... 111

Chapter 17: Governing Cyber Risk Management in the Twenty-First Century: A Forward-Looking Strategy ..... 117

Chapter 18: What Is . . . "Industry Standard"? ..... 127

Chapter 19: Contracting with Vendors for Information Security and Resiliency ..... 131
Chapter 20: Insurance ..... 139
Chapter 21: Emerging Technologies—An Illustration of the Technology-Legal Landscape ..... 145
About the Authors ..... 149
Tips for Lawyers to Engage Effectively with Clients about Technology ..... 153
Index ..... 155

## CHAPTER 17

# Governing Cyber Risk Management in the Twenty-First Century: A Forward-Looking Strategy

Mike Jerbic

## Issue Overview

At the highest level, boards have four fundamental governance objectives:

1. *Consent* to corporate objectives in the pursuit of opportunity,
2. *Consent* to the rules or prohibitions management must conform to in achieving those objectives, *including prohibitions against taking risk beyond the board's risk appetite*,
3. *Delegate* authority to management to achieve those objectives, and
4. *Evaluate* how those objectives were met and take corrective action, if needed.

In governing how the firm manages risk, boards define or consent to the allowable risk that management can take on behalf of corporate shareholders—in other words, the board's risk appetite. Management then assembles and organizes the firm's factors

of production to accomplish corporate objectives within this risk appetite. In defining a risk appetite and governing risk management, the board is exercising its *fiduciary* responsibility in defining acceptable business risk exposure and governing the management of risk within that risk appetite, and its legal *compliance* responsibility in disclosing material business risk to investors.

Defining a *cyber risk appetite* and managing to it have been a governance and management challenge for many years. That challenge started out as one primarily relegated to the IT teams and the chief information security officer or chief information officer. But as the frequency and significance of impact of cyber events, both internally to the firm and among the broader community of the firm's external stakeholders, have risen from an IT risk to a significant enterprise risk, regulators and corporate director professional associations now place cyber risk governance responsibility directly upon the board itself. Directors have duties to govern cyber risk management and to disclose those risks in ways that accurately and adequately inform shareholders, customers, suppliers, and regulators of the firm's cyber risk exposure and risk management.

But cyber risk is rarely presented to boards using the same metrics and terminology used to express other enterprise risks. Frequently, boards get presentations related to the state of the enterprise's cybersecurity and its compliance to industry standards, best practices, and regulatory compliance. All these are examples of metrics, but they do not present the state of the firm's cybersecurity and cyber risk exposure in terms that express "risk" in the sense of the SEC description of risk, i.e., "a forward-looking estimate of the probability and magnitude of potential loss."

Unable to assess risk as an estimate of likely potential loss, boards are left to arrive at that estimate by discussing the potential threats to information security, the information assets themselves, the methods threat agents use to damage those assets, and the likely losses that might follow, all of which boards are not usually well equipped to do. Board members make judgments about the forward-looking estimate of the probability and magnitude of potential loss using their own mental, subjective models of risk informed by general discussion of threats and security but without truly discussing the *risk* associated with the security of their information technology assets. Boards, their management, and their IT teams debate security, not risk. Because cyber risk is so rarely presented to boards in traditional risk terms, commensurate with the presentation of other enterprise risks, boards and management have confused a debate over the means to the end of risk management, not risk management itself.

What most board members don't know is that the third decade of the twenty-first century is seeing a fundamental change in how cyber risk is defined, discussed, assessed, measured, and managed. New methodologies, which have sufficiently matured to become industry standards, enable boards and their management to measure cyber risk in the same terms as other enterprise risks. Cyber risk measurements expressed this way let boards more effectively define risk appetites, govern corporate management to operate within that appetite, and collaborate with management to manage and mitigate that risk. Using these methods, corporate boards can increase the

quality of their governance decisions and make more fully informed and defensible risk management decisions. Firms that disclose cyber risk in these terms will, in turn, help investors improve the quality of their investment decisions.

Governing cyber risk as an enterprise risk requires four steps, which are the focus of the rest of this chapter:

1. Establishing the *goal* of effective cyber risk management, not information security management, as the enterprise board governance objective;
2. Choosing the *language to frame and analyze questions* that the board, senior management, and operational staff will use to effectively communicate with each other in defining, managing, and communicating risk-based objectives;
3. Choosing the *decision process maturity level* that will be used to make cyber risk management decisions; and
4. Defining the *information* the board, senior management, and operational staff will produce, present, and rely upon to effectively inform decision-making consistent with the *language, goals*, and *decision process maturity level* chosen.

These four steps, taken together, form a complete, disciplined, and coherent way of effectively managing cyber risk as an enterprise risk.

## Establishing the Goal of Effective Cyber Risk Management

With respect to cybersecurity, boards have two main areas of responsibility as articulated by the U.S. Securities and Exchange Commission (SEC) and the National Association of Corporate Directors (NACD): accurate disclosure and cyber risk management governance. Boards must understand that cybersecurity—the set of administrative, technical, and physical controls that operationally constrain corporate activity—is a means to an end. The end is effective cyber risk management.

### *The Board's Responsibility for Disclosure*

The SEC initiated its first guidance on the duty of public companies to disclose cyber risk in 2011 and, in 2018, it elaborated upon that guidance. Firms must disclose cyber risk as a business risk that "that a reasonable investor would consider important to an investment decision." The 2018 elaboration clarified that these disclosures need to avoid boilerplate, be specific to the firm and its business, and should not give adversaries additional information they could use to add to the firm's cyber risk. Disclosures must be fit for purpose; namely, to help investors make informed investment decisions without adding to the firm's risk.

## *The Board's Responsibility in Cyber Risk Management Governance*

In 2014, the NACD released guidance to directors on their duties to govern cyber risk, putting boards on notice that they are responsible to govern how the firm manages cyber risk. As part of their duties to shareholders, directors and the full board need to:

- Understand and approach cybersecurity as an enterprise risk management issue, not just an IT issue;
- Understand the legal implications of cyber risks as they relate to their company's specific circumstances;
- Have adequate access to cybersecurity expertise and give regular and adequate time on the board meeting agenda to discussions about cyber risk management;
- Expect management to establish an enterprise-wide cyber risk management framework with adequate staffing and budget; and
- Engage with management to identify specific cyber risks and jointly determine which cyber risks to avoid, accept, mitigate, or transfer through insurance, as well as the specific plans associated with each approach.

Following the guidance to treat cyber risk as an enterprise-wide risk implies that cyber risk should be measured and reported in terms similar to those used for measuring and reporting other enterprise-wide risks. With all risks measured consistently, risk disclosures present cyber risk in a manner that gives investors a view of an enterprise's cyber risk that's consistent with its other enterprise risks. Measuring cyber risk in the same terms as other enterprise risk measurement also better enables the board to make informed enterprise-wide risk management decisions and tradeoffs.

With that foundation, the board can turn to the four steps for governing cyber risk as part of the organization's overall enterprise risk management program. The organization must execute its risk management program in a manner that lends itself to effective board governance. Effective board governance requires:

- Clearly communicated risk management objectives and well-defined risk appetite;
- Timely measurements of risk communicated in units of measure consistent with those objectives;
- Policies, procedures, and guidelines that enable operating units within the business to effectively manage risk to board objectives; and
- Effective risk-based comparisons of alternatives that let the board see cyber risk management results as a component of overall enterprise risk management reporting.

## Choosing the Language to Frame and Analyze Questions

Executive management operationalizes cyber risk management objectives through the means of information security, which itself is a specialized field. As practitioners in a highly specialized field, security subject-matter experts think and communicate in the language of security frameworks, such as the NIST Cybersecurity Framework, not in the business language of risk and risk management. Boards and executive management must establish a bridge between the board's objectives of effective cyber risk management and the operational discipline of information security. The common mission is effective risk management, and the effective language for the mission is, therefore, the language of risk. The language of risk can thus be a tool in harmonizing business management with security operations.

To be effective in managing risk to the board's objectives, the organization needs to bridge the rhetorical gap between risk management and information security operations so that the operational teams can internalize the risk management objectives and translate those objectives into actions that implement information security controls corresponding to the objectives. Within their specialized discipline, the operations teams will use the terms, definitions, and relationships (the language of cybersecurity) that enable them to communicate effectively to implement *and operate cybersecurity controls. Implementing and operating information security controls are the means to the end goal of effectively managing cyber risk*.

## Choosing a Decision Process Maturity Level

Once the language has been established, the board must decide the process by which it will make decisions. Decision-making processes, like any other business process, can be characterized by a maturity level. Process maturity levels were introduced decades ago with ISO 9000/9001 being one of the first in 1987. Software development process maturity levels followed, and today many business processes have their own corresponding maturity levels.

Maturity levels typically follow a five-level hierarchy. (Watts Humphrey, in his article *Characterizing the Software Process: A Maturity Framework*, describes five process maturity levels that are consistent with other capability maturity models. The levels described here are consistent with that model.)

> Level 1 is characterized as undocumented and unstructured with the quality of business results achieved through heroics of talented individual staff members. Processes at Level 1 have little consistency in quality or results when different people perform them.
>
> Level 2 is characterized as repeatable within a specific work group. Processes at Level 2 yield consistent results when performed by the same organization within the firm, but they can vary substantially between

organizations, geographies, divisions, etc., each of which follow different documented processes for completing similar activities (such as software development projects).

Level 3 is characterized as defined policy and procedure throughout the entire firm. Processes at Level 3 are consistent throughout the firm and tend not to vary. Every activity is covered by an enterprise policy, and procedures are expected to conform with minimal variation by organization, geography, and division.

Level 4 is characterized as managed where policy and procedure is quantitatively measured, evaluated, and managed. Processes at this level have metrics that are measured with deviations from allowable norms reported and responded to. When results fall outside of defined tolerances, corrective action is taken. Metrics, measurements, and corrective action distinguish Level 4 from Level 3.

Level 5 is characterized as continual improvement or as optimized. With the metrics and measurements of Level 4, processes are now continually improved through the Shewhart-Deming Plan-Do-Check-Act (PDCA) cycle of continuous improvement. At Level 5, metrics include costs of improvement and benefits of improvement, with economic optimization of the process being the goal. Metrics are now economic, not just technical, and staff throughout the firm use those metrics to make cost-benefit tradeoff decisions, optimizing cost-effectiveness of the investment.

Most publicly traded companies are probably at Level 3 in their cyber risk management decision-making process maturity. In an organization at Level 3 maturity, the board and senior management have defined common policies that everyone within the firm is expected to comply with, and they have insisted upon common security controls to be deployed throughout the firm. Measuring compliance is accomplished through everyday management practice and internal and external audit. Industry standards, such as the NIST Cybersecurity Framework, ISO 27000, and COBIT describe controls that the board and management assume will manage the organization's cyber risk effectively.

Some firms are elevating their decision process maturity to Level 4, incorporating quantitative methods, such as the Open Group's Open FAIR methodology to measure cyber risk in terms commensurate with other enterprise risks such as credit, market, and operational risk. Using quantitative methods, decision makers evaluate the likely economic impact of complying with defined policies, giving individuals throughout the firm freedom to apply controls that are more cost effective than the one-size-fits-all compliance to policy that Level 3 demands.

Maturing beyond Level 4, organizations have the opportunity to model the cost-effectiveness of risk mitigation strategies before they are implemented, leading to continuous improvement of cyber risk management. Using the metrics in Level 4 and estimating how new policies, procedures, and security controls will affect those metrics,

firms can optimize their future security investments and focus on "what matters most." At Level 5, boards and management will have the information to make "risk-based decisions" and can justify security investment on a cost-benefit basis.

Boards should know that the choice of risk-management decision-process maturity level is a business decision, and no level is better than another in every instance. That said, in an environment characterized by rising global competition, increased reliance upon technology and information to run the business, and higher costs to the public from breaches, regulators and shareholders will likely demand boards increase their cyber risk management maturity and intelligence. Whatever cyber risk management decision process maturity level is adopted, the choice must be deliberate and, once made, will have significant implications for the information operational units will have to provide the board so that it can govern to the chosen maturity level.

## Developing and Producing Information Consistent with the Language, Goal, and Decision Process

A mature board, especially that of a public company, should be choosing between Level 3, 4, or 5 as the process maturity level for making cyber risk governance decisions. Each of those levels has distinctly different information requirements to equip the board to make informed decisions, and the operational units informing the board need to know what information to provide the board and how to get it. Some examples follow.

- To make maturity Level 3 decisions, the board needs to be informed of "best practices," industry standards, and regulatory compliance requirements. Boards at this level may rely upon qualitative assessments of organizational results, such as those provided in an audit report.
- To make maturity Level 4 decisions, the board requires quantitative measurements of how its decisions are being accomplished throughout the enterprise. To evaluate risk quantitatively, boards need measurements of cyber risk expressed in risk terms: the likelihood and severity of future losses associated with information technology. For the board to consider cyber risk as an enterprise risk, these measurements must be in the same units of measure as other enterprise risk measurements. In other words, cyber risk must be measured in economic terms, just as other enterprise risks are measured.
- To make maturity Level 5 decisions, the board needs to have quantitative measurements (as in Level 4) and will also require estimates of how proposed risk management remediation will affect risk, all expressed in economic terms so that the board can evaluate whether the benefits of a risk reduction program exceed their cost. Optimizing cybersecurity investment to manage cyber risk requires models that estimate how those security investments are likely to reduce risk. Directors will need to ask for estimated impacts of investments from operational units responsible for developing risk remediation proposals.

Boards may not be aware that cyber risk can be measured to support decision process maturity Level 4 and Level 5. The additional reading section at the end of this chapter includes resources for applying the language and logic of quantitative risk to cyber risk.

## Key Questions for Management

1. Does the board approach its governance objective as effective cyber risk management or cybersecurity management? Does the board view the cybersecurity organization a means to the end of effective cyber risk management or an end in itself?
2. How does the board view cyber risk governance—as a compliance goal or as an evidence-based, continuous improvement problem?
3. How does the board define its cyber risk appetite? What is that risk appetite?
4. What decision maturity level has the board chosen to govern cyber risk management? Is the board and executive management informed about methods to define and measure cyber risk in the same terms as other enterprise risks?
5. How effective is the board at governing cyber risk and cybersecurity to its risk appetite? What measurements or information does the board need to assess the extent to which management is running the company within the established risk appetite?
6. Is the board getting the right information for effective risk management governance? How is the information the board receives helping it make cyber risk decisions?
7. Do board members find risk metrics presented by management meaningful to support board decisions? What units of measure does the board want to have to measure cyber risk?
8. Are cyber risk metrics in the same units of measure as the risk appetite? If not, why?
9. Do the risk metrics presented adequately inform decisions about alternatives to mitigate risk? How complete is the evidence the board receives?
10. Over time, does the information reported to the board increase its cyber risk intelligence?

## Additional Reading

National Association of Corporate Directors resources are available from its online Cyber-Risk Oversight Resource Center, https://www.nacdonline.org/insights/resource_center.cfm?ItemNumber=20789 (accessed January 24, 2021).

Securities and Exchange Commission, Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2 Cybersecurity, October 13, 2011, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (accessed January 24, 2021).

Securities and Exchange Commission, SEC Public Company Cybersecurity Disclosures, Feb 2018, https://www.sec.gov/rules/interp/2018/33-10459.pdf (accessed January 24, 2021).

Jack Freund & Jack Jones, Measuring and Managing Information Risk (2014).

Douglas Hubbard, How to Measure Anything: Finding the Value of "Intangibles" in Business (2007).

Watts Humphrey, Characterizing the Software Process: A maturity framework (Software Engineering Institute, June 1987), ftp://ftp.sei.cmu.edu/pub/documents/87.reports/pdf/tr11.pdf (accessed February 4, 2021).

Sam L. Savage, The Flaw of Averages: Why We Underestimate Risk in the Face of Uncertainty (2012).

The Open Group, *The Open Risk Taxonomy Standard (O-RT)*, https://publications.opengroup.org/c20b (accessed February 4, 2021).

The Open Group, *The Open Risk Analysis Standard (O-RA)*, https://publications.opengroup.org/c20a (accessed February 4, 2021).

The Open Group, *The Open FAIR Risk Analysis Spreadsheet Tool*, https://publications.opengroup.org/i181 (accessed January 24, 2021).