



**Cyber Risk Governance:  
An Operating Model**

September 2022



## Jonathan Goldsberry

Cyber Risk Senior Manager

Deloitte & Touche LLP

Jonathan is a senior manager in Deloitte's Cyber Risk Practice. In his tenure at Deloitte, he led the creation of the corporate board cyber risk awareness education materials as well as designing and facilitating wargames and tabletop exercises to test both recovery and response activities from technical to board levels. He developed the Ransomware Strategy initiative and leads hunt, incident response, and cyber strategy readiness teams.

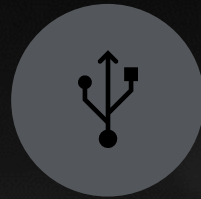
Prior to Deloitte, he ran his own private consulting practice for 14 years, serving his clients as a strategic advisor fulfilling the roles of CIO, CTO and CISO and has over 25 years of experience in IT. Jonathan earned a Master's of Science in Technology Management from Columbia University with a focus on C-Level management of Cybersecurity and possesses multiple technical certifications across numerous facets of technology.

# Introduction

What is cyber risk? What does it mean to government executives?



Cyber risk is multi-dimensional and crosses functional areas and disrupting strategic, operational, and regulatory business activities.



*Cyber is everywhere*—beyond an organization's walls and IT environments and into the products they create and services they provide.



As the world becomes more connected, *cyber threats continue to grow in number and complexity.*



Cybersecurity should not be “bolt-on” after the fact; it must be “baked-in” as a core element of organizational culture.



As a leader, your elevated access to sensitive and valuable company information means *you will likely be targeted.*

# The evolution of cyber risk

The evolution of cyber risk is generally cumulative. That is, the drivers and opportunities in one era do not replace those of the preceding era. Rather, they expand the horizon.

**2005-2012**

**2013-2020**

**2020 and beyond**



Market drivers
  Key Decision Makers
  Key areas of investment

# Cyber risk governance operating model

Cyber risk, like all risks an organization faces, requires established and mature governance and oversight.

An organizations' cyber risk culture is shaped by leaders' actions and decisions.



# Governance

The board and C-Suite sets the culture and “tone at the top” for cyber risk



Boards and organization executives believe oversight of cybersecurity to be a top three concern at the board level, and a top two time commitment<sup>1</sup>

## Some key questions:

- Are cyber risk, crisis management, incident response and enterprise resource management/planning aligned?
- Are we able to monitor, measure, communicate, and manage cyber risks and cyber resilience at all levels, including the board?
- Is there adequate oversight into how cybersecurity investments are made including decisions over architecture, incident response, recovery, and testing?
- Are policies, standards, procedures specific to cybersecurity established, functioning, and measured?
- Is cyber risk “baked-in” to our strategies?
- Do we have the right expertise on cyber risk and do our meetings give ample time for cyber risk discussion?

1. nacdonline.org, “2022 Governance Outlook,” [https://boardleadership.nacdonline.org/rs/815-YTL-682/images/2022\\_Governance\\_Outlook.pdf](https://boardleadership.nacdonline.org/rs/815-YTL-682/images/2022_Governance_Outlook.pdf)

# Talent

Ensuring your organization has optimized the workforce and created an organizational structure that supports cyber needs, to include a cyber aware workforce



Globally, 42% of respondents placed by far the greatest emphasis on the development and retention of existing staff as having the greatest impact on shrinking the cybersecurity workforce gap.<sup>2</sup>

## Some key questions:

- Have we developed a measurable strategy to recruit and retain highly skilled cybersecurity professionals necessary to protect the company?
- Are we organized for success to include aligning roles and workforce structure to improve organizational and technical (as supports the business model) resiliency?
- Are we cultivating the culture to hold each other responsible for cyber policies and leading practices?
- Are programs and measures in place to build a cyber-aware workforce?
- How do we assess our own skill sets including cyber risk readiness and technical savvy as leadership?
- Is our reporting structure appropriate given our cyber risk profile and do we have the right access to the information needed to oversee cyber governance?

2. ISC2.org, "Cybersecurity Workforce Study 2021," <https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx>.

# Integrity

Having systems, processes, and people that do what they are supposed to do—effectively, accurately, reliably, and securely—with the resilience to withstand threats and bounce back quickly from problems, no matter how severe.



Operational disruption is the #1 concern for executives. With businesses increasingly dependent on reliable data, data integrity is the primary concern for organizations<sup>3</sup>

## Some key questions:

- Are we providing the right disclosures and protecting data that could cause insider trading or fraud concerns?
- What are we doing to ensure critical data, including internal Intellectual Property (IP), as well as data of our stakeholder's, is protected, private, and safe from corruption, destruction, or theft?
- Have we taken steps to appropriately empower employees across the organization to identify and call out unethical or inappropriate access to our data sets?
- Do we have the right controls and policies in place to build ethical boundaries, identify insider threats, and account for the cyber issues relative to our threat profile?
- Are we in compliance with all applicable privacy laws? Do we know which privacy laws apply to us?
- Is our team prepared for a potential breach? Do they have the appropriate cyber incident response procedures documented to handle a high profile, brand impacting, crisis inducing event?

3. Deloitte.com, "2021 future of cyber survey," <https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html>



# Compliance

Legal and regulatory issues surrounding cyber risks are growing nearly as fast as the threats themselves. Not only do organizations need to stay on top of rapidly changing technologies, but also in the recently changing laws, regulations, and compliance issues surrounding cyber risks.



83% of organizations studied have had more than one data breach. The average cost of a data breach in the United States was \$9.44 million<sup>4</sup>

## Some key questions:

- Are we meeting the required public disclosures and reporting requirements surrounding cyber-related risks and regulations and have we considered the SEC guidance on cybersecurity disclosures?
- Does our M&A process properly account for Cyber Risks and concerns regarding due diligence?
- Does our Cyber Insurance policy properly account for, and updated for, recently changing regulations regarding privacy and other cyber related risks?
- Are we in compliance with all applicable privacy laws in every region we can be held accountable in?
- Is the proper management in place to stay on top of compliance changes?

4. IBM, "Cost of a Data Breach Report 2022," <https://www.ibm.com/security/data-breach>

# Metrics & Reporting

Organizations collect a lot of data, but putting that data into specific views that provide business-oriented insights that are actionable is often a challenge.



Risk quantification had a considerable effect on data breach costs, saving up to \$2.10 million on average<sup>4</sup>

## Some key questions:

- ❑ Accounting for cyber is about proving a negative or taking a risk-adjusted net present value (NPV) approach and it can be difficult to find fresh, relative data. What do we have in place to ensure we can effectively put a dollar amount on cyber risk and make investments accordingly?
- ❑ Have we adopted a process to effectively translate technology taxonomy to business language?
- ❑ Do we have an index to measure and report risks that cover the enterprise including third-party and consumer facing statistics that can rapidly affect shareholder value?
- ❑ Is the budget for cyber risk adequately mitigating risk, and how does it compare to our peers and competitors?
- ❑ Do our reports enable the right discussions and dialogue when making risk investment decisions?
- ❑ How is our performance relative to our peers, industry, and the maturity goals of the organization?

4. IBM, "Cost of a Data Breach Report 2022," <https://www.ibm.com/security/data-breach>

# Operations

In their oversight role, leaders need to know the right questions to ask and how to monitor the effectiveness of management's plans and responses.



Most US surveyed executives view operational disruption as the biggest fall out from cyber incidents or breaches<sup>3</sup>

## Some key questions:

- Who is the appropriate executive to be leading cyber risk management?
- What are the greatest cyber threats our organization faces?
- What are the 'crown jewels' that we must protect, including data and other assets?
- Do we know what business processes and applications are most critical to operations?
- Do we have a cyber resilience framework that provides a structure for identifying, designing, implementing, and managing the capabilities which improve resilience to cyber attacks?
- Have we considered the impacts of third-party risks? Do we fully understand our operational dependencies?
- Can we withstand operational disruption due to a cyber event? When is the last time we tested our business continuity and disaster recovery plans?

3. Deloitte.com, "2021 future of cyber survey," <https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html>

# Planning

Planning for the ambiguity of an ever evolving, complex threat such as cyber risks means planning to be resilient. While the resources required to be prepared for anything are significant, planning to bounce back, or fail forward, are more agile strategies to reduce both the time and monetary costs of incident response and disaster recovery.



\$2.66 million is the average cost savings associated with an incident response (IR) team and regularly tested plan<sup>4</sup>

## Some key questions:

- Do we have simple, flexible and distributed plans to provide guidance to responsible parties throughout the organization during a cyber event?
- Have we tested our plans and procedures through cyber wargaming and tabletop exercises?
- Are we able to sustain our targeted cyber resilience posture?
- Did we involve business operations in cyber–Incident response planning so that mission critical processes and systems are available when crises occur.

4. IBM, "Cost of a Data Breach Report 2022," <https://www.ibm.com/security/data-breach>

# Performance

Cyber risk operations should be assessed on a regular basis to ensure that current activities are not only in alignment with the strategy, but that the efforts are performing at the level required to meet or exceed the designated risk appetite.



Organizations with XDR (extended detection and response) technologies identified and contained a breach 29 days faster than those without XDR<sup>4</sup>

## Some key questions:

- ❑ What are the metrics (Key Risk and Performance Indicators) we should be watching to understand performance of the cyber risk program?
- ❑ Have we established the appropriate baseline KPIs for our risk appetite?
- ❑ What are some of the key enhancement initiatives currently ongoing and how often should their status be communicated to the c-suite and/or board level?
- ❑ How are other players in our market/industry focusing their time and efforts on cyber risk initiatives?
- ❑ How are we measuring the C-Suites performance in protecting the company?

4. IBM, "Cost of a Data Breach Report 2022," <https://www.ibm.com/security/data-breach>

# Strategy

Cyber risk strategy should be an inherent part of the company direction as set by the board, aligned with the mission of the organization, and protect the best interests of stakeholders.



When asked how often they conduct risk analyses/threat modeling for new and/or existing applications, 37% of CIOs and CISOs indicated they do so quarterly, and 29% do so monthly.<sup>3</sup>

## Some key questions:

- Do we understand our cyber risk threat profile:
  - What makes us a target (including identifying our “crown jewels”)?
  - Who are the likely threat actors, and what is their motivation?
  - What are the likely methods of attack?
- Do we have an enterprise cybersecurity strategy and roadmap to mitigate our threat profile?
- Have we set an appropriate risk appetite regarding cyber risks and established the thresholds for escalation?
- Have we prioritized the risks we’ve identified and do our cyber initiatives align with this prioritization?
- Has our cyber risk strategy been communicated to executives and translated to operations?
- Are we spending our money in the right spot to mitigate risk?

3. Deloitte.com, “2021 future of cyber survey,” <https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html>

# Some questions leadership should consider asking



Is cyber risk “baked-in” to the company strategies?



Are we building a cyber risk intelligent culture?



Are we adequately protecting critical data, IP, as well as data belonging to any of our stakeholders?



Are we in compliance with all applicable privacy laws in every region we can be held accountable in?



Do our reports enable the right discussions and dialogue when making risk investment decisions?



What are the greatest cyber threats to our operations?



Do we have simple, flexible, and distributed plans to provide guidance to responsible parties throughout the organization during a cyber event?



How are we measuring our cyber risk posture and performance?



Is our cyber strategy aligned to our cyber risk threat profile?



Do we have the right leadership and organizational talent to execute a viable risk mitigation program?



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.