October 2021

Cyber Oversight Effectiveness Development

A New Approach for Boards of Directors

tapestry NETWORKS

CLTC Center for Long-Term Cybersecurity
UC Berkeley

King & Spalding

Cyber Oversight Effectiveness Development: A New Approach for Boards of Directors

TABLE OF CONTENTS

I. Introduction

Cyber Oversight Effectiveness Development (COED) is a new approach for building a board's capabilities as it oversees cybersecurity risk and provides strategic leadership in this critical area. Nearly every large public company board has made significant investments in cybersecurity, enhancing human capabilities in both management teams and boards and allocating major capital to secure their IT infrastructures. But we regularly hear from directors that these are no more than steps on a long journey. Even in a company where internal management of cyber risk appears strong, the board of directors can worry that its oversight may not be adequate—or that it has no reliable way to assess its adequacy or to compare its capabilities with those of boards of other firms.

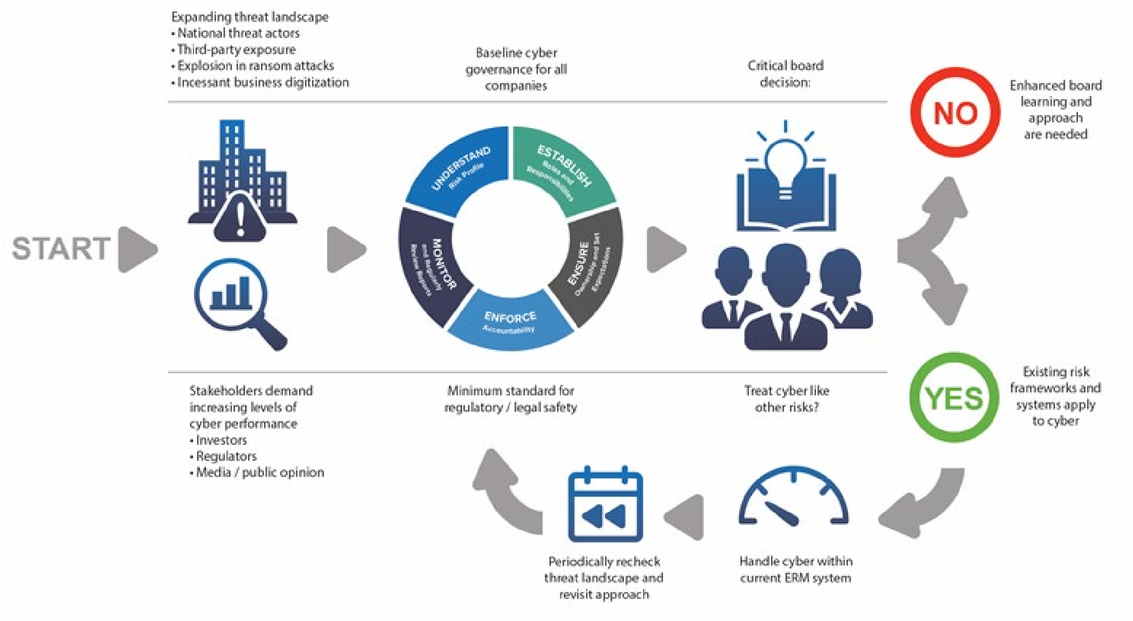
Even where internal management of cyber risk appears strong, the board of directors can worry that its oversight may not be adequate – or that it has no reliable way to assess its adequacy or to compare its capabilities with those of the boards of other firms.

COED seeks to address this gap. It is predicated on the belief that cyber risk often requires fundamentally different treatment than other risks, such as health and safety or fraud. Directors, executives, company secretaries, and others who care deeply about effective governance are the intended audience for this report and for the COED approach.

COED was developed by Tapestry Networks, the Center for Long-Term Cybersecurity (CLTC) at the University of California, Berkeley, and King & Spalding. Many of the key insights in this report stem from conversations with members of the Cyber Risk Director Network (CRDN), a multiyear initiative led by Tapestry Networks in collaboration with King & Spalding and CLTC, and with the financial sponsorship of King & Spalding.

Cyber risk is in constant evolution, driven by an insatiable demand from consumers and corporate leaders for information density, ubiquity, accessibility, and the like, and by a large and constantly evolving set of attackers with a wide range of motivations. Any model for assessing oversight must therefore be dynamic; it cannot move in a linear way from low performance to a static high-performance equilibrium, because today's excellence will be inadequate for tomorrow's challenges.

Before pursuing enhanced cybersecurity oversight, every organization should ensure that it meets minimum expectations for cyber oversight, as described in the following section. The risk of litigation or regulatory intervention means that all boards should achieve this baseline level of oversight, but other factors may prompt a board to invest further in its cyber oversight. *These factors are outlined on page 12.*


START
Expanding threat landscape
• National threat actors
• Third-party exposure
• Explosion in ransom attacks
• Incessant business digitization
Baseline cyber governance for all companies
Critical board decision:
NO
Enhanced board learning and approach are needed
UNDERSTAND
Risk Profile
ESTABLISH
Roles and Responsibilities
ENSURE
Ownership and Set Expectations
ENFORCE
Accountability
MONITOR
and Regulatory Review Reports
YES
Existing risk frameworks and systems apply to cyber
Stakeholders demand increasing levels of cyber performance
• Investors
• Regulators
• Media / public opinion
Minimum standard for regulatory / legal safety
Treat cyber like other risks?
Periodically recheck threat landscape and revisit approach
Handle cyber within current ERM system

In these situations, we propose going from basic board education to board evolution. The enhanced oversight we recommend includes many well-known board actions for individual and collective learning—threat awareness, simulations, war games, and scenario planning—but it assumes that these will be repeated and adapted as the threat landscape shifts. The goal is increased speed of adaptation (getting better faster) rather than achievement of a stable outcome (getting to good, or even to great). We can understand this approach through an analogy to athletics or music, where even the most accomplished practitioners constantly hone both basic and advanced skills, repeating an unending cycle of assessment, improvement, and reassessment. In cybersecurity, this is essential because attackers, like biological viruses, are also in constant evolution.

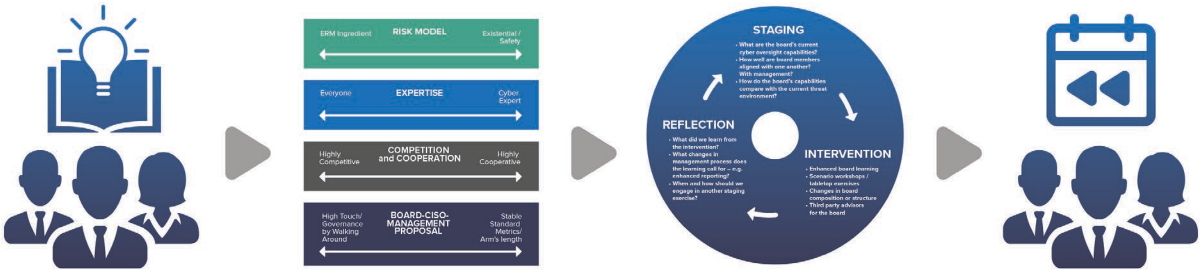
In each cycle, the aim is to increase board members' individual and collective self-awareness, moving from an emergency ad-hoc posture … toward a stance that is both proactive and resilient.

COED, therefore, starts with basic oversight but goes further, with three board actions that repeat over time:

- **Staging** creates a snapshot of where the board is at a given moment, and COED provides diagnostic tools to help establish this snapshot. *See diagnostics described starting on page 166.* It is also at this point that the board's location within five developmental stages is determined. *See page 14 for a description of the five stages.*
- **Intervention** comprises board actions—including education, reorganization, seeking out internal and external expertise, running war games, and engaging in scenario planning—to accelerate learning and move the board toward greater cyber-risk capability and confidence. *See page 23 for potential interventions.*

- **Reflection** involves measuring the impact of the interventions. The approach then cycles back to a new round of staging and repeats over time, ideally on a cadence determined by the board's view of the threat environment and its own needs.

In each cycle, the aim is to increase board members' individual and collective self-awareness, moving from an emergency ad-hoc posture—where the board has little choice but to accept management's guidance on the threat landscape, the company's handling of it, and the questions the board should be asking—toward a stance that is both proactive and resilient, where the board and management share an anticipatory view both of the threat landscape and of the capabilities the company will need to prosper in the emerging environment.


ERM Ingredient
RISK MODEL
Existential / Safety
Everyone
EXPERTISE
Cyber Expert
Highly Competitive
COMPETITION and COOPERATION
Highly Cooperative
High Touch/ Governance by Walking Around
BOARD-CISO-MANAGEMENT PROPOSAL
Stable Standard Metrics/ Arm's length
STAGING
• What are the board's current cyber oversight capabilities?
• How well are board members aligned with one another? With management?
• How do the board's capabilities compare with the current threat environment?
INTERVENTION
• Enhanced board learning
• Scenario workshops / tabletop exercises
• Changes in board composition or structure
• Third party advisors for the board
REFLECTION
• What did we learn from the intervention?
• What changes in management process does the learning call for – e.g. enhanced reporting?
• When and how should we engage in another staging exercise?

Enhanced board learning and approach are needed

Diagnostics help clarify current board alignment

Begin cycle of learning, continuing as threat landscape evolves

Periodically revisit approach

There are several considerations when implementing enhanced oversight, including whether it is carried out by the full board or smaller subsection of the board, such as a board subcommittee; whether to initiate the process under legal privilege; and what role management will play in the process. *See page 26 for implementation considerations.* Finally, it may be helpful to understand how COED would be implemented practically in a complex business environment using a fictional case study. *See page 28.*

II. Context and baseline requirements for cyber oversight

Boards exercise oversight of all risks in three ways, both continuously and in parallel, which in the case of cyber risk can play out as follows:

- **Direct or operating oversight.** The board works with management on immediate threat response, protection, and compliance. The board's role is not to substitute for or second-guess management but to ensure, mostly by asking questions, that management is going as far and as fast as possible in the immediate circumstances. Individual board members with specific skills may be pulled in to deliver particular advice or challenge. The intensity of direct oversight will vary over time; for example, it may increase after a major breach.
- **Resource oversight.** The board assures itself that assets and resources are in place for the longer term. These include tangible assets (e.g., network infrastructure), human capital (talent), and financial protection (insurance) and resilience (solvency, redundant capabilities).
- **Strategic oversight.** The board establishes the company's competitive positioning, risk appetite, innovation, and the like and ensures that management is acting accordingly. This means higher levels of engagement in how management conceives and organizes functions like product design, so as to push cybersecurity considerations down the organization. The board also plays a role in developing and implementing a value-creation mindset and strategy attached to cybersecurity.

The relative weight of the three forms shifts situationally. Strategic oversight will often take on more weight as boards become more effective. The intensity of oversight will also vary by industry sector and over time. In the nuclear power industry, for example, safety concerns have led regulators to demand that their own oversight and that of directors be "intrusive": not second-guessing management or going beyond oversight but asking more detailed questions than a board might typically do.[1] A director has suggested that similar issues might lead to "intrusive oversight" for cyber risk.

Unlike almost any other risk, the likelihood and impact envelope of cybersecurity is difficult to measure and can range from harmful to disastrous.

Virtually every director we speak with acknowledges that cyber risk is new and highly challenging for boards. Unlike almost any other risk, the likelihood and impact envelope of cybersecurity is difficult to measure and can range from harmful to disastrous. As almost every company pursues greater digitalization, cyber is an escalating risk. It forces companies to look beyond their own walls, as they must assess and mitigate threats originating with suppliers, partners, distributors, and even customers.

In such a dynamic environment, even full-time cybersecurity professionals are challenged to stay ahead; the majority of directors lack direct personal experience in dealing with cyber risk.

Risks arise not only from the actions of distant actors, such as criminal gangs and leaders of nation-states, but also closer to home, such as from the actions of employees or third-party providers. The motivations of external attackers are often unclear or obscure, making it difficult to anticipate their moves. Threat actors operate outside the bounds of international rules and norms. They rapidly adopt new technologies and find new vulnerabilities to exploit—vulnerabilities often enabled or created, whether knowingly or unknowingly, by internal factors such as employees or third-party partners. In such a dynamic environment, even full-time cybersecurity professionals are challenged to stay ahead; the majority of directors lack direct personal experience in dealing with cyber risk.

Given the daunting characteristics of cyber risk, does effective board oversight call for extraordinary board capabilities and actions? Answering this question is a first and crucial step.

Some companies are not even at the stage of making a decision on how to handle cyber risk, as they have not yet taken even the baseline steps of cyber hygiene demanded by regulation and legal prudence. *These baseline actions are outlined in the following section.*

Some boards, once they have established basic oversight, may reasonably conclude that cyber risk can be handled using standard enterprise risk management (ERM) approaches. In our experience, such a decision should not be taken without careful deliberation

[1] Institute of Nuclear Power Operators, *Convention on Nuclear Safety Report: The Role of the Institute of Nuclear Power Operations in Supporting the United States Commercial Nuclear Electric Utility Industry's Focus on Nuclear Safety* (Institute of Nuclear Power Operators, 2007); US Nuclear Regulatory Commission, *The United States of America Seventh National Report for the Convention on Nuclear Safety* (US Nuclear Regulatory Commission, 2016).

and, possibly, external counsel. More often than not, boards have underestimated the operational and strategic impact of cyberattacks on their companies.

COED provides for boards that have decided to manage cyber risk in a fundamentally different way than they handle other strategic and operating risks, instead choosing to engage in an accelerated, continuous program of learning and development.

With more established risk domains, such as financial control or operating safety, an independent director will generally have an independent framework for questioning management. Directors will not have management's detailed on-the-ground knowledge of company operations, but they will have their own perspective of a risk area, often formed from previous leadership experience. The chair of an audit committee, for example, will often have been a CFO, and will not rely on the company's CFO or controller to indicate what questions to ask about financial controls or asset impairment decisions. An independent perspective helps directors decide how to balance the three forms of oversight and when and how to move to "intrusive oversight."

Attackers have a structural advantage over defenders: they only have to succeed a few times, or even once, while defenders have to succeed nearly all the time.

To help directors achieve similar independence around cyber risk, COED aims to make the board a learning organization. The objective is to have boards conduct all three above-mentioned forms of oversight at a higher and more precise level than most are currently doing, and to make this development continuous. A visual analogy might be a spiral staircase that ascends infinitely.

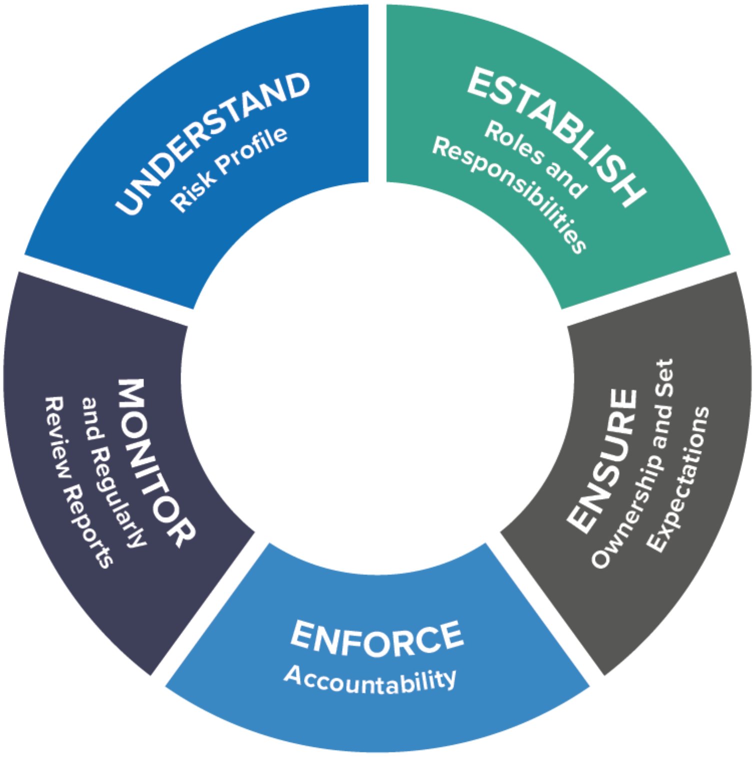
An important objective is to enhance the speed of ascent. Attackers have a structural advantage over defenders in the digital environment: they only have to succeed a few times, or even once, while defenders have to succeed nearly all the time. Cyberattackers have the added advantage of being able to innovate without the constraints of rules or laws. Failed attacks cost attackers very little, and attackers are unlikely to be caught or punished. The table is tilted in their favor, which is why the defenders need to learn speedily if they are to have a chance of leveling the field.

Implementing baseline cybersecurity governance

COED begins with cybersecurity oversight practices that the board of every large company, in every industry, should consider foundational. These practices will help meet a baseline level of expectations, such as those of regulators or of investors. There are many tools available to support this baseline work, including guidelines from the National Association of Corporate Directors.

Directors have found the following model for baseline governance both comprehensive and practical.

Figure 1. Five key areas of focus for baseline cybersecurity governance


UNDERSTAND
Risk Profile
ESTABLISH
Roles and Responsibilities
ENSURE
Ownership and Set Expectations
ENFORCE
Accountability
MONITOR
and Regularly Review Reports

Baseline governance may not be sufficient, given a company's strategic direction or risk profile, but it is a necessary first step. Before even considering whether to go further, every board should carry out an assessment to learn whether or not they are currently achieving this baseline. Such an assessment represents only a snapshot in time, and even baseline cybersecurity governance requires regular reconsideration and adjustment. Boards may undertake reassessment on a regular schedule—annually or biannually, for example—or a reassessment may be triggered by an external shift in the threat landscape.

Understand the risk profile

A board needs to understand its company's risk profile and how this might evolve over time. Cybersecurity risk varies from company to company and is determined by factors including the organization's current level of digital hygiene, the industry in which it operates, its operational needs, and its vendors and suppliers. Boards must also understand the external threat landscape, how threat actors are evolving, and the implications for the organization. Further, the company's legal liabilities related to cybersecurity should be well understood. The regulatory landscape surrounding cybersecurity and privacy continues to evolve at a rapid pace and can affect the risk profile of an organization, particularly in regulated industries like financial services.

Boards would also be well advised to discuss the cybersecurity risk appetite of the organization, as this can make revealed preferences more explicit and help to establish triggers for incident escalation. Though board members are not expected to know intricate technical details, a high-level understanding across the breadth of the risk profile is essential. At the start, an extensive board assessment of the organization's cybersecurity risk profile may require significant time commitment, but future reassessments become easier to update and review. Evaluating the organization's vulnerabilities and weaknesses in these areas, as well as understanding the evolving nature of the threat landscape, is perhaps the most vital aspect of effective cybersecurity governance as it drives decision-making and establishes needs for the rest of the organization.

> Boards would be well advised to discuss the cybersecurity risk appetite of the organization, as this can make revealed preferences more explicit and help to establish triggers for incident escalation.

Establish roles and responsibilities

Roles and responsibilities must be clearly defined and communicated at both the board and management levels, giving particular consideration to the following factors:

- **Board oversight structure.** A variety of approaches exist for board-level cybersecurity oversight. Boards constantly adjust which committee should have primary responsibility for cyber issues. Many assign cyber risk to the audit committee, but some delegate it to another existing committee or to a special cybersecurity or technology committee. Some boards have the full board oversee it. Experts say that there is no one-size-fits-all approach; what is most important is to ensure that cyber risk is receiving a level of oversight appropriate to the organization's risk profile and is not assigned to a committee lacking the necessary skills or bandwidth.
- **Board skills.** Directors need to ensure that the board has the skills necessary for cyber-risk oversight. Many boards have added a technology expert, such as a former chief information security officer (CISO); others do not see such a "cyber director" as a necessity. In every case, boards should consider the skill sets of the directors charged with this area of oversight and ensure a base level of technological comprehension and an understanding of the key issues. Further, boards should ensure

that outside directors, no matter how skilled, do not step into the role of management, since this can create dysfunctional tension and weaken board-management communication.

Ensure board and management ownership and set expectations

In addition to establishing roles and responsibilities, boards and management should create consistent expectations with management regarding issues such as incident response, escalation policy, and decision rights in the event of different forms of attack—for example, deciding whether to pay a ransomware demand or when and how to inform the media about a breach. Often, when a breach or attack is first detected, the full scope of the situation is not immediately obvious. As the investigation proceeds, understanding may rapidly evolve. Establishing a policy and process for escalating communication to senior management and to the board is important to reduce uncertainty and ensure the board is apprised of critical information.

Establishing a policy and process for escalating communication to senior management and to the board is important to reduce uncertainty and ensure the board is apprised of critical information.

An incident response plan can also have unambiguous triggers that engage the company's legal department so that an investigation can be protected under attorney-client privilege. Boards should make certain that the escalation policy is practical, avoiding the escalation of immaterial incidents and "information overload." The policy will vary by organization and can be tricky to establish via quantifiable factors, so boards and management should ensure they communicate and agree upon principles in this area.

Enforce accountability

As noted, the board depends on management to effectively oversee cybersecurity. Boards should understand management's responsibilities around cyber risk and enforce accountability in this area. In some cases, management bonuses are tied to cybersecurity outcomes and the performance of the organization in cyber crises. Even where there are not explicit cyber-bonus metrics, readiness and response can be included in the board's assessment of the CEO.

Monitor and regularly review reports

Board oversight of cyber risk depends heavily on reporting from management. Reporting to the board on cybersecurity can be difficult because of the technical nature of the subject matter and the various ways in which information can be presented, which makes a thoughtfully constructed reporting dashboard critical. Directors must understand the issues well enough to provide effective oversight without having to master technical information and jargon that is likely to change rapidly. Management must communicate risks clearly enough for directors to understand their severity and strategic implications.

Board directors should establish who from senior management will brief them on cybersecurity issues, and how often. Candidates include the chief information officer and the CISO, among others. Third parties can also help a board better understand the most important risks, and boards increasingly meet directly with cybersecurity consultants and other outside experts to get an unvarnished view of the organization’s risk profile.

III. Going beyond the baseline

When might a board decide to invest further in its cyber-oversight capabilities? Several situations might prompt the decision, as well as certain types of firms. Many firms may fit into two or more such categories, and boards of firms that do not fit into any of them may still decide that it is prudent to invest in a higher level of board readiness. Boards of certain types of companies (e.g., financial services firms) may already be highly developed in their oversight of cyber risk, but even sophisticated boards need to consider when further investment is warranted. Firms serving end consumers may be more inclined to invest than those serving businesses, but there are many reasons why the board of a business-to-business firm might decide to increase investment, and the distinction may become less relevant over time.

Figure 2. Deciding to invest further in cyber-oversight

Firm-specific factors	Post-crisis situations	Major systemic risk	Global supply chains
• Critical cyber or tech infrastructure providers • Firms where digital security is a critical element of the value proposition (e.g. autonomous vehicle makers) • Firms at the leading edge of technology (e.g. biotech, virtual reality providers)	• Firm has been a victim of major ransomware attack • Major competitor has been a similar victim • Recent CISO turnover, or board doubts CISO capabilities • Merger derailed because of insufficient cyber capability	• Financial services where a large cyber incident could become a national crisis • Sectors where a cyber breach could have widespread health and safety impact (e.g. power generation, airlines, hospitals)	• Firm dependent on global supply chain performance • Numerous suppliers and logistics providers • Complicated internal logistics requiring IT-driven coordination (e.g. cross-dock manufacturing)

The following circumstances and conditions could prompt a board to increase its investment in cyber oversight:

- **When cybersecurity is a significant element of value creation for the firm.** Examples include the following:
  - Technology firms that are critical supply-chain players for cyber infrastructure (e.g., SolarWinds) or that supply critical technology products and services to a large customer ecosystem (e.g., Microsoft, Zoom, Google, Apple).
  - Firms for whom security risks substantially constrain the rate of innovation and for whom digital security is an underleveraged opportunity for differentiation and playing offense. Companies in such arenas as healthcare, home internet of things, autonomous vehicles, gaming, and advanced manufacturing, as well as certain media firms and professional-services firms that steward customer data, might fall into this category. We believe that more firms will likely

  find themselves in this category over time—for example, firms in the retail and hospitality sector.

  - Firms at the leading edge of technology development, such as biotech and augmented or virtual-reality firms (both consumer facing and providers of industrial simulations). These are particularly vulnerable to industrial espionage and data manipulation attacks.

- **When a cybersecurity crisis reveals that the board needs substantially improved capabilities to fulfill its governance responsibilities.** Examples include the following:

  - Firms that have been victims of major attacks (e.g., data breaches, sophisticated ransomware, data manipulation attacks). Companies whose direct competitors have been victims may also see a stronger case for investment, but while "a major competitor of ours has just been hacked" will naturally prompt a board to reexamine its oversight activities, it should not be thought of as either a necessary or a sufficient condition for increased attention and investment.

  - Firms with a much higher than average CISO turnover rate and/or firms whose boards lack confidence in the CISO.

  - Firms that suffered the derailment of a high-stakes merger or had a merger fail to deliver expected returns because of cybersecurity. Firms with significant merger-and-acquisition activity, based either on the number of acquisitions or their scale, might also proactively invest before an event occurs or a systematic vulnerability is uncovered.

- **Firms in sectors in which a cybersecurity failure could prompt a cascading crisis:**

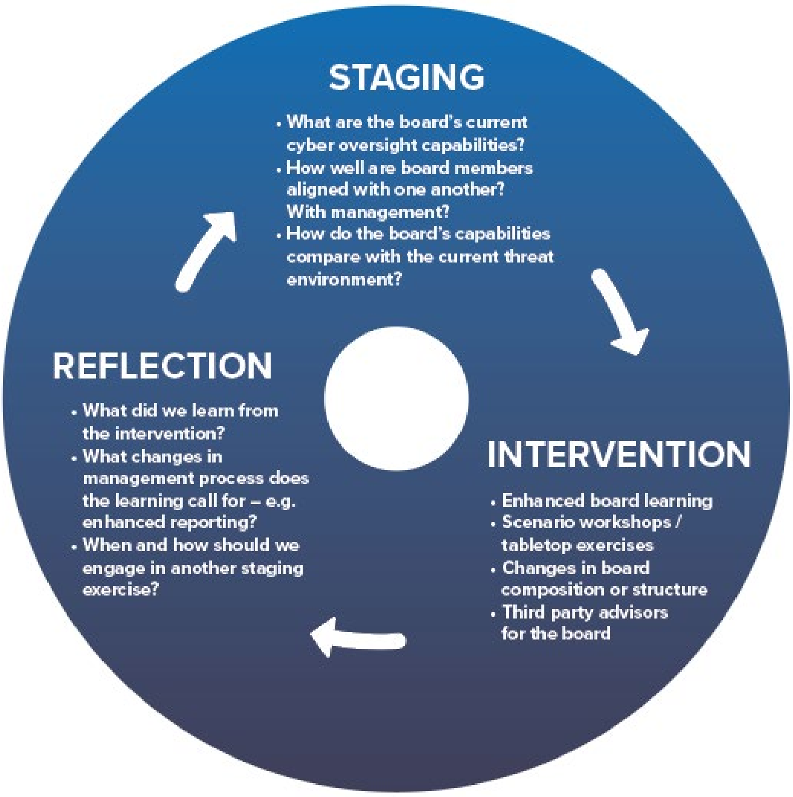
  - The financial sector, in which a major cybersecurity incident could prompt a national or even a global crisis.

  - Sectors in which a cyber breach would have major physical or health-and-safety consequences, including transportation (e.g., the airline, automobile, and aerospace sectors), infrastructure and energy (e.g., power generation and distribution, water supply, oil and gas transmission), hospitals, logistics companies (e.g., vaccine distribution).

- **Firms facing significant global supply-chain risk**

The enhanced cyber oversight that a board may decide to adopt typically involves three repeating steps: staging, intervention, and reflection. *See figure 2, below.*

Figure 3. Three steps of enhanced cyber oversight


STAGING
• What are the board's current cyber oversight capabilities?
• How well are board members aligned with one another? With management?
• How do the board's capabilities compare with the current threat environment?
INTERVENTION
• Enhanced board learning
• Scenario workshops / tabletop exercises
• Changes in board composition or structure
• Third party advisors for the board
REFLECTION
• What did we learn from the intervention?
• What changes in management process does the learning call for – e.g. enhanced reporting?
• When and how should we engage in another staging exercise?

Staging

Staging is the process of establishing a snapshot of where the board is at a given moment.

Staging is the process of establishing a snapshot of where the board is at a given moment. COED identifies five stages of board development, each with dimensions that we believe can be assessed and even benchmarked:

- **Ad hoc stage:**
  - Some board members may have experience relevant to cyber, but it does not represent a prominent part of their qualifications.
  - Technical knowledge is more or less random; board members don't really know what other board members know and may not have a good understanding of what

    other board members assume and believe about the risk landscape.

    - Directors understand questions to ask management to ensure compliance, but beyond that, the board isn't taking an independent view of cyber risk. Directors may feel intimidated by technical details, and the board takes cues from the CISO and other executives on the questions it should be asking.

- **Self-aware stage:**
    - Board members know more about what they don't know and have a better understanding of dispersion of beliefs and assumptions amongst their colleagues.
    - Directors seek education, probably through standard and mostly high-level programs on an as-needed basis. They have a reasonable understanding of where technical, legal, economic, and regulatory expertise relevant to cybersecurity is available to them.
    - Directors understand their structural disadvantage with regard to the CISO and are trying to compensate with questions that go beyond compliance.
- **Intentional stage:**
    - The board seeks in-depth education in specific areas, possibly allocated among different directors. (Some might learn about breach detection, some might learn about attribution, etc.) This search goes beyond standard offerings and may involve bespoke briefings by outside experts, with a multiyear learning plan.
    - Directors have a clear idea of where to find relevant experience when they want it and can judge how much of it is useful.
    - At least some directors are engaged in tabletop exercises and simulations, likely alongside management, using these to create closer and more balanced ties to the CISO.
- **Adaptive stage:**
    - Directors seek out better knowledge on emerging cybersecurity issues, from both inside and outside the firm. They have a repeatable means of assessing their own knowledge and an ongoing education agenda that is revised on a regular basis.

    - What counts as "relevant" experience changes as new cyber issues rise to the board level.
    - The CISO and the board interact regularly and often informally around emerging issues; questions to the CISO are more open ended ("How might we …").
- **Resilient stage:**
    - Directors have a well-developed point of view on the future landscape and how risk is changing.
    - This view is supported by knowledge of emerging technologies relevant to cyber and an informed perspective on threats that have not yet been invented.
    - The CISO and board engage around long-term futures (possibly three years out) to build and deploy anticipatory capacities and technologies.

As the technology, regulatory, and threat landscapes co-evolve, boards will repeatedly traverse these five stages. A learning organization would likely cycle through some of the earlier stages, and possibly all of them, for each emerging major risk category. The more discontinuous and radical the change in the threat environment, the further down the spiral staircase the organization is likely to find itself when starting a new cycle of response. "Getting better" means improving the speed with which the board advances up the spiral.

As boards continue their upward progress, cybersecurity as an element of valuation creation will likely grow in proportion to the effort and attention required to address it.

As boards continue their upward progress, cybersecurity as an element of value creation for the firm will likely grow in proportion to the effort and attention required to address it, and cybersecurity will be seen not only as a hazard but as a source of opportunity.

Key diagnostic exercises

For boards that decide to move beyond baseline oversight, a critical first step is to understand where the board itself is or is not in alignment around cyber risk. COED provides two diagnostic exercises, developed at the Center for Long-Term Cybersecurity (CLTC) at the University of California, Berkeley, and drawing on a large set of interviews with board members. Their purpose is not to score or grade a board but to uncover areas where there are internal gaps in alignment.

The diagnostics build on the axiom that a learning organization doesn't need to be (or aim to be) "right" at any single moment. Rather, it needs to be intentional about the direction it seeks to go, and that kind of intentionality is enabled when individual board members and the board as whole understand where they agree and disagree and, most importantly, know what they are uncertain about as they assess the internal and external environments in which they are operating.

First diagnostic: location on four continuums

For the first diagnostic, board members need to articulate three sets of beliefs as precisely as possible and then hold those up to the light:

1. Strategic assumptions about the threat and risk environments in which the firm is operating, which, in most cases, include both officially proclaimed beliefs and views held quietly or privately.
2. Inward-facing assumptions that individual board members may hold—again, often implicitly and/or privately—about what other board members believe and why they hold those beliefs. Put simply, these are places where individual board members disagree with the espoused strategy (as in 1, above) and/or with one another.
3. Awareness around the most important areas where directors feel uncomfortably uncertain as they assess the internal and external environments in which they are operating.

These beliefs are mapped on dimensions that CLTC developed in an earlier study[2] and termed "dynamic tensions." *See figure 3, below.* These may not be the only dimensions that are relevant at this level of significance, and the exercise can be modified to accommodate other dimensions. There is value in keeping the overall number of dimensions relatively small, however, so that the exercise yields manageable results that illustrate the variation in board members' beliefs regarding what they are now doing, what they believe they should be doing, and why.

We propose that a healthy board process for cybersecurity governance should do the following:

- Locate self-consciously and explicitly on each of the dynamic tensions, so that board members know where the board is and why it has chosen to be there.
- Understand the pros and cons of each choice. Boards should actively work with management to multiply the upsides and de-risk the downsides of their choices.

[2] Center for Long-Term Cybersecurity, Resilient Governance for Boards of Directors: Considerations for Effective Oversight of Cyber Risk (CLTC and Booz Allen Hamilton, 2020).

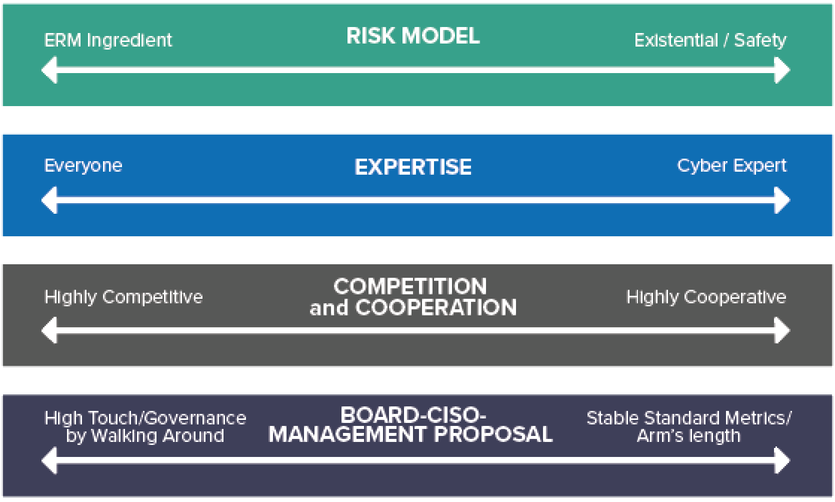
- Regularly reevaluate the landing spot on each dynamic tension to test for changes in the threat landscape or business environment.
- Grade both for effectiveness and adaptability. Boards need to know not only how well the enterprise is managing cybersecurity but also how effectively their oversight is adapting over time.

Many see cyber as a fundamentally distinct category of risk, often an existential or "safety" requirement that must be in place before any other risk can be addressed.

The four dynamic tensions address four fundamental questions facing every board; these questions have complicated and interdependent answers, with no choices that are either optimal or unchanging over time:

1. What is our overall risk model for cyber?
2. How do we access cyber expertise on the board?
3. How does cybersecurity fit into our competitive strategy?
4. How do we share information with management, especially the CISO?

Figure 4. The four dynamic tensions


ERM Ingredient
RISK MODEL
Existential / Safety
Everyone
EXPERTISE
Cyber Expert
Highly Competitive
COMPETITION and COOPERATION
Highly Cooperative
High Touch/Governance by Walking Around
BOARD-CISO-MANAGEMENT PROPOSAL
Stable Standard Metrics/ Arm's length

These four dynamic-tension continuums can be described as follows:

1. **Risk model.** Some boards treat cyber as a business risk like any other, fitting it into the existing ERM system; we call this the ERM side of the continuum. But many see cyber as a fundamentally distinct category of risk, often an existential or "safety" requirement that must be in place before any other risk can be addressed. These beliefs can shift with external events, such as a high-profile ransomware incident.

2. **Expertise.** Boards make choices about how to access the knowledge that informs oversight. Should they reserve a seat for a single highly knowledgeable cyber expert to whom other members turn for help? Or do all board members need baseline knowledge about cyber-relevant technology? Boards must determine how much expertise is necessary and how much authority should be delegated, as well as whether to create a board technology or cybersecurity committee.
3. **Competition versus cooperation.** The third dynamic tension is around the right balance between cooperation and competition with other enterprises when it comes to cybersecurity. Does the board treat cybersecurity as a collective good, supporting initiatives for cooperation—for example, information and threat-intelligence sharing—or does it try to compete over cybersecurity? Historically, banks have competed on the basis of how securely they protect money, so why should they naturally cooperate now when it comes to protecting data?
4. **Board-CISO management protocol.** Boards structure their oversight relationships with management in different ways. Some try to maintain a strict line between the board and management, relying heavily on metrics and dashboards. They look to the CISO to provide plain-speaking translations of technical concepts and an overview of what is being done to keep the company safe. Some directors worry that existing metrics lean too heavily toward showing how much progress has been made against yesterday's threats. They not only seek third-party input but strive for a much more granular relationship with the CISO and employees further down the organization. They want to hear what keeps the CISO up at night and how things could go wrong. Building these relationships requires a "walking around" approach. It does not scale easily, and it is subject to its own misinterpretations. It can be hard to translate such interactions into the kinds of high-level governance and oversight decisions that boards ultimately need, but many directors say that they cannot do their jobs without more of this kind of input.

To conduct the exercise, individual board members are asked to place a mark (X) on each dimension at the point where they think their board currently operates; this is called the "is." They then place another mark (Y) on each dimension at the point where they think their board ought to be; this is called the “ought.” Then board members are asked about their own degree of confidence in their answers. The collated results reveal the degree of consensus across board members—in other words, strategic assumptions become visible by examining where board members agree and disagree on the “is” and the “ought.”

An independent third party collates these results and reports back to the board on points of agreement and difference. These results then provide a strong foundation for a disciplined strategic discussion about where, why, and how these important, but sometimes nonintentional, decisions were made. The discussion progresses to what should change and why, along with what it would take to move closer to the desired “ought” from the current “is.” The objective of this exercise is stronger alignment, along with an awareness of how that alignment reflects assessments of facts and uncertainties in the strategic and internal environments. It is an exercise that can easily be repeated, possibly on an annual basis, to assess both change and progress.

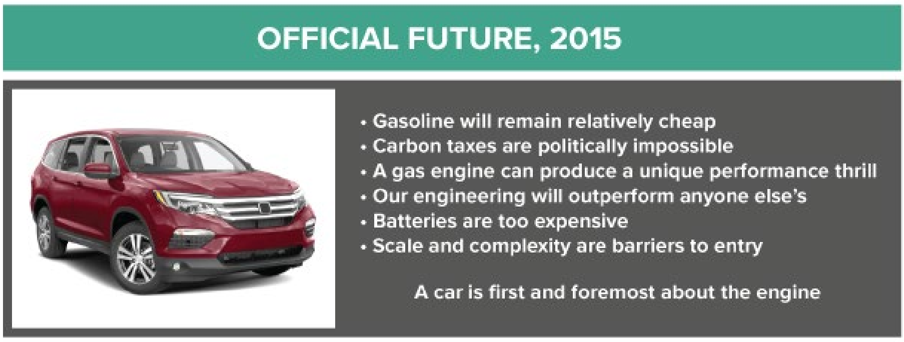
The objective of this exercise is stronger alignment, along with an awareness of how that alignment reflects assessments of facts and uncertainties in the strategic and internal environments.

Second diagnostic: the company’s “official future”

The second diagnostic is an official-future exercise. The concept of an official future was developed by scenario-planning experts as a way of extracting deeper beliefs and assumptions from what economists call “revealed preferences.” In plain English, it means asking, What would you have to believe about the business and the external business environment in order for your current actions to be a rational response? Put another way, What beliefs about the business and the external business environment do your current actions imply that you hold?

Consider the imaginary official-future exercise below, which might have been done to try to understand why a major auto manufacturer took as long as it did to invest in electric vehicles.

Figure 5. Official-future exercise



OFFICIAL FUTURE, 2015

- Gasoline will remain relatively cheap
- Carbon taxes are politically impossible
- A gas engine can produce a unique performance thrill
- Our engineering will outperform anyone else’s
- Batteries are too expensive
- Scale and complexity are barriers to entry

A car is first and foremost about the engine

To get to this simple distillation, an outside team would have interviewed and held workshops with relevant executives, board members, and possibly key customers, investors, and other professional-services providers to derive the key statements below. It's worth emphasizing again that these official-future components might not necessarily be what the company would have been saying to the world or even internally. Instead, it is a third-party parsing of what they were actually doing (in terms of product mix, research and development priorities, engineering decisions, merger-and-acquisition interests, and external-facing communications), from which fundamental beliefs were then reverse-engineered and inferred. This set of beliefs are those for which the company's actions would represent a logical and rational response.

This exercise leads to a deeper and more shared understanding of current board practices and the revealed rationale for those practices.

To run a similar exercise to reveal a board's beliefs about cyber risk and cyber governance, we would begin with what the board currently does in its oversight practices (the revealed preferences) and then reverse-engineer to pull out the assumptions against which those practices appear to be optimized. Those assumptions, explicitly stated, then become the center of discussion and investigation. Does the board actually believe those assumptions? If so, with what level of confidence? What evidence could be collected to evaluate and refine them? How confident is the board that these assumptions are stable, and what evidence would it need to see to change those assumptions, and then the actions, processes, and decisions that spring from them? If the board doesn't believe them and/or if there is insufficient evidence to support them (even as strategic assumptions), why is it acting as if it did?

An obvious contemporary example might be assessing the official-future belief set that grounds a decision to move a significant proportion of data storage, management, and processing from on-premises data centers to the cloud—or to go in the opposite direction. What would you need to believe—about the firm, its technical capabilities, its risk profile and risk tolerance, the value of its digital assets, and more—and what would you need to believe about the threat environment and about the regulatory, competitive, and reputational environment in order to have the decision you are making be a rational one?

This exercise leads to a deeper and more shared understanding of current board practices and the revealed rationale for those practices. It helps untangle known knowns from known unknowns, grounded assumptions from simple beliefs, and blind spots from reasonable heuristics and rules of thumb that boards (like all strategists, governance bodies, and decision makers) rely upon.

From experience, one of the most valuable outputs of these kinds of exercises is the ability to articulate in fairly precise terms a relatively small number of *critical uncertainties*. Critical uncertainties are those that are simultaneously most important and most uncertain in the board's decision making—the two or three most critical questions that a board member would ask an infallible oracle, if given the opportunity. Critical uncertainties are often fulcrums around which change and evolution take place, and seeing them as clearly as possible in a shared light will help boards to allocate resources and attention most efficiently.

Going back to the example of cloud migration above, for some boards, the most critical uncertainties might relate to their future competitive positioning with the cloud provider itself. For others, the most critical uncertainties might involve the nature of a potential cyberattack (state-sponsored vs. criminal vs. hacktivist). Where are the most serious threats likely to originate, and who can be mobilized as allies against them?

Applying the diagnostics

These two diagnostics are used to inform a plan that involves the three repeating elements of advanced cyber oversight: staging, intervention, and reflection. *For more about the intervention and reflection steps, see pages 23–24.* They reveal key information that a board would use to assess itself against the five-stage model outlined above. For example, large gaps between board members' positions on the four continuums (diagnostic 1) or between the official future and the board's actual cybersecurity governance strategy (diagnostic 2) suggest that the board may be starting from a less mature developmental stage.

Significant value can be gained by a disciplined and regular reflection at each iteration of the process to check progress and to ensure that boards are moving forward, especially as new threats emerge.

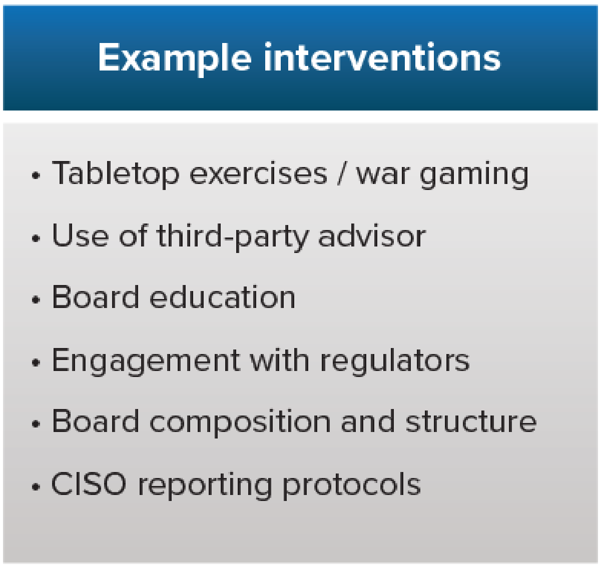
The diagnostics also point to the kinds of interventions that are needed to advance the board up the spiral staircase. For example, a board that is relatively strongly aligned on the four continuums (diagnostic 1) but discovers that its official future is not consistent with the logic implied in those first results would almost certainly benefit from war-gaming exercises to recheck its beliefs and stances. Alternatively, a board that examines its official future and finds that it lacks the expertise or processes to proactively determine if that future is in fact coming to pass would almost certainly benefit from reexamining alternative choices—for example, on the question of the board-CISO management protocol.

Significant value can be gained by a disciplined and regular reflection at each iteration of the process to check progress and to ensure that boards are moving forward, especially as new threats emerge. This may include periodic reapplication of the diagnostics as boards move to more mature developmental stages in the COED model.

Intervention

In the intervention step of enhanced cyber oversight, boards can consider a range of activities:

Figure 6. Example interventions



Example interventions

- Tabletop exercises / war gaming
- Use of third-party advisor
- Board education
- Engagement with regulators
- Board composition and structure
- CISO reporting protocols

- **Tabletop exercises/war-gaming.** Involving board members in management-led tabletop exercises is a proven technique for surfacing and resolving gaps in understanding and alignment among board members and between the board and management. These exercises can be powerful learning experiences, often spotlighting functional interdependencies in a crisis. Directors who have participated have consistently reported that they were highly educational and that they fostered important dialogue between the board and management. Scenario planning is less interactive than a tabletop exercise, but it can be useful for sharing critical assumptions and enabling deeper dialogue between management and the board.

- **Use of third-party advisors.** Many companies employ third parties to conduct penetration testing of their cybersecurity defense; some companies use third parties to benchmark their cybersecurity policies and processes. Some boards have engaged outside advisors directly as a way of getting an independent view of the company's capabilities unfiltered by management, or as an independent audit of the company's implementation. Some board members may be concerned that the board may overreach by engaging directly with third parties; nevertheless, board members should have access to different perspectives on the company's cyber risk and cybersecurity posture, particularly if individual board members don't have prior experience in technology or cybersecurity matters.

- **Board education.** As part of a learning organization, board members should expect to continue their own education on topics that are rapidly evolving. Many companies provide opportunities for board members to learn—sometimes through a deep dive in the annual strategy session or a shorter, informal discussion during the board dinner—but these may not be sufficient. Some boards expect their members to be responsible for their own continuing education, while others devote time during key committee meetings for members to go deeper into topics. Regardless of the educational approach, it is important for the board to understand how board members and the board as a whole will further their learning.
- **Engagement with regulators.** Where there is an ongoing, established dialogue between a board and its regulators, as in the financial-services sector, boards may benefit from deepening this engagement. Both sides can benefit from explaining what they are seeing and what is needed to improve the overall cybersecurity environment. Commitment to this kind of dialogue and engagement can help boards move to a more proactive stance, rather than simply reacting to and complying with expanding cybersecurity and privacy regulation. Regulator dialogue needs to be carefully managed, typically with the help of a company's legal team; it is often inappropriate in the immediate aftermath of a cyber-breach incident.
- **Board composition and structure.** Some boards determine that they need members with specific expertise to exercise cybersecurity oversight. The need for a cyber expert on a board depends on the circumstances and risk profile of each organization, but the presence of board members who thoroughly understand the modern technology landscape is increasingly becoming an expectation. A board may also rethink how its committees are structured. Many assign cyber risk to the audit committee, but alternative approaches are growing in popularity, as boards create new committees or delegate oversight to another committee to ensure that cyber risk is receiving sufficient oversight.

After an intervention, in the reflection step, a board can look back at the original staging assessment, review the process of intervention, and identify specific learnings from the intervention.

Reflection

After an intervention, in the reflection step, a board can look back at the original staging assessment, review the process of intervention, and identify specific learnings from the intervention. A tabletop exercise in one large company, for example, revealed that its incident-response plans were no longer adequate given shifting patterns of ransomware attack; the board is now working with management both on new response plans and on enhanced reporting from the CISO to the board. Third-party experts may be helpful as board and management engage in reflection on the progress they have made. And a board may use the reflection process to decide on the timing of its next staging exercise or the external events that might trigger a restaging.

IV. Implementation considerations

Boards are skeptical that a one-size-fits-all model for dealing with cyber risk exists. The learning-organization model agrees and is intentionally flexible.

Some boards may prefer to conduct these diagnostics and develop an intervention plan first within a smaller committee (e.g., the audit committee) before investing time with the full board. Committee leadership of the process is a reasonable, feasible, and possibly more efficient approach to implementation of the COED model for some boards.

Boards should decide, typically with the firm's general counsel, whether to initiate the COED process under legal privilege or to make it more public, and they should understand the risks and motivations of their choice. Each has advantages: for example, if part of the board's motivation is to demonstrate its commitment to improving firm cybersecurity capabilities, there may be benefits to sharing some outcomes of the COED process with third parties; however, the board might prefer to conduct the process under privilege if it would like to protect the gaps and areas of improvement that engagement with the COED model identifies.

In many cases, it would be useful to have management undertake a parallel diagnostic assessment. Dynamic tensions and revealed preferences are important concepts for the senior team, whose members—the CISO, chief information officer, chief technology officer, and CEO, for example—may have their own unexamined assumptions and implicit differences from one another. Comparing the results of these exercises done in parallel could be valuable as a way of bringing the board and management into closer dialogue and alignment around strategic goals, and it could contribute to the development of upgraded metrics that both board and management understand in the same ways.

We think that it will be relatively uncommon for a board to conclude that cyber risk requires far more extensive action than management recommends, but if such a disconnect is uncovered and made visible in a detailed way, it could prompt difficult but valuable discussions between the board and its management team.

Boards are skeptical that a one-size-fits-all model for dealing with cyber risk exists. The learning-organization model agrees and is intentionally flexible. However, there may be specific interventions that can be packaged for relevant segments and dimensions of firms (e.g., business-to-business, industry sector, company size). Understanding those segments and dimensions is a task for further research and will happen through further testing and refinement with willing board partners in the field.

Board agendas are also tightly time constrained, and cybersecurity discussions often get cut short. Becoming a learning organization requires a time investment, so the question of who will make this happen is very real. Understanding how board evolution on cybersecurity can happen within current board and management constraints will also require further experimentation. One possibility is that COED could be a tool not only for the board but also for management and the general counsel, with staging and reflection done under privilege.

A note on Tapestry and CLTC's intentions for the development and use of this model: It is *not* the intention of Tapestry or CLTC to build proprietary consulting services on top of or around this model. Rather, we wish to enable a competitive marketplace for such services, operating in the context of the model, which would act as a common standard of evaluation of success. Ideally, COED would eventually contribute to cyber-insurance risk ratings and possibly to general audit evaluations and reporting as well.

V. Case study: ACME meets COED

This fictional case study aims to show how a company might apply the COED approach.

Devika Mani, Acme Corporation’s lead director, rubbed her eyes. After two days at an intensive cybersecurity boot camp for directors, she felt like she had a better understanding of technology, terminology, and tactics, but she worried deeply about whether Acme was doing enough—and enough of the right things—to protect its network and digital assets. And had its security measures enabled or impeded Acme’s competitive advantage in an increasingly tough marketplace? Devika was beginning to wonder whether the strategic stakes were far higher than she—or the board—had previously imagined. The board was going to need to engage more deeply on cybersecurity and to radically sharpen its capabilities.

Acme is a designer and manufacturer of high-precision industrial fasteners whose headquarters and design facilities are still in the building where the company was born in 1945, in Omaha. Today it has major advanced manufacturing facilities in New Jersey, Ireland, and Malaysia, and a large technical sales force serving customers in over 70 countries. Acme’s designers are deeply proud of how they continuously push the envelope on materials science and manufacturing tolerances to build fasteners that make so many aspects of modern life possible. Their products are in SpaceX rockets and F-18 airplanes, in hip and shoulder replacements, and in electric-vehicle battery assemblies. By 2022, they will be in the new casings that Apple is (secretly, with Acme’s help) designing for the iPhone 13.

Acme’s leading engineers could talk for hours about the extraordinary properties of a new alloy, the doubling of average time to failure, or a product road map that should keep Acme comfortably ahead of its East Asian competitors, but when Devika asked these same engineers about the digital layer of their business, their dependence on data flows, and the algorithms that were being used to run quality control, manufacturing processes, and design-led sales, she could see their attention wander. They saw themselves as fastener people or materials people; the digital layer was somebody else’s job to provide and secure.

Devika knew that last week RailRunner Industries, one of Acme's most important competitors, had been implicated as a target in the SolarWinds attack. RailRunner's board had had no idea that the firm's IT division relied on SolarWinds, nor had it understood what a US government "notice of vulnerability" really meant. What RailRunner's board did know was that its CEO, Melissa Hartoonian, had ordered a week-long production shutdown and a massive examination of the company's network, employees' devices, and its cloud-service providers. Hartoonian was also planning to spend upwards of $50 million for a third-party audit of data security throughout the enterprise.

Devika had also heard through personal channels that Hartoonian had told RailRunner's board that she really did not know what these emergency actions would reveal and whether they would be sufficient to uncover damage or risks of future damage associated with the attack; she was treating them as a down payment only. This story wasn't helping Devika's insomnia. Seemingly unquantifiable risk, spread throughout the enterprise (and, who knows, perhaps among its suppliers and customers as well); vague concerns about technology and data that might take months to work through; the possibility of regulatory or even legal action—it sounded like a corporate governance nightmare, and she felt that she needed to prevent Acme from ever encountering anything like it.

Devika approached Jeffrey Kirk, the audit committee chair, with whom she had a close and trusted relationship, for an informal conversation about where Acme really stood on cyber risk. She didn't find the conversation reassuring. Jeff's credentials were impeccable, and he had a background in technology that positioned him well for cyber-risk oversight. He assured Devika that his committee kept a very close eye on the National Association of Corporate Directors guidelines and was always on the lookout for new practices that he could integrate into their work. He seemed very positive about Acme's CISO. But when pressed, he wasn't nearly as confident in the ability of his fellow audit committee members (let alone the full board) to understand what the CISO was doing and why. He told Devika that Acme was in compliance with relevant legal and professional standards—"We have checked all the boxes," he said—but he admitted that RailRunner had also done all of those things.

What was most worrying was when the conversation turned to the five-year product road map. Acme had invested nearly $200 million in additive manufacturing equipment (3D printers) for its next-generation products. These machines relied on digital "build files" that a third-party vendor in Singapore compiled using designs drawn up in Omaha and code from contract engineers based in Shenzhen. Had the audit committee—or anyone else—really examined what management was doing to assure the accuracy and security of those build files? Could anyone be certain that the designs had been faithfully translated? Or that the underlying intellectual property hadn't been stolen along the way?

Devika had been told that it was possible to introduce instructions into build files that would weaken the tolerances of a product and reduce its mean time to failure by a factor of 10 without any manifestation of the attack that could be picked up by standard quality-control assessments. It might have sounded like a science-fiction nightmare, but it was real, and the human and economic impact of hip replacements failing, rockets blowing up in mid-air, and a billion smartphone cases cracking in users' back pockets was terrifying. Could Acme really go forward with this product road map without better assurances?

Devika realized that the board's cyber-risk governance and oversight was facing an inflection point. With the risk landscape looking dire and Acme's innovation road map dependent on digital security, she felt strongly that the board needed a fundamentally different approach. The board needed to get measurably better at questioning management and understanding their answers, more effective in dialogue with regulators and government officials, and more confident that Acme was positioned to deter, respond to, and recover from the next generation of cyberattacks. This would demand a serious expansion of board time and resources this year and continued investment over time. It would mean a cultural change, extending to board meetings, individual director time investment, and the relationship between the board and management and among board members.

With that in mind, Devika decided to experiment with a more intensive approach to cyber oversight, using COED. The first step was to commit Acme's audit committee to a two-hour facilitated exercise to map the directors' operating assumptions around four dimensions of variance in cyber-risk governance practices (the "dynamic tensions"). Each director was asked to specify where they thought the board currently was on each dimension. Next, they were asked to specify where they thought the board ought to be. When the results came back, the directors realized that they didn't have a clear understanding of each other's operating assumptions and beliefs about cyber oversight. They were able to clarify the sources of some of those differences without trying to force convergence, which led to a more disciplined discussion with the full board about where on each dimension the board would be best positioned to help Acme reduce the risk of what had just hit RailRunner. The goal of this meeting wasn't to agree on an optimal set point for that purpose; it was to clarify the differences in views within the board and what might be the sources and consequences of those differences.

Following this discussion, Devika used COED's staging framework to assess which of five developmental stages the board as a whole had achieved. Her assessment was that Acme's board was roughly at stage two, the self-aware stage. She made it an explicit objective to advance the board to at least stage three (intentional) and, ideally, stage four (adaptive) over the next 12 months. She worked with an independent third party who helped her develop measurable indicators of progress that would be made visible to the entire board. She set out a bespoke learning plan for the directors that would move the board up the spiral staircase of preparedness in a timely and efficient manner, with checks along the way to assess progress. That plan included specific education objectives as well as tabletop scenario and simulation exercises, some of which would be conducted jointly with the CISO. A central tenet was that the board and management would grow their capabilities and confidence together.

As the board grew more comfortable with this approach, Devika decided it would be useful to dig deeper into the board's implicit strategic direction on cyber risk. To do this, she engaged her colleagues in an official-future exercise, again from the COED playbook. The result of the official-future exercise would answer this question: What would the board need to believe for its current practices and policies around cyber governance to be an optimized, rational response?

This exercise took several hours of board time, including advance preparation. Some board members were hesitant at the start, but they came to see the value when they realized that the official future against which their behaviors were optimized did not appear to be an adequate pathway for the business, given the threat environment, the regulatory environment, and the technologies the company was developing.

For example, one official-future assumption that surfaced was roughly, "Within 18 months, our cloud migration strategy will transfer much of our operational cyber risk to cloud providers." But the CISO had to say, "Well, not exactly," since Acme had carved out an exception for the critical intellectual property in the build files to drive the 3D printers, keeping them on private servers at headquarters, linked to manufacturing facilities abroad by virtual private network connections.

Seeing these disconnects and others like them was a catalyst for strategy conversations with management that led to a reallocation of investment priorities and some new tracking measures. The next time the board met with the CISO, the conversation focused directly on indicators of progress in aligning Acme's digital-security program with a more clearly articulated and common understanding of how the threat and business environments were likely to evolve.

Acme's board came to understand that its new approach to oversight and governance of cyber risk was highly dynamic, needing regular reevaluation and co-evolution with the threat environment. It was uncomfortable for many directors and for the group as a whole at times, but also rewarding for individual directors. Many directors said that it was bringing them into closer alignment with management around the digital aspects of the business, and both the CISO and the CEO quietly echoed that sentiment. Everyone was moving faster, but now they were moving in closer sync with each other, speaking similar languages, asking and answering better questions, and having higher confidence in the results.

But was it really worth the investment of time and energy? The increase in velocity turned out to be extremely important a few months later, when a new set of data manipulation attacks began to emerge—sooner than expected—creating a new frontier for cyber-risk practice. Thanks in part to the board's faster learning cycle and improved cyber-oversight processes, Acme had already discussed and begun to address these kinds of scenarios internally. It gained market share as customers began to trust Acme's processes as part of their own security audits.

Devika wondered how long this high-pressure, high-velocity oversight atmosphere would last and how much time the board would need to continue to commit to cyber oversight over the next few years or decade. The answer seemed to her to be "more than you think and certainly more than you would have wanted," but it also seemed that there was no other choice.

VI. Acknowledgements

We would like to express our gratitude to those whose time, talent, and energy have driven this project to a conclusion with the creation of COED, a new approach for building a board's capabilities as it oversees cybersecurity risk.

The non-executive directors, listed below, provided invaluable guidance and feedback throughout the creation of COED. They generously and candidly shared their unique expertise and perspectives, providing the foundation of COED and verifying it as a useful tool for corporate oversight of cybersecurity. The directors not only identified the need for enhanced board oversight of cybersecurity but also played a major role in shaping the final work.

- Joan Amble, Zurich Insurance Group, Booz Allen Hamilton
- Marianne Brown, Northrup Grumman, Akamai, VMWare, Charles Schwab
- Bill Easter, Delta Air Lines, Emerson Electric, Grupo Aeroméxico
- Linda Gooden, Bright Health Group, General Motors, Home Depot
- Fritz Henderson, Marriott International, Adient PLC, Horizon Global Corp., Arconic Corp.
- Tom Killalea, Akamai, Capital One Financial, MongoDB Inc.
- Jane Holl Lute, Union Pacific, Marsh McLennan, Royal Dutch Shell
- Risto Siilasmaa, F-Secure OYJ
- Suzanne Vautrinot, CSX, Ecolab, Wells Fargo, Parsons Corp

Tapestry Networks is grateful for our collaboration with the Center for Long-Term Cybersecurity (CLTC) at the University of California, Berkeley, which was central to the effort from its start. Professor Steve Weber, faculty director of CLTC and Ann Cleaveland, CLTC's executive director, were full members of the team, writing, editing, and challenging the thinking throughout. This report has benefitted from CLTC's earlier work on cybersecurity governance.

We are similarly indebted to the international law firm King & Spalding for their sponsorship of and contributions to COED. Partners Phyllis Sumner, global leader of King & Spalding's Data Security and Privacy practice and the firm's chief privacy officer, and Keith Townsend, co-leader of the Public Companies Practice Group, helped guide the work and kept it grounded with cutting-edge legal perspectives and deep field experience.

The project was produced and coordinated by Tapestry Networks. Michael Mahoney led our team, working with Jonathan Day and Brennan Kerrigan. Meeting and production logistics were handled by Amy Christenson, director of operations, and Margaret Chouinard, project and event manager.

About Tapestry Networks

Founded in 2003, Tapestry Networks exists to help leaders of the most important institutions in the world do their work more effectively and with greater confidence. Each year, hundreds of senior executives and independent directors participate in our networks and research initiatives, representing large, global companies from North America and Europe. Many involve members who share the same role, such as public company audit committee chairs, and are committed to improving performance and to learning from one another. Others form around a specific sector or issue, such as banking, board oversight of cybersecurity, or personalized medicine. In many cases, regulators and government officials are active participants. Our networks and research projects are based on candid views from top leaders on the realities of leading the world's largest and most complex firms. Learn more at www.tapestrynetworks.com.

About the Center for Long-Term Cybersecurity

The Center for Long-Term Cybersecurity is a leading hub for cybersecurity research, education, and collaboration. From our home at UC Berkeley's School of Information, with close ties to Silicon Valley, we act as a translator and two-way bridge between cutting-edge academic research and industry and policy needs. We serve as a convening platform to promote dialogue across government, academia, industry, and civil society. In affiliation with UC Berkeley's Master of Information and Cybersecurity degree program, we are developing the next generation of professionals who will shape cybersecurity practice and policy for years to come. Learn more at cltc.berkeley.edu.

About King & Spalding

King & Spalding is an international law firm with a substantial data privacy and security practice, working in more than 160 countries with 22 offices globally and more than 1,200 lawyers. The firm's Data, Privacy and Security team counsels clients on a broad range of legal issues faced by multinational organizations, including global privacy programs, data protection and cybersecurity assessments, crisis management in responding to internal and external privacy and data security incidents, health information governance and compliance, and defending clients in regulatory enforcement proceedings and class-action litigation. For more information, see www.kslaw.com.