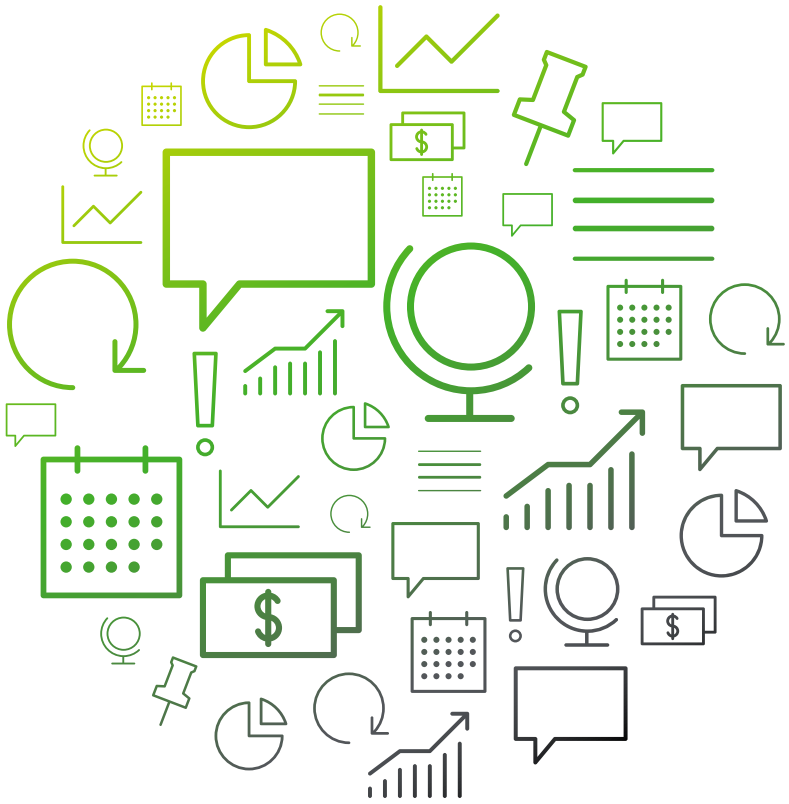
Deloitte.

February 2018



On the board's agenda | US

Cyber risk in the boardroom: Accelerating from acceptance to action

Cyber risk is a top-level business risk that boards may find challenging to oversee and difficult to address. By using a maturity model for board stewardship of cyber risk and understanding the actions available at each level of maturity, boards can accelerate their transition from awareness to meaningful oversight.

Boards are being constantly bombarded by the breadth, depth, and technology-specific aspects of cyber risk. NYSE Governance Services and *Corporate Board Member* magazine[1] recently surveyed 200 audit committee members and found that nearly 60 percent of them believe that it's necessary for companies to have at least one board member with a specific IT background. Moreover, nearly 60% also worry that their boards, as currently constituted, may have members without the skills and understanding of technology necessary to provide effective oversight of IT and cyber risk.

Deborah DeHaas, Vice Chairman, Chief Inclusion Officer and National Managing Partner of the Center for Board Effectiveness, Deloitte, agrees. "Frankly, a lot of boards start out bewildered by this topic," she said. "It's unlike most topics that are covered in the boardroom. Many directors feel they don't have the knowledge to provide effective oversight."

But she also says that in her work with boards, she sees many move along a continuum from acceptance to understanding to meaningful oversight. "I've seen that over time, good boards evolve. Through a number of steps, they come to accept that cyber risk is a significant exposure. Next they often try to translate this broad acceptance into an understanding of cyber risk exposures and capabilities specific to their company. They can then question management and learn how their company is prepared to address the issue."

1. Deborah Scally, "Managing Cyber Risk: Are Companies Safeguarding Their Assets?," *Corporate Board Member Magazine*, 1st Quarter 2015, https://www.nyse.com/corporate-services/nysegs/CBM_1Q15_Special_Report

Center *for*
Board Effectiveness

And in the most mature stage, they act. "Once they recognize that cyber is a top-level business risk," she said, "strong boards shape the cyber risk profile of their companies through their stewardship and governance responsibilities."

To more rapidly achieve the state in which a board is actively overseeing the company's cyber risk profile, boards can leverage this same model, moving from acceptance to understanding to meaningful oversight.

A primer on cyber risk

Because cyber risk is a topic that board members find challenging, it may be valuable to become grounded in a few key concepts. The first is an understanding of the basic ways cyber attacks can adversely affect a business. The second is a view of what a good program looks like.

Below are some of the typical ways cyber attacks can impair a business:

1. ***Financial loss or fraud.*** This may include theft of personally identifiable information, intellectual property, or financial assets.
2. ***Reputation or brand damage.*** This may stem from the unauthorized release of information that can reflect poorly on the company, often breaking trust with customers, partners, regulators, and shareholders.
3. ***Process or technology disruption.*** A cyber attack (such as a distributed denial of service attack) makes services unavailable for some period of time, interrupting normal business operations
4. ***Loss or destruction of data and assets.*** Malware, for example, can destroy hardware or wipe out corporate data. With "ransomware," systems are held hostage until a ransom is paid to a criminal.
5. ***Regulatory impact.*** Companies may face disciplinary action, fines, or supervised remediation from regulatory agencies as a result of cyber incidents if the organization has been negligent in its security practices. Depending upon the nature of a cyber attack, a company's ability to comply with financial and other disclosure requirements can also be adversely affected.
6. ***Life and safety consequences.*** In some industries, such as healthcare, energy, utilities, or life sciences, a cyber attack can cause actual harm to individuals.

Board maturity levels for stewardship of cyber risk

Looking at what other boards have done to strengthen their governance and stewardship of cyber risk can be a very helpful tool.

Phase 1: Accept

In the "accept" phase, board members begin to recognize cyber risk as a significant exposure and begin to get educated. Activities undertaken by board members in this phase may include:

- Getting broadly educated, understanding threats and actors, and risk and business impacts
- Holding conversations on cyber with peers serving on other boards
- Asking internal and external experts to present at board meetings
- Obtaining lessons learned from executives at other companies who have experienced a cyber incident
- Understanding how cyber is connected with risk frameworks (i.e., fit with technology risk, operational risk, enterprise risk)
- Understanding resources available from local, national, and global law enforcement and how to engage them (before and during a crisis)
- Understanding what "good" looks like, including industry leading practices for companies of similar size and complexity

The CIO of a mid-market manufacturing company gave their first presentation to the board of directors' audit committee on the state of the organization's cybersecurity posture. The IT leader stood in front of the committee and guaranteed that the enterprise was safe. The level of risk, was low.

After the CIO left, an outside observer told the committee that no CIO in any industry could or should make such an assessment or proffer such a guarantee. The CIO's lack of concern was, in fact, cause for concern. Indeed, just a month later, consultants identified a major security hole in the one of the company's critical systems.

Phase 2: Understand

In the "understand" phase, board members translate broad awareness into knowledge of company-specific cyber risk exposures and capabilities. Activities that can be undertaken by board members in this phase include:

- Understanding "crown jewels" of the company and the degree of exposure/ vulnerabilities in the environment
- Understanding the controls management has put in place or is considering, including roadmap for implementation
- Understanding the company's cyber risk management framework
- Reviewing cyber metrics and trends
- Asking the right cyber risk management questions, begin to demand more from management (see green box on page 4)
- Participating in industry forums
- Transitioning to seeing cyber as a risk to be managed, not a problem to be solved

Phase 3: Act

In the "act" phase, board members oversee shaping the cyber risk profile of the company through board stewardship and governance. Activities undertaken by board members in this phase might include:

- Determining whether the right skillsets are on the board (i.e., 1–2 directors who understand cyber at the business and technology level) and, if not, considering adding directors with those skillsets
- Considering assigning a board committee (e.g., Risk or Technology) to directly oversee cyber
- Reviewing risk appetite at both the enterprise and line of business level
- Evaluating whether the cyber governance and operating model is appropriate for the size and complexity of the company—including accountability at Business, IT, and Executive levels
- Verifying appropriate incident escalation playbooks and processes are in place
- Driving more effective cyber risk board reporting, a customized package
- Participating in cyber war games
- Commissioning periodic independent testing; asking for results of tests and maturity assessments.

Challenging management through critical questions

In both the "understand" and "act" phases of the model, board members can harness their experience in managing other business risks to ask probing questions on cyber that challenge management. Corporate boards can and should gain improved visibility into management's cyber risk management practices and strategies by taking a more active role in helping management improve its performance in this increasingly critical area. There are a number of questions boards can ask to move from a basic awareness of cyber risk to a deeper understanding of that risk in the context of business strategy and operations, permitting it to discharge its responsibilities to all relevant stakeholders.

Corporate boards should consider asking for a customized reporting package that articulates cyber risk in terms of its impact on the business. Boards can emphasize to management that the board should not be expected to translate and interpret cyber jargon, and the metrics contained in these reports should have clearly defined business impacts.

Boards should also consider requiring management to provide a set of key performance indicators and key risk indicators that can enable them to quickly ascertain the state of cybersecurity in the company. Directors can work directly with management to develop these board-level metrics and benchmarking tools.

Boards can also ask management about its use of risk-sensing tools. A recent global survey of C-level executives conducted on behalf of Deloitte Touche Tohmatsu Limited found that while many organizations have risk-sensing capabilities, they often overlook key elements and lack technical depth. Boards can also work with management to define the thresholds at which cyber incidents or actions should be brought to the board's attention, including significant cyber investments, proposed vendor contracts that represent a significant change in cyber risk levels, breaches within the company or industry, and other material events.

Many companies increasingly are using cyber war games to help them visualize how their response strategies would play out during an actual event. However, today, very few board members ask if these exercises have been conducted, who participated and what gaps were identified. These type of simulation exercises can provide much needed context and education around what can be an opaque subject because they can offer an accurate view of the tensile strength and resilience of an organization's plans. Boards that want to know about real-life incident response should have the opportunity to ask how the company is poised to respond.

It is tremendously useful for corporate boards to ask expert third parties to help them assess the strength of their cyber programs. These experts can report independently to the board, providing unbiased analysis and guidance. Some boards have invited senior executives from companies that have experienced a breach to share their experience and insights, and offer hard-won knowledge about what directors and executives could have done differently to prevent or mitigate the damage done.

Questions for boards to consider:

1. What is the level of technical knowledge on IT matters on our board? Do we need to add one or more directors who have the requisite degree of technical knowledge?
2. Even if we decide to bring more tech-savvy directors on board, that will take a while. In the meantime, can we engage outside advisors to assist us in this area? Should we engage outside advisors even if we have the requisite level of knowledge?
3. Do we need to create a technology or similar board-level committee to address cyber risk, or are we better off having the full board address it?
4. What are the most likely adverse impacts on our company from a cyber attack? Would the impact vary depending upon the nature of the attack (e.g., malware, ransomware, theft of information)? Can we get a dashboard or matrix or the like?
5. How far along is our board on the continuum of cyber "maturity"? Have we merely accepted our vulnerability and the level of risk we face, or do we really understand it? Are we prepared to address it proactively?
6. Are we getting the right kinds of reports from management on cyber risk?
7. Management has given us assurances that our risk of cyber attack is negligible. Is that realistic?
8. We have crisis management and business continuity plans in place. Do we have a cyber attack plan in place? If so, what is it; if not, why not?
9. Have we conducted war-games to simulate different types of cyber attacks? What have been the results of these war games? What have we learned?
10. What risk-sensing tools do we use in the cyber area?

Board members needn't become cyber security specialists. But by bringing to bear their deep experience in risk management, they can push management to answer tough questions and identify potential weaknesses in an organization's cybersecurity strategy and capabilities. Knowing that every company will have to accept some risk, the board can help management focus its efforts on the highest risk areas, while preserving the company's ability to innovate. Again, the question returns to the organization's risk appetite, and the board's ability to make sure the organization's cyber security efforts align with agreed upon risk parameters.

Conclusion

Cyber risk is a complex business issue, one of the few categories of risk that are truly systemic, affecting every aspect of the business. It is also a risk that increases the more innovative a company becomes. And, unfortunately, it is a risk that can never be eliminated as it is a shape-shifter, assuming new forms on an almost constant basis.

In recent years, boards have done a good job of recognizing the importance of effective cyber risk management to corporate performance. But many are still struggling to figure out more specifically what their fiduciary and oversight responsibilities are in this area. That will require a greater understanding of the true nature of cyber risk, both in general and in the context of the companies they direct. Forward looking boards can make the effort to increase their collective understanding by pursuing greater visibility into management's cyber risk management practices, processes, and performance. And that education and action must be ongoing because, as noted, cyber-threats are evolving on a daily basis. Consequently, cybersecurity risk mitigation, monitoring, and management needs be a dynamic practice.

Despite these significant challenges, cyber risk is manageable if boards can develop an approach similar to the steps they take to direct corporate responses to other business risks, such as liquidity or supply chain risk. By developing a broad understanding of cyber risk, a familiarity with the specific questions to ask management in order to understand the organization's evolving cybersecurity stance, and becoming more involved in setting up processes to monitor performance, corporate boards will be better able to fulfill this increasingly important aspect of their oversight role.

Authors

Mary Galligan
Managing Director
Cyber Risk Services
Deloitte & Touche LLP
mgalligan@deloitte.com

Bob Lamm
Independent Senior Advisor
Center for Board Effectiveness
Deloitte LLP
rlamm@deloitte.com

Contact us

Deborah DeHaas
Vice Chairman, Chief Inclusion Officer, and National Managing Partner
Center for Board Effectiveness
Deloitte
ddehaas@deloitte.com

Henry Phillips
Vice Chairman and National Managing Partner
Center for Board Effectiveness
Deloitte & Touche LLP
henryphillips@deloitte.com

Maureen Bujno
Managing Director
Center for Board Effectiveness
Deloitte LLP
mbunjo@deloitte.com

Debbie McCormack
Managing Director
Center for Board Effectiveness
Deloitte LLP
dmccormack@deloitte.com

Krista Parsons
Managing Director
Center for Board Effectiveness
Deloitte & Touche LLP
kparsons@deloitte.com