Deloitte.

November 2020

On the board's agenda | US

Cyber: New challenges in a COVID-19–disrupted world

Background: The pre-COVID-19 environment

Cyber, and the challenges it presents to businesses of all types and sizes, was on the board's agenda well before the onset of the COVID-19 pandemic. Many boards, including their committees, engaged in a wide range of activities to stay informed and vigilant on the topic. As a result, these boards had reason to believe that they were exercising an appropriate degree of oversight regarding cyber.

As in so many other areas, the pandemic and the many disruptions it has caused have created new challenges for boards to consider. In addition, an increasing focus on areas such as the use of data, privacy, and artificial intelligence (AI) ethics has further expanded the areas that boards need to address. This *On the board's agenda* discusses the nature of those changes and how boards can adapt to the new environment, supporting a resilient response to the new challenges and opportunities of cyber.

What has changed?

The changes brought about by the COVID-19 pandemic with respect to cyber are extensive. However, the most significant ones are as follows:

Center for Board Effectiveness

- **A rapid transition to remote work:** While the details have varied based upon geography and other factors, businesses worldwide seemingly awakened one day to realize that significant portions of their workforces would not be coming to the office for the foreseeable future. This rapid transition placed unprecedented stresses on networks that had previously facilitated remote access for a limited portion of the workforce, often only at limited times. Other stresses included the inability to obtain the technology needed to move employees from an office "desktop" environment to a home "laptop" environment.

  A collateral effect of the rapid expansion of remote working has been the related risk of cyberattacks aimed at the remote workforce. Aside from the need to rely upon home Wi-Fi or other networks potentially lacking the protection available in a workplace setting, employees working remotely may forget or ignore basic "rules of the road," such as failing to use virtual private networks (VPN) or signing into work accounts using shared family devices.

- **Uncertainty about the return to work:** Decisions regarding cyber have been made more challenging by the many questions that surround the issue of returning to work. And those decisions are likely to evolve over time, necessitating a nimble approach.

- **Increased cyberattacks:** Whether or not a result of increased susceptibility to attacks, numerous sources have reported significant increases in cyberattacks since the onset of the pandemic.[1] The types of attacks reported include online scams and phishing; disruptive malware, including ransomware; data-harvesting malware; malicious domains; and misinformation. While the types of attacks may not be new, their volume has made it difficult to monitor and address in a timely manner, especially across a cyber workforce that is already stretched thin.

- **Budget and resource constraints:** While cyber challenges may not be addressed merely by throwing money or other resources at them, the severe retractions suffered by so many businesses have resulted and will likely continue to result in ongoing budget and resource constraints. And despite the recognition that cyber is a priority, scarcities of funds and other resources may inevitably lead to fewer dollars and resources being committed to cyber, aggravating the challenges faced by an already stretched workforce, as noted above.

In addition, the pandemic has increased awareness of how cyber impacts many aspects of business. Perhaps the area of greatest focus in this regard are the supply chains on which businesses—and individuals—rely. Many individuals experienced supply chain disruptions when they went to a supermarket in the early days of the pandemic and found empty shelves where paper towels and other staples used to be in abundant supply. Businesses, far beyond just supermarkets, have experienced similar disruptions.

The disruptions of supply chains have also heightened awareness of the extent to which our business systems are interconnected and interdependent. In the 21st century, it is difficult to envision a business—any business, no matter how small—that is not connected to and dependent upon a range of systems. From a taxicab or shoeshine stand that accepts credit cards to a global corporation that provides goods or services across global boundaries, the degree of interconnectedness and interdependency is literally staggering. Moreover, the more geographical regions in which a business operates, the greater the degree of dependency, given the multiplicity—and often the inconsistency—of regulatory requirements and prohibitions in different parts of the world.

As noted above, the impacts of COVID-19 are not the only challenges facing boards in overseeing cyber. There is significant pressure from many sources—including governments—for businesses to use data appropriately, to maintain data privacy, and to implement and maintain ethical standards in the use of data, including in AI applications. As companies seek to use data to drive customer behavior, enhance and develop new products and services, improve business processes, and make better business decisions, boards should be satisfied that their companies are looking closely at the methods by which these goals are achieved.

Moving forward

The above and other challenges may be steep, but they need not be insurmountable; indeed, in a period when resiliency is critical, these challenges should be addressed to respond, recover, and thrive. So what can be done? And how can boards help? The following summarizes a number of considerations that boards can take into account in helping their organizations to address the ongoing challenges of cyber in a post-COVID-19 world, along with questions that directors can ask to assist them in their oversight role:

- **Setting goals:** One goal of effective board oversight of cyber is to mitigate risk while enabling the business to operate as effectively and efficiently as possible. Boards can establish parameters so that risk is mitigated without stifling legitimate business objectives. In addition, a more overarching goal is to establish trust among the business's constituencies—its workforce, its customers, its suppliers, the communities in which it operates and, ultimately, its owners. Establishing goals and keeping them in mind in these and other areas can help facilitate more effective board oversight.

  Questions:

  – What is the right amount of threat intelligence and monitoring? Are we as on top of things as we should be, or are we being so risk-averse that we're stifling growth?

  – Are we taking steps now to determine what our technology "landscape" might look like in 12 months?

- **Having the "right" board:** Having the "right" board composition does not solve the challenges presented by cyber. However, boards need to consider whether they have the mix of skills needed to understand and help address those challenges.

1. See, for example, "INTERPOL reports alarming rate of cyberattacks during COVID-19," at https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

Some boards may believe that a cyber "guru" is critical for that purpose, while others may opt to have one or more directors who are "tech-savvy"—among other attributes.[2]

Questions:

- Does our board have the right mix of skills and experience to properly oversee the challenges of cyber?
- Should we engage a third party to conduct a cyber assessment to determine how and to what extent have our cyber risks have changed, whether as a result of COVID-19 or otherwise?

- **Determining where board oversight responsibility for cyber resides:** Some boards may decide to keep oversight responsibility for cyber at the full board level; others may determine to delegate that responsibility to a committee of the board. Given the role of the audit committee in overseeing the risk process generally, some boards may decide that the audit committee is where cyber should reside. To the extent that boards have a committee dealing with technology,[3] they may delegate cyber to that committee.

  Questions:

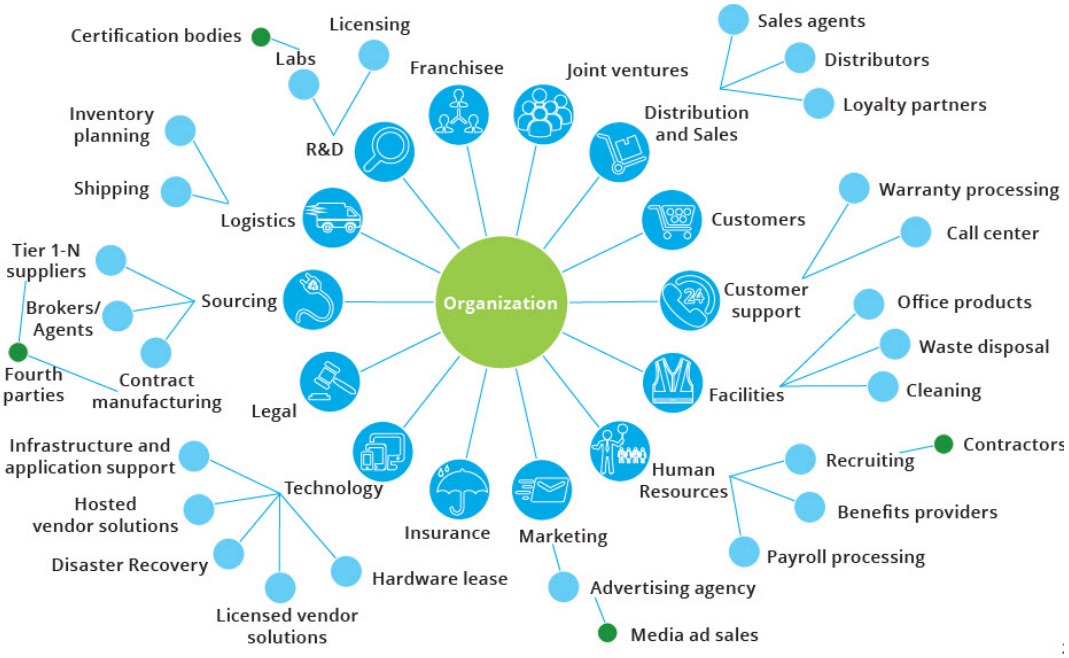
  - Where does oversight responsibility for cyber best reside? With the full board or a committee and, if the latter, which committee?
  - Should we create a separate committee to oversee cyber?

- **Understanding with the company's risk controls:** Although the board has ultimate oversight responsibility for risk, management and the risk controls it maintains are where the risk "rubber" meets the road. Accordingly, boards should understand and be satisfied with the structure, content, and frequency of management reports. Many companies have developed dashboards and "heat maps" that graphically highlight cyber and other risks, conveying their significance and other characteristics. Some boards (and managements) have also implemented methods to measure the extent to which the company can prevent and recover from cyber-attacks.[4] At the same time, boards need to accept that these and other reporting methods will not address the risks themselves and will rarely, if ever, show a risk-free picture.

  Questions:

  - Is the board getting adequate information on ongoing risks, trends, and metrics? What formats/approaches might provide better and/or more timely information on the topic?
  - Do we want to develop methods by which to measure cyber risk?

- **Expanding the ERM universe:** At a minimum, boards need to establish that cyber risk is an integral part of the business's enterprise risk management (ERM) structure. Beyond that, however, boards need to consider whether the company's ERM program, adequately addresses the many risks—cyber and otherwise—that come from external sources that may be beyond the company's control. Accordingly, boards may wish to consider whether their companies need to implement an "extended" ERM (EEM) program. As noted in a November 2019 *On the board's agenda*,[5] EEM recognizes "that the enterprise is subject to a wide range of acts, omissions, and influences originating inside and outside the enterprise. These… may have positive or negative impacts, but their common denominator is that the enterprise needs to understand who and what they are, the risks and benefits they create, and develop, modify, and execute strategies accordingly."



2. See "On the board's agenda: The tech-savvy board—A director's perspective" at https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-board-effectiveness/us-center-for-board-effectiveness-on-the-boards-agenda-the%20tech-savvy%20board.pdf.
3. The 2019 Spencer Stuart Board Index notes that only 10% of the companies it surveyed had a separate committee dealing with science and technology, up only slightly from 8% in 2014. See https://www.spencerstuart.com/-/media/2019/ssbi-2019/us_board_index_2019.pdf.
4. A recent article in the *Harvard Business Review* points out some benefits and risks associated with cyber measurements, including that they can divorce cybersecurity decisions from the business. See https://hbr.org/2020/09/does-your-board-really-understand-your-cyber-risks.
5. See "On the board's agenda: Outside the four walls: The board's role in extended enterprise management," at https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/audit/deloitte-ch-en-the-boards-role-in-extended-enterprise-management-nov-19.pdf.

Implementing an effective EEM process not only can aid the company in assessing and managing risk, but also can help it to establish and maintain trust throughout the extended "universe" of its stakeholders.

Questions:

- Is our existing ERM process sufficiently robust?
- Do we want or need to implement an EEM program?

- **Disclosing and communicating:** There are numerous legal requirements to report and disclose during and after a cyber attack. For example, state and federal laws require companies to report various types of attacks to authorities. The federal securities laws require public companies to disclose potential risks, and many companies' "risk factors" disclosures include lengthy discussions of the various types of risk that could adversely impact the company. Public companies are also required to disclose developments that could materially impact the company, which would require disclosure of actual cyber attacks or other incidents.

  However, as necessary and important as required disclosure—and related board oversight—may be, boards also need to be mindful of, and to support, communications that are not required but that are critical to establishing and maintaining trust among all stakeholders. Keeping customers, suppliers, and stakeholders informed about your cyber and other risks that could affect them not only helps to maintain good relations with them, but also helps to establish credibility and trust. In particular, it is critical to determine the facts and then to let these stakeholders know about a breach or other cyber incident, ideally before they read about it, possibly saving a relationship that might otherwise be jeopardized.

  Questions:

  - Do we understand which regulators and other authorities we need to notify and in what order in the event of a cyber incident? Do our disclosure controls appropriately address these and other disclosure requirements?
  - Does our crisis management plan cover how we will communicate any incidents to the affected stakeholders?

Conclusion: Respond, recover, thrive

As noted earlier, the challenges posed by COVID-19 and other factors may be steep, but they are not insurmountable; indeed, boards need to demonstrate resiliency both in responding to the challenges of the new environment as well as taking advantage of its opportunities. The role of the board continues to evolve. Investors, regulators, and other external and internal stakeholders increasingly view boards as being responsible for anything and everything that their companies do—or don't do. Even if that were not the case, cyber has been and remains one of the areas that stakeholders expect boards to oversee, recognizing the dynamic nature of this environment. Considering the points outlined above, and the related questions, can help boards to fulfill these expectations.

Additional featured resources

Recovering from COVID-19 disruption: Accelerating security imperatives of the future

COVID-19 cyber risk preparedness and response: Securing your environment against elevated threats

Managing Cyber Risk in a Digital Age

The rise of cyber threats to supply chains amid COVID-19

Authors

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

Deborah Golden
Principal, US Cyber and Strategic Risk Leader
Deloitte & Touche LLP
debgolden@deloitte.com

Contact us

Carey Oven
National Managing Partner
Center for Board Effectiveness
Chief Talent Officer, Risk & Financial Advisory
Deloitte & Touche LLP
coven@deloitte.com

Maureen Bujno
Managing Director and Audit & Assurance Governance Leader
Center for Board Effectiveness
Deloitte & Touche LLP
mbunjo@deloitte.com

Audrey Hitchings
Managing Director
Executive Networking
Deloitte Services LP
ahitchings@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

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

MAKING AN IMPACT THAT MATTERS since 1845