EY Building a better working world

EY Center for Board Matters

What boards are doing today to better oversee cyber risk

In this Transformative Age, technology can make the impossible possible, but it also opens the door to exponentially increased cybersecurity risk.

A company's board plays an important oversight role and is well-positioned to guide management in the development of an effective cybersecurity risk program.

In spring 2019, the EY Center for Board Matters hosted a series of private dinners as well as its second annual day-long Cybersecurity Board Summit. These gatherings brought together board members for discussions on the latest challenges and leading practices in overseeing cybersecurity risk. Their conversations centered on cyber threats, the processes and controls that can detect and mitigate such threats, the importance of planning and preparing for cyber incidents, and the board's oversight role.

Read on to learn what we heard in person from over 100 directors who collectively represent in excess of 200 public companies.

Key takeaways

Our conversations revealed several key actions boards can take as they oversee security risk. These include:

- Set the tone that cybersecurity is a critical business issue; the time and effort the board spends on cybersecurity signifies if it is a priority for the company.
- Confirm that the company's new technology and business arrangements are designed with security in mind from the beginning by embracing a "Trust by Design" philosophy.
- Understand the company's value at risk in dollar terms.
- Understand the company's processes to identify, assess and manage third-party and supply chain risks.
- Make sure the cybersecurity risk management program (CRMP) is independently and appropriately assessed by a third party and the third party should report back to the board.
- Have comprehensive knowledge of the company's ability to respond and recover, which should include simulations and arranging protocols with third-party specialists before a crisis hits.
- Have a thorough understanding of the cybersecurity incident and breach escalation process and protocols within the organization, including when the board should be notified.
- Stay attuned to evolving board and committee cybersecurity oversight practices and disclosures, including asking management for a review of the company's cybersecurity disclosures over the last two to three years with peer benchmarking.

Tone at the top: cybersecurity is a critical business issue

When it comes to cybersecurity governance, one of the most important things a board can do is set the proper tone and align with management on the appropriate risk appetite related to cybersecurity. The board can send that message in part through its own governance and focus on cybersecurity. How much time is the board spending on cybersecurity throughout the year? Is it on the agenda once a year or is it part of most board meetings? Two of the board's primary responsibilities are for strategy and risk management, and it is virtually impossible to have those conversations without a thorough discussion of technology and security.

Boards that have the appropriate focus on cybersecurity are those that consistently integrate the topic into regular discussions about strategy and risk, and prioritize self-education and seek external advice to enhance the board's cyber competency. They also have unfiltered discussions with the Chief Information Security Officer (CISO) in executive sessions and consistently send a clear message to management that prioritizing cybersecurity is part of the company's DNA.

Another critical part of setting the right tone is emphasizing that cybersecurity risk is not just an IT concern, but is an enterprise-wide business issue that cuts across all divisions and functions. Accordingly, management — beyond the security function — needs to be fluent on what controls and processes are protecting its operations, how employees are trained and tested from management down to the front line, and what protocols to follow in the event of a cybersecurity incident or breach.

Through its oversight, the board plays an important role in encouraging management to take broader ownership of cybersecurity risk, and it is incumbent on them to understand if and how the responsibility for cybersecurity is shared across the company.

The CISO might formally brief the board, but the board can initiate a cyber discussion with anyone appearing before it. Infusing cyber in the overall boardroom conversation with all the C-suite executives and division leaders makes evident that cyber is embedded in operations across the company, and that leaders are accountable for their role in supporting the cybersecurity infrastructure. Giving cybersecurity the same prominence as finance and legal in board decisions reinforces the message that it's a critical business issue.

Building in cyber resiliency from the beginning

Despite the challenges posed by today's continuously evolving cyber risk landscape, where the expertise of the bad actors increases and the threats seem to be multiplying daily, directors discussed a key opportunity: building cyber resiliency into the foundation of any company change. As one participant put it, cyber protection "is not hopeless, so long as you think about things at the inception of new initiatives, get the C-suite to recognize what must be done with new technology, systems, products, etc., and ask, 'where is the security?'"

This is a reference to the spreading practice of "Trust by Design," a top-to-bottom mandate to build in cybersecurity when designing or redesigning all products, processes, apps and services or when contemplating an M&A deal or joint venture. The board can support and reinforce this concept by asking about security any time these initiatives are contemplated.

It is important to recognize that the typical Internet of Things (IoT) device may pose challenges for Trust by Design. Generally built with speed in mind, these technologies may offer easy access for bad actors. Similarly, many digital transformation programs don't include security until they are out the door, and the security is bolted on later, a process that almost always creates safety gaps.

Thus, the need for boards and management to think about, and act upon, inserting security at the very beginning — to build trust into everything that is being designed or redesigned. This may seem straightforward, however, there may be internal resistance. The security function is often not brought in for fear that it will slow things down on the business side, so the function must be innovative and practical. This is where boards can ask the appropriate questions early on to make sure that the security and business functions are working together.

> "Cybersecurity risk is not just an IT concern, but is an enterprise-wide business issue that cuts across all divisions and functions.

The risk equation

While building security into the design phase of key initiatives enables companies to mitigate risk, it does not eliminate risk, and companies may need to make tough decisions about where to invest — and that is where risk quantification comes into play.

It is critical that boards understand from management what's at risk, the probability of the risk occurring and the estimated financial cost of the damages that would result. "I need dollar signs on my dashboard, in addition to red/yellow/green designations, to emphasize that business decisions are at stake," said one director.

The potential magnitude of a given risk can be calculated using this formula: *Risk = threat* (e.g., external actor, malware) x *vulnerability* x *impact on the company (*e.g., to its operations, sales, reputation). While numerous assumptions are built into such an equation, directors are seeking greater financial quantification to make more informed governance decisions around risk appetite and tolerance.

Of course, quantification poses its own challenges. One panelist added a caveat in making cost-benefit assumptions in such calculations: "Quantification is a laudable goal," he said, "but don't forget the human element — and the price tags people put on safety and health."

Some companies use a high-value digital vault for the company's crown jewels, protected in the most powerful ways. Your digital crown jewels go into the vault and can't be removed without the simultaneous code approval of two, three or even more individuals.

When it comes to its most valuable assets, a company must spend what it takes to secure them, but it shouldn't overspend unnecessarily. As one panelist put it: "You shouldn't put a $100 fence around a $10 horse." The risk equation is about helping the company identify its most valuable assets, and invest and prioritize security accordingly.

The importance of an objective assessment

Many companies use well-known frameworks and principles to address cybersecurity governance (see sidebar), but using a third party for verification is a key step in linking risks to programs and controls and tying results back to the business. Cyber oversight and verification "can seem overwhelming to civilians who don't do this kind of thing all of the time," said one panelist. "Get a smart third party to assess your program to see if the cooking is right."

Directors discussed many approaches for assessing cybersecurity risk programs. Some boards choose to have a very simple inquiry and observation with the CISO involving a limited number of hours. For more assurance, others seek additional control testing of whatever framework (e.g., National Institute of Standards and Technology (NIST)) the company employs. And for the greatest assurance, an attestation opinion should be sought from an independent third party utilizing the American Institute of Certified Public Accountants' (AICPA) System and Organization Controls (SOC) for Cybersecurity framework, which provides for an entity-wide evaluation of the company's cyber risk management program.

Directors should understand there is wide variability in what goes into a third-party assessment — and it's critical to get comfortable with the provider's experience and confirm whether the budget and scope of work is appropriate.

Boards should approach independent third-party and supply chain assessments in the same way they approach seeking fairness opinions and financial statement auditing. They should also consider the value of an attestation that results in a report, which may build confidence among the board and key stakeholders. One panelist commented, "Trust and verify, but board members also need to follow up."

Addressing cybersecurity governance

Frameworks and principles are required to put governance to work. Two of the most common are:

- The NIST cybersecurity risk framework utilizes five phases: identify, protect, detect, respond and recover. The emphasis during our dinners and summit was on detecting, responding and recovering.
- A refresh of the National Association of Corporate Directors' (NACD) Cyber Risk Oversight: Director's Handbook Series is in the works, but the following five often-cited principles will remain:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
5. Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Third-party risk management

The cyber environment is becoming more perilous every day, as new threats and vulnerabilities multiply. The seemingly infinite number of potential entry points is even more eye-popping — thanks to the steady flow of new technologies, the linkage of billions of devices through the IoT, marriages of systems in M&A deals, and third-party and supply chain vulnerabilities.

"Every single bit of information, every system, every network is a target [and] every link in the [supply] chain is a potential vulnerability," says Christopher Wray, FBI Director. Many view supply chain as a house of cards. The company can do everything to protect its own systems but it is likely reliant on thousands of suppliers. To get comfortable with the supply chain, companies need an extensive third-party risk management governance program. The program will vary, party to party, but key performance indicators and suppliers' Service Organization Control 2 reports can tell you a lot. As networks of suppliers grow and become more reliant on technology, third-party and supply chain cybersecurity risk will continue to be an area of increasing emphasis. The NACD Cyber-Risk Oversight Handbook coming out in early 2020 will include enhancements for overseeing these risks.

Response and recovery

Because even the most robust cybersecurity program is going to leave the company vulnerable to some degree, planning and preparing for response and recovery must be a fundamental component of any cybersecurity risk management program — and a central part of the board's oversight. Tabletop exercises and simulations can serve as an acid test of how prepared the company is for a cyber incident or breach, and provide essential opportunity for exercising the muscles that must respond if a crisis occurs.

What happens if your company goes dark in a cyber-attack? Really dark — across dozens of countries around the world. Your data is missing and your computers aren't working. Even phones connected to your network are out. Moreover, large sections of your crisis planning are suddenly irrelevant — no one anticipated *this* kind of damage. As board members and management struggle to get their footing amid all the chaos, they may regret, far too late, not insisting on more training through simulated crises that might have made the early hours of this real crisis less terrifying and damaging.

A significant attack will be different from what anyone anticipates, and your plan may not fit exactly, or even closely. In fact, while it is important to have a plan or playbook, it is best to focus on key operating principles and be willing to adjust them when the crisis occurs.

Regulatory expectations for cybersecurity governance

The U.S. Securities and Exchange Commission (SEC) has been very transparent and forward leaning in the cybersecurity area — it had its own breach two years ago — and Chairman Jay Clayton is focused on the problem. The SEC just appointed a special advisor on cybersecurity, showing how much the threat is on the minds of regulators in Washington.

It's been nearly a year and a half since the agency issued interpretive guidance on cyber, much of it a carryforward of staff guidance that came out in 2011. The earlier guidance concentrated on disclosures, risk factors and management discussion and analysis (MD&A). The new one went further on disclosures as well as insider trading and board oversight. In between, the agency held a roundtable on cyber in 2014 and went through its cyber incident, in 2017, involving an intrusion with EDGAR.

The agency has let it be known that it will not second-guess good-faith efforts to disclose cyber-related incidents. The volume of disclosures increased in the wake of the 2011 guidance. But there was too much boilerplate in those disclosures and not enough specifics about the companies. Were market stakeholders getting what they needed, the agency asked? And it answered by going a little beyond in the successor guidance. So far, though, a new trend hasn't been detected.

Indeed, in 2018, the first year in which the interpretive guidance took effect, the agency sent out very few comment letters about compliance. It would not be surprising, however, for the letter volume to rise as the agency studies the most recent crop of 10-Ks.

Who owns cyber disclosure oversight? In the agency's most recent review of proxy statements of the 50 biggest companies, the ownership was mostly at the audit committee level.

We asked board members how involved they are in disclosure discussions, or was the matter left to management? "I add commentary and critiques," said one. Said another, "As chairman of the audit committee, I go through proposed disclosures carefully and amend them before they go out. I get little pushback from management."

One piece of advice the members received during the session: management's focus should be on managing risk governance for the company, not on managing the risk of getting a comment letter.

One of the most important things to do is hold tabletop exercises, with as many people as makes sense, with periodic participation by the board. One participant described a quarterly exercise that involves several hundred people in offices around the world. Senior managers are involved, but so are third parties who will be critical resources if a serious attack occurs, including lawyers, crisis managers and forensics specialists.

In the wake of a serious breach, companies need mechanisms in place to resume normal operations as quickly and smoothly as possible. They must have a recovery plan on the shelf (knowing full well they may need to pivot from the plan), fully understand their legal requirements and have policies pre-established for potential threats such as ransomware. They must be able to immediately coordinate restoration activities with external parties and advisors (e.g., public relations, forensic, legal), who should be prequalified, with terms and conditions already agreed upon, and on retainer. And they should closely monitor market events and other breaches to incorporate lessons learned and adjust existing plans accordingly.

"When a cyber crisis hits," said one panelist, "you want to have your plans set and your protocols in place, and not be caught like a deer in headlights." When talking about simulation playbooks, the group noted that there can be unforeseen challenges. For example, when it comes to communicating, many assume telecommunications will be available, or that laptops will be working, but this could be wrong if the company goes dark. They suggested that important numbers of key contacts be saved in multiple places, including hardcopy, and alternative ways of communicating be identified.

Disciplined preparations can go a long way to help a company's leaders be effective and flexible when a breach or incident happens. Management should review where threats and vulnerabilities exist and the potential impact of each, and then confirm that cybersecurity risk management programs address the most important of these risks. The board should ask management about what sort of processes and programs are in place, what testing is being conducted, what issues have been identified and what changes are necessary.

Keep asking and clarifying

As daunting as the cyber threat is, the directors we talked to agreed that they can help keep it at bay with the right governance, processes, protocols, collaboration and hygiene. Above all, board members encouraged each other to keep asking questions of everyone on the senior team and others too. "Communication brings enlightenment. Use pragmatic, basic English in an open-ended Q&A. And don't be afraid." One panelist suggested the best way for boards to govern cybersecurity risk is, "Don't ever get comfortable."

Questions for the board to consider

- Does the board understand the company's total risk exposure of a cyber attack, including financial, legal and reputational impacts?
- Has the board practiced a cyber breach simulation with management in the last year? If not, why?
- How does the board evaluate the company's culture with respect to cybersecurity? For example, are employees routinely trained? What security awareness messaging is regularly conveyed to employees? Are performance bonuses at stake?
- Has the board leveraged third-party expertise, as described in the NACD's Cyber-Risk Oversight Handbook, to validate that the risk management program is meeting its objectives?
- What information has management provided to help the board assess which critical business assets and critical partners, including third parties and suppliers, are most vulnerable to cyber attacks?
- Is the board comfortable with the process used to assess the company's cyber risk management program by a third party, and do the results offer a comprehensive view?
- How is management managing critical vulnerabilities and how old are they?
- Has management indicated where the next cybersecurity dollars should be invested and why?
- How is the company handling privileged access and how do they oversee employees with privileged access?
- Is the company looking externally at other publicly-disclosed breaches to see how it might handle a similar situation, and are lessons learned from those incidents being incorporated into the company's response plan?
- Have appropriate and meaningful cyber metrics been identified and provided to the board on a regular basis and given a dollar value?
- How does management evaluate and categorize identified incidents and determine which to escalate to the board?

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About the EY Center for Board Matters
Effective corporate governance is an important element in building a better working world. The EY Center for Board Matters supports boards, committees and directors in their oversight role by providing content, insights and education to help them address complex boardroom issues. Using our professional competencies, relationships and proprietary corporate governance database, we are able to identify trends and emerging governance issues. This allows us to deliver timely and balanced insights, data-rich content, and practical tools and analysis for directors, institutional investors and other governance stakeholders.

US SCORE no. 06573-191US
CSG no. 1907-3206653
ED None

Learn more about how Fortune 100 companies are approaching cybersecurity-related disclosures.