Building a better working world

EY Center for Board Matters

Understanding the cybersecurity threat

People, process, controls, culture and, yes, technology

On June 11–12, 2018, more than 30 board members and panelists met in Dallas for the EY Cybersecurity Board Summit. The event featured deep-dive discussions on cybersecurity risk and oversight.

The board members who participated sit on about 50 boards, representing a cross-section of industries, geographies and sizes, including many Fortune 500 companies. The goal was to learn more about cybersecurity threats, the systems and controls that could detect and mitigate such threats, and the oversight role the board should play from a governance perspective.

Discussions included an overview of the cybersecurity landscape, lessons learned from recent breaches, the cyber risk executive's perspective, regulatory expectations and leading practices for board oversight. Summit attendees also visited the EY Cybersecurity Center in Dallas, one of six that the firm operates globally on an around-the-clock basis. Here we offer 10 key takeaways and a summary of the various sessions of the program.

Top 10 Summit takeaways

1. Never stop being vigilant; the cybersecurity threat is dynamic and ongoing.
2. The board's role is not cybersecurity risk management; it is cybersecurity risk oversight.
3. Boards may need to restructure their committees and develop new charters to adequately oversee cybersecurity risk management.
4. Directors want and need more education on cybersecurity risk.
5. Boards need to engage a third party to independently and objectively assess whether the company's cybersecurity risk management program and controls are meeting its objectives.
6. These third parties should have direct dialogue with the board to report on the effectiveness of the company's cybersecurity risk management program.
7. Boards and companies need to adequately plan for a cybersecurity crisis, including having an arrangement with all their third-party specialists in place before a crisis hits.
8. The board and management need to routinely practice the cybersecurity response plan.
9. Management should consider providing the board regular updates with key metrics on critical cybersecurity controls communicated in plain English.
10. While improved detection efforts may increase the rate of cyber-related incidents, the rate of noteworthy incidents should decline as organizations improve how they manage and contain these incidents.

“Are we doing well, or have we just been lucky?”

Almost all of the Summit attendees serve on their audit committees, and most serve as chair. Most agreed that they have primary board responsibility for cybersecurity. Yet some feel unsure about what they should be doing — and how well they are doing it. Because of all the unfamiliar terminology related to the sophisticated technology involved, cybersecurity feels functionally different from other oversight responsibilities, they said, and they are searching for more knowledge to inform better judgment.

As one director put it, “Are we doing well, or have we just been lucky?” Another asked, “Have we done enough?” A third put it this way: “How do I get my hands around the issue to know it better? I want to ask the right questions [of management] and be able to interpret their answers to better protect the company.”

So a central theme of the Summit was learning how to leverage the directors’ broad business and risk management experience to better support their oversight role, including ways to obtain necessary information despite possible gaps in cyber-related technical knowledge.

A related theme was recognizing the importance of independence and objectivity in assessing a company’s cybersecurity risk management program and controls and increasing the board’s trust through third-party validation. The people in charge of those controls shouldn’t be the ones doing the assessment or hiring others to do so, because self-protection could likely get in their way while investigating a breach.

The conversation touched on a broad range of topics, including the parameters for cybersecurity disclosure; whether the audit committee, or a more specialized subcommittee, is the proper venue for board oversight of cybersecurity risk; and the metrics to use to determine success or failure.

“I don’t see a trend,” one board member said. “I don’t have any sense of what good or bad looks like.”

> A related theme was recognizing the importance of independence and objectivity in assessing a company’s cybersecurity risk management program and controls and increasing the board’s trust through third-party validation.

An overview of the cyber landscape

At a dinner discussion on the opening night of the Summit, Jonathan Trull, Global Director of Microsoft’s Enterprise Cybersecurity Group, took the attendees on a verbal tour of the cyber landscape. He explained how the explosion of new technologies is transforming business but is also causing the risk to rise sharply.

No matter what level of sophistication you bring to this landscape, you have to remain humble, according to Mr. Trull, fearing what you don’t know and recognizing that you will never know everything. He describes his own concern this way: “What did we miss?”

That said, you need strong controls and, ideally, uniform hardware and processes — to detect attacks, remediate them and be resilient in recovering from the damage. As a best practice, he cited the SANS Institute’s Top 20 CIS Critical Security Controls for Effective Cyber Defense (SANS 20).

In trying to ward off attacks, worry about flaws and shortcomings in the technology, but worry even more about the people who have authorized access to the fortress you are trying to build. “They are often the weak link,” Mr. Trull said. Either inadvertently or intentionally, some of your employees, or those at third parties you deal with or at supply chain partners, will open the door to bad actors. Board members should be asking if their companies have the right controls and processes to limit access to the right people, for the right purposes. Additionally, they should consider whether the corporate culture is permissive or strict when it comes to security concerns. Making sure that the right controls and processes are in place up and down the supply chain is also critical.

There are many ways to keep the door closed, Mr. Trull noted. Give employees in sensitive positions a privileged access workstation, which connects to the company network, but not the internet. Use deception techniques to ensnare attackers, periodically recheck employees’ backgrounds and deploy “red teams” to aggressively hunt for system weaknesses.

But remember to stay humble and be wary. As you close some doors, new ones open, courtesy of new technologies, and these may be harder to close. Thanks to the Internet of Things, for example, interconnected smart devices (everything from sensitive gauges on oil-drilling rigs to kitchen toasters) are proliferating by the millions. Many makers of these devices are low-tech companies — as they jump into high tech, their risk levels are jumping as well, potentially raising your risk level too.

The takeaway is to never stop being vigilant — the cyber threat is dynamic and continuous. The bad guys never really go away. Instead, they keep retooling to stay one step ahead of you, and they only have to be right once. You may think you are the safest company in the world this morning, only to find out that the world has changed this afternoon.

Lessons learned from cyber breaches

On day two of the Summit, one panelist echoed a note from the dinner session. "The number one thing to worry about is your personnel," he said. "But in doing postmortems of significant breaches, it becomes clear that bad decisions by management are another big concern."

Plans are drafted but not put into place, so when a breach comes, the reaction is largely improvised. "And that's really bad," according to the panelist. "People need to know what to do, and the first week is critical — you don't want to spend that week getting people up to speed." Another added, "You need a checklist in place before the crisis hits, and you need to routinely practice the response plan." In fact, you have to do a lot of things now to try to prevent a crisis and to be ready if one occurs.

Your company should pick a cybersecurity framework (the most cited is the one offered by the National Institute of Standards and Technology) and follow up with a maturity and effectiveness assessment, which drives a road map and investment. Organizations should think beyond the framework, which is just a tool, and implement additional controls, like the SANS 20. They should also keep a strong focus on the people factor, including performing background checks, removing credentials following terminations, unplugging acquired technology that is no longer necessary, and the like.

We're heading into a "zero-trust environment," the Summit attendees were told, one in which every system and everyone's identity will be continually checked. For example, is the person who is using this password working at an odd time, based on past patterns? Accessing unusual files? Some companies are already doing this, and there will be a greater uptick in three to five years.

To check on the efficacy of your program, it's critically important to bring in a third party for an independent assessment. The company needs to know which of its crown jewels must be protected at all costs. Often there isn't agreement within the company about this or if the focus is on insurance rather than protection. The assessment should also bake in legal risks: How are you protecting data that is governed by regulations or belongs to outside parties? Too often, the assessment is done on breach day.

Likewise, don't wait for the crisis to hit to start looking for outside help. Find essential experts (e.g., legal, public relations, business continuity) ahead of time and sign them up now. Board members in attendance were reminded that "you will need their cell numbers if a crisis hits on a weekend."

If a big breach does occur, you will also need an independent team, including a technologist, to ferret out the cause. The team should not report to the chief information security officer (CISO).

> We're heading into a "zero-trust environment," one in which every system and everyone's identity will be continually checked.

"It's a big mistake," said one panelist, "to have the people who oversaw the program be the ones to investigate why there was a significant breach."

In a more general way, you have to recognize that people in charge of the program can allow self-interest, whether intentionally or not, to affect their communications to the board. That can affect when or if disclosures are made, opening up additional regulatory and legal risks. "Too often, the IT team tries to fight the kitchen fire for too long before calling for help," noted another panelist.

In terms of a response plan, there are a number of ways to prepare. The chairs of the board and the audit committee can do a "war game" to assess escalation methodologies. The full board can do its own tabletop exercise to figure out a communications strategy.

The key is engagement. But boards are often reluctant to engage in this area even though it is now a core pillar of their role. As a director, it's not necessary to be a techie in order to be effective, but you can't be intimidated by the topic either. Instead, you have to learn enough to ask smart questions and make sure that management's answers are complete and clear, giving you the information you need to effectively oversee cybersecurity risk.

The cyber risk executive's perspective

How can boards best support their cyber executives? The three panelists who spoke during this session underscored the importance of board members becoming savvy enough to ask the right questions — not the "ticky-tacky techie kind," as one called them, but those that are strategic in nature.

Many cyber executives are highly technical and intensely focused on protecting their company's data. They have to be good at determining why something is at risk and then fashioning a fix. Because they have one foot in the tech team and the other in the executive team, CISOs also have to keep the business in mind by balancing the dangers of new technologies against the business need to quickly adopt them. Put another way, they need to help the company find the right mix of risk avoidance and business enablement. So the CISO also has to be good at negotiating and brokering solutions with lots of stakeholders when the business is affected. The goal is to explain the risks well enough to the business leaders so that they take more ownership of the controls to protect the company.

Those risks are constantly changing. Companies and their CISOs have to step back and assess all of the different catalysts — macroeconomic, geopolitical, the pace of technological change, higher consumer expectations and more — and then "raise their game" to update their defenses. IBM's 10 essential security practices were described as a flexible framework to address security risk at any size company.

In terms of the corporate audit function, it's good to have all of the controls in place, but life isn't perfect. "The last thing you want is to have to ask yourself, 'why didn't I catch it?' So you need to assess where the risks are and assign a team to produce a risk mitigation plan, tied to a determination of the company's risk appetite," said one panelist. Companies have to keep up with new threats; communicate with customers, managers and third parties; and figure out protections and workarounds.

They also have to watch out for turf wars among their cyber executives. The CISO, the chief information officer (CIO) and the chief privacy officer all need clearly defined roles and responsibilities.

A good CISO puts together a wish list for the board but also a menu of what is practical. For example, the CISO might say, "For these threats, this is the amount of money we need — and this is what it will cost us if we don't do what I suggest." Transparency with the board is also key. It's good for the board to hear that the CISO is not 100% sure. Still, it is really hard to tally a win, and really easy to say there was a breach.

When presented with so much information, the board may wonder what it all means or how to know if it is good or bad. A dashboard that can be monitored in real time can be valuable, just like when "the red light goes on in a car before the engine seizes up," explained one panelist.

> There is a difference between disclosing more and disclosing better.

Given the growing sophistication of cyber attacks, the proliferation of access points and improved detection efforts, directors should expect the overall rate of cyber incidents to increase. Conversely, the rate of **noteworthy** incidents should decrease as organizations improve their ability to effectively manage and contain these cyber incidents.

Regulatory expectations

In February 2018, the U.S. Securities and Exchange Commission (SEC) released its interpretive guidance on cybersecurity disclosures, which provides a statement of the SEC's expectations.

When there is a breach, companies must take time to understand the full depth and scope of the breach to avoid disclosing dribs and drabs of information, which can lead to additional problems. How long this will take is sometimes left to good business judgment, but companies cannot sit on information forever, especially given some states' time limits for disclosure. The prudent thing to do, if you are contemplating taking action but are not yet sure what the evolving facts will show, is to contact the SEC, as a "placeholder," so that the agency knows that something is going on. Companies can contact a regional office or the headquarters in Washington, depending on the relationships, and then the SEC can attempt to work with the company.

There is a difference between disclosing more and disclosing better. The main focus should be on protecting against cyber attacks and mitigating losses and on educating stakeholders about the company's cybersecurity risks, controls and processes.

Bob Sydow, EY Americas Cybersecurity Leader, recently testified before the Senate Committee on Banking, Housing and Urban Affairs about cyber risks facing the financial services industry. He briefed the board members on several cyber-related changes that Congress is considering, cautioning that any number of things could shift in the event of additional major breaches. The possible changes to consider include:

- **Requiring boards to add a cyber expert:** Should it be approved, this could be a difficult mandate to fulfill, given the shortage of qualified talent. Directors should have more of a role in this area, rather than ceding authority to an expert.
- **Mandatory attestation for cybersecurity:** The American Institute of Certified Public Accountants (AICPA) issued a cybersecurity risk management evaluation and reporting framework in 2017 that includes an attestation component. But the framework is voluntary and intended to be market driven.

- **More consumer protections:** There is a trade-off between privacy protections and information sharing that could limit innovation. For example, would the tough new internet privacy law in the European Union, the General Data Protection Regulation (GDPR), be a good thing for the US?

Separately, a number of states have enacted their own cybersecurity laws, creating multiple sets of regulations. How onerous is that? And would it be better to push for a single federal standard to pre-empt a complex and possibly conflicting set of state initiatives?

Mr. Sydow mentioned the need for more protections against litigation that impedes the sharing of information related to cybersecurity threats and attacks. Litigation's inhibiting effect could be hurting companies that might have escaped or limited their damage if helpful guidance had reached them before they were attacked. But he added that some groundwork for sharing has already been laid by the FBI, which gathers and shares information about encryption keys related to ransomware.

In the case of a cyber incident, organizations should have a policy related to trading. For example, there was a discussion about trading that might occur around the time of a breach. Even if such trading is innocent in nature, it could still lead to reputational damage. Therefore, disclosure controls and procedures should provide an "early warning system" to enable companies to determine whether they need to file a current report on Form 8-K, make disclosure in any other SEC filing, issue a press release or suspend trading in their stock. Boards should make sure that companies have clear restrictions in place and that these policies are widely communicated. This may require companies to assess whether their codes of ethics and insider trading policies take into account measures to prevent trading on the basis of material nonpublic information regarding cybersecurity risks and incidents.

Cybersecurity Center tour

Board members then toured EY's Cybersecurity Center in Dallas, one of six globally that it operates 24 hours a day, 7 days a week, monitoring threats to clients and reacting in real time to prevent attacks or contain damage. EY has more than 7,000 security professionals globally.

Many companies are either not equipped to fully protect their assets or choose to retain a third party to support their internal activities in these areas. For one thing, there is a talent shortage, with estimates of a global shortfall of about 1.8 million security professionals within five years. In addition, centers like EY's have a significantly broader scope and reach than some companies can achieve on their own.

EY's center tracks threats across industries, sectors and geographies, revealing the latest twists in attack profiles and threat exposures. It can extrapolate clues and lessons learned from an attack on one company to a potentially similar situation facing others, all without compromising the confidentiality of any company's operations or data. And the center obviates the need for clients to maintain their own infrastructure.

In addition to detecting and responding to threats, the center applies necessary patches and erects and maintains barriers around legacy systems, among other defensive measures.

On their tour, board members were able to peek into a threat detection and response room, filled with concentric rings of cyber analysts. If anomalies are detected, an analyst may call in a supervisor. The analyst and the supervisor can go to a separate "war room" to discuss next steps, via videoconference, with the affected company's personnel.

If a threat is determined to be serious enough, the analyst will employ tools to immediately shut down the company's affected systems and contain the damage. Specifically, the analyst can move to isolate client "hosts" — PCs, servers, apps — that appear to be infected.

Leading practices for board oversight

In this final session of the Summit, those gathered were asked the inevitable question: How can you organize all of this information on cybersecurity risk oversight?

One suggestion was to use the five principles found in the National Association of Corporate Directors' (NACD) Cyber-Risk Oversight: Director's Handbook Series:

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.

Additionally, five questions can be asked:

1. Where does governance reside?
2. What should management be asked to do?
3. What are the company's critical assets?
4. What cyber threats are the company or others in their industry facing?
5. Is there an appropriate level of cyber insurance, and what does it actually cover?

One Summit panelist described being part of an ad hoc special committee that a medium-sized company used for a deep dive on cybersecurity risk management to find answers to these and other questions. The catalyst for creating the ad hoc committee was an outbreak of big breaches within the company's industry and a sense that the board was not sufficiently prepared to support management in responding to attacks that might come its way.

The ad hoc committee was made up of two audit committee members, the Chief Financial Officer and the CIO. The committee created a charter outlining its responsibilities. One of the committee members wanted more background information on cybersecurity risk management, so they attended the 20-hour NACD Cyber-Risk Oversight Course. The ad hoc committee, which reported directly to the board, looked at the company's assets and determined which were critically important and then put a monetary value on each in terms of mitigating the cyber risk, accepting it, avoiding it or transferring a portion of it. That exercise determined the level of investment — for insurance, red teams and other tools and processes. The ad hoc committee was dissolved once its charter was completed. Cybersecurity risk management is now discussed in depth every six months by the audit committee and every year by the full board.

In assessing all that they had heard at the Summit, the board members discussed why boards are generally uncomfortable dealing with cybersecurity risk. One noted the daunting pace at which change is occurring, in both new technologies and new threats. Another pointed to the different environment that the digital revolution has fostered. And a third said that there just wasn't a lot of codified practice to follow, at least before the appearance of the NACD Cyber-Risk Oversight Handbook. Management might not be that comfortable dealing with cyber risks either, another board member added.

So what are the takeaways from the Summit, and how will the attendees build on what they learned? As a group, they sounded both more aware of the challenges posed by cyber and more empowered to perform their oversight role.

Many said they are eager to follow up on a number of fronts: to learn more about the SANS 20 security controls, about third-party assessments, about metrics and industry benchmarking.

They said they have new questions to raise with their boards about committee oversight of cybersecurity risk. Should that role reside with the audit committee, a more specialized subcommittee or even an ad hoc group like the one described?

As to whether boards should add someone with cybersecurity knowledge, they would want that person to also be knowledgeable about broader business issues and have deep management experience. But they acknowledged how difficult it is to find qualified candidates, with some suggesting searches among the senior military ranks and the use of recruiters.

Most of all, they agreed on the need to press management for more complete and clear answers about their companies' cybersecurity risk management programs, even if that meant asking more questions and adding time to an already full agenda. And they agreed on the need for independent and objective verification of what they are being told.

EY Cybersecurity Board Summit panelists

- **Amy Brachio**, EY Global and Americas Risk Advisory Leader
- **Larry Clinton**, President and CEO, Internet Security Alliance
- **Mark Ferguson**, Board Member, VSE Corp., and a former admiral who commanded US Naval Forces in Europe and Africa
- **Kris Lovejoy**, Founder and CEO of BluVector Inc. and a former CISO at IBM
- **Tim Ryan**, US Cyber Investigations Leader, Ernst & Young LLP
- **Shamoil Shipchandler**, Director, Fort Worth Regional Office, Securities and Exchange Commission
- **Bob Sydow**, EY Americas Cybersecurity Leader
- **Wayne Terry**, VP Corporate Audit Services and ERM Committee Chairman, Flowserve
- **Ben Trowbridge**, EY Americas Cyber Risk Co-Sourcing and Managed Services Leader
- **Jonathan Trull**, Global Director of Microsoft's Enterprise Cybersecurity Group
- **Don Vieira**, Senior Cybersecurity Attorney, Skadden, Arps, Slate, Meagher & Flom
- **Jamie Millar**, Founder and President of SkyBridge Associates, Moderator
- **Stephen Klemash**, EY Americas Leader, Center for Board Matters
- **Chuck Seets**, EY Americas Assurance Markets Leader

Questions for the board to consider

- From a governance perspective, who owns cybersecurity risk for the company?
- Does the board understand the company's total risk exposure from a cyber attack perspective (e.g., financial, third parties, legal, reputation)?
- How does the board evaluate the company's culture with respect to cybersecurity? For example, are employees routinely trained? Are performance bonuses at stake? What security awareness messaging is routinely conveyed to employees?
- Has the board leveraged third-party expertise, as described in the NACD's Cyber-Risk Oversight Handbook, to validate the cybersecurity 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, are most vulnerable to cyber attacks?
- Has the organization considered benchmarking its cybersecurity efforts against comparable companies?
- Have appropriate and meaningful cyber metrics been identified and provided to the board on a regular basis?
- How does management evaluate and categorize identified incidents and determine which to elevate 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. 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.

SCORE no. 03865-181US
CSG no. 1806-2791460

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/boardmatters