Board and audit committee oversight of cyberrisk

On June 9–10, 2015, members of the North American and European Audit Committee Leadership Networks (ACLN and EACLN) met in New York for their 10th summit meeting. On June 9, members were joined by George Allport, Vice President at Chubb Group of Insurance Companies; Eric Friedberg, Executive Chairman and Co-Founder of Stroz Friedberg; and Siobhan MacDermott, Principal in EY’s IT Risk and Advisory Services, for a discussion on cybersecurity and how boards can oversee cyberrisks as part of their duties.

ViewPoints provides a summary of key issues from the discussion, along with background information and insights that members and guests shared before and during the meeting.1 For further information on the networks, see “About this document,” on page 10. For a full list of participants, see Appendix 1, on page 11.

Executive summary

Cyberattacks on companies have grown in breadth and sophistication in the past few years, and have risen to the top of board agendas. But the dynamic nature of the risk, added to the technical aspects, makes oversight a challenge for boards, audit chairs said. At the summit and in discussions before the meeting, members focused on the following themes regarding their oversight of cyberrisks:

- **Assessing cybersecurity risks**

  Unlike many other risk areas, cybersecurity is still a rather new phenomenon, which makes it difficult to know if organizations and their boards are effectively assessing the risks and applying appropriate mitigation, members and experts said. As one expert stated, questions that need to be asked about cyberrisks today are completely different from questions that were asked a year ago. Members also discussed the dynamic nature of the risk environment, and experts warned that the information assets that companies believe may be targeted may not be the ones attackers are now after. They noted that attackers tend to target companies during times of transition, for example, when there are changes in executive leadership or when a merger or acquisition is under way. Attackers are also now increasingly seeking financial profit from cyberattacks, using attacks against companies to influence stock prices and other similar activities.

- **Mitigating cybersecurity risks**

  Cybersecurity risk mitigation efforts have evolved to focus on rapid detection and effective response to breaches, rather than on purely defensive measures, experts said. As part of that effort, experts suggest companies have a structure in place in which someone outside of the IT department leads cybersecurity efforts. Members and experts also recommend working with industry associations and

---

1 ViewPoints reflects the network’s use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Italicized quotations reflect comments made in connection with the meeting by network members and other meeting participants.
the government to share intelligence and best practices, but they said that more protections are needed for companies when sharing information with the government, due to lack of liability protections in the current law.

**Audit committee and board roles in overseeing cybersecurity efforts**

Most members agree that the board must play a critical role overseeing cybersecurity and cyberrisk. Audit chairs present said the audit committee has oversight of the company’s major business risks and the integrity of the financial reporting process, so cybersecurity must be a core responsibility of the committee. However, some audit chairs suggested that the situation has become so complex that boards should set up a new committee or pass responsibility to an existing one, such as the technology committee. Members and experts agreed that using a dashboard to measure and track cybersecurity risks, mitigation efforts, and other activities in a company can help organize board oversight regardless of where responsibility resides. They also agreed that having an external party attest to a company’s cybersecurity efforts would be valuable.

For a list of discussion questions for audit committees, see Appendix 2 on page 12.

**Assessing cybersecurity risks**

In the meeting and in pre-meeting discussions, audit committee chairs wondered whether they are doing enough to oversee cyberrisks. “We all understand that cyber is a major issue. I am looking to define what, at a minimum, I, as an audit committee member, am requiring of management,” a member said. The cyberrisks that companies face today are numerous. They include loss of private customer or employee information, theft of intellectual property, business interruption, shutting down or taking control of devices that may cause real-world physical damage, and using attacks to exploit companies for financial gain. Unlike many other risk areas, members and experts said, cybersecurity is still a relatively new phenomenon, which makes it difficult for boards to determine if organizations are effectively assessing the risks and applying appropriate mitigation. As the nascent cybersecurity insurance market takes root, underwriters are also dealing with how to assess ever-changing cyberrisks. “Five years ago we asked about firewalls, intrusions, incident response plans – if a laptop was stolen and it has personal information of people on it, what do you do? Today, we look at cyberrisk and an organization’s response to it as more of an overall management issue,” Mr. Allport of Chubb said.

The interconnected nature of technology today also means that a company’s cybersecurity risks extend well beyond the company’s boundaries and into the information systems of suppliers, customers, and partners.

**Think like an attacker**

Assessing cyberrisks may be more challenging because of the evolving nature of the risks. “With cybersecurity, you always need updates on how things are changing, because it’s changing so rapidly. You can never say you are absolutely secure, that everything is okay,” a member said. Mr. Friedberg, of Stroz Friedberg, agreed: “You need to assess the risks dynamically; companies need to adapt their thinking to a dynamic landscape. You need to figure out what your critical assets are not only from your point of view
but also from the attackers’ points of view and what they can exploit.” He cited the example of the US Office of Personnel Management, in which seemingly unimportant background information on federal employees and potential hires was stolen. Mr. Friedberg said that as attackers move to exploit such weaknesses in company systems and use breaches as a means of manipulating stock prices for financial gain, companies need to take a harder look at what data they deem needing the highest level of protections.

EY’s Ms. MacDermott added that “attackers look for companies that are in perceived states of turmoil or transition.” For example, she said during changes in leadership, people may be distracted or new names and faces may not yet be known and employees may be vulnerable to spoofing, whereby an attacker pretends to be a new executive in order to get valuable information from employees. Another time of vulnerability, she noted, occurs during mergers and acquisitions, when companies are incorporating new systems and people into their organization. The former organization may not have used the same rigorous cyberrisk scrutiny for their internal systems or their employees. She recommended that cybersecurity be included in due diligence efforts.

Mitigating cybersecurity risks

Efforts to improve cybersecurity and mitigate risks include practices within companies and collaborative approaches between companies and governments. At the recent EACLN meeting, members discussed a number of mitigation efforts, including creating a culture of cybersecurity in which the CEO and top management take leadership roles in the effort and in which employees are thoroughly trained to create a “human firewall” and form an “an emotional bond” with the issue of cybersecurity. At the summit, members and experts also stressed the need for executive and board leadership on cybersecurity, and Mr. Allport said the insurance industry increasingly looks for ownership at the executive management level, as well as board involvement in overseeing efforts.

Leadership structure

A role recommended to lead cybersecurity efforts is the Chief Information Security Officer (CISO) (or the Data Protection Officer [DPO] in many European companies), a senior-level positions tasked with overseeing company protection of information. Mr. Friedberg and Ms. MacDermott both said the CISO or the DPO should report to the CEO or to another senior manager, not to the chief information officer (CIO), which tends to be a more technology-focused role. They also recommended that the CISO or DPO have a dotted-line reporting structure to the board itself. “The CISO is there to give an independent view of what the CIO is doing. That’s why the reporting line needs to be separate,” Mr. Friedberg said.

---

3 European Audit Committee Leadership Network, Cyberrisks and Cybersecurity, ViewPoints (Waltham, MA: Tapestry Networks, 2015), 5.
Yet EY’s 2014 Global Information Security Survey found nearly 80% of CIOs and IT departments have the cybersecurity function reporting directly to them. “Lack of executive buy-in opens the doors to mistakes and cyber criminals; cybersecurity will miss the necessary direction and investments,” the report concluded.

Working with industry groups and governments

Members and experts agreed that cyberrisks are so large, and span industries and political boundaries so vast, that information sharing within an industry and with the government can help reduce the mitigation burden on any one entity. A number of members said their companies are working with industry associations not only to benchmark and share intelligence, but also to combine resources to mitigate risks that companies in common industries likely share. “The problem can’t be solved individually and [our company] can’t go it alone. We have open dialogues at the industry trade associations,” a member said. Ms. MacDermott also emphasized the need for companies to view their cyberrisks through an industry lens, which can spotlight potential risks and, in the case of the financial services industry and industries with critical infrastructure, be aware of existing regulatory requirements regarding cybersecurity. But members also wondered how to share information with competitors without giving away too much: “How do you share information with the competition? IT people have been pretty good at learning from each other, but there’s concern, too. You need the right way, you need controls on it.”

Government initiatives in cybersecurity

Governments in the United States and the European Union are seeking to facilitate a coordinated, structured response to an increasingly organized cyberthreat. As a cybersecurity expert told EACLN members at another meeting, “It takes a network to defeat a network.” In most major countries, governments have set up platforms for public-private sharing of information. However, members were wary about sharing information with the government, a concern that Mr. Friedberg said was not unfounded: “If you give [the Department of Homeland Security or another US government agency] information on the weaknesses that resulted in the breach, another regulator or government agency may come after you for the breach, and [since] the information you gave is not privileged, they can subpoena it.” He recommended that companies involve general counsel in the discussion with the government, so the information that is turned over can meet the government’s needs without jeopardizing the company.

The US government has recognized this issue. For instance, President Obama’s cybersecurity initiative includes a provision that offers liability protection to the private sector when information regarding a cybersecurity breach is shared with the government, a move that members welcome. “As an audit committee member, I want a safe harbor,” a member said. In March, general counsels from 32 major US companies wrote two letters to congressional leaders urging the White House and Congress to pass

---

5 Ibid.
legislation that provides such protections and also to include other safeguards. The Cybersecurity Information Sharing Act is now being discussed in congressional committee.

In the European Union, improving the coordination of cybersecurity across member states has been a major focus of the European Commission’s (EC) Digital Agenda. Efforts have primarily been geared toward improving interaction among government agencies and protecting the privacy of citizen information, and have focused less on public-private cooperation. Conversations about how companies can be protected in sharing cybersecurity information are still in discussions at the European Network and Information Security Agency, which is the EU-wide coordinating body of member-state cybersecurity agencies. Still, an EU-wide platform, similar to the various platforms in the United States for reporting malware, viruses, and other attacks, is still lacking, and most such platforms remain at the country level, such as the UK’s Cybersecurity Information Sharing Partnership.

Prepare for a 100-year-flood

Given that different types of attacks carry varying degrees of severity, experts said companies need to decide what type of event they are willing to be prepared to respond to most. Mr. Friedberg compared the issue to preparing for a 100-year flood that may never happen. “A major decision [companies] have to make is whether you are going to build preventively for severe attacks when they hardly ever happen. If not, then know that you can’t get systems in place quickly if they do occur,” Mr. Friedberg said.

While less severe attacks – such as a distributed denial-of-service attack used to shut down a website – are most common and have been the focus of most efforts, large companies are increasingly in the line of fire for more frequent and more severe attacks. Mr. Friedberg said most companies don’t have the systems and tools in place to deal with those attacks and installing them after the fact can extend response time significantly and hamper the performance of other systems needed to run the business. For large scale, critical attacks, Mr. Friedberg stressed that “you need technology that can record anything at any time. It’s not an easy thing to scan 100,000 computers overnight. You need to decide if you want to invest in technology that you may not need or explain why you were slow to respond should the worst occur.”

Audit committee and board roles in overseeing cybersecurity efforts

The role of the board and the audit committee in overseeing their companies’ cybersecurity efforts remains a key challenge. “What are the questions I have to put to management and get acceptable answers? After I get answers, which aren’t likely to be acceptable, then what additional resources do I need?” a member asked. Among the issues boards are grappling with is deciding where responsibility should lie at the board level.

---

8 Ivan K. Fong et al., letter to John Boehner (Speaker of the House) et al., March 2, 2015.
9 Ivan K. Fong et al., letter to Ron Johnson (Chairman, Committee on Homeland Security and Governmental Affairs), April 23, 2015.
12 CERT-UK, Cyber-security Information Sharing Platform (CiSP)
Full board, audit committee, or another committee’s responsibility?

Increasingly, audit committees are taking on more responsibility for cyberrisks, the experts said. “If you think about market manipulation and manipulation of financial data, that [area of expertise] sits with the audit committee,” Ms. MacDermott said. Mr. Friedberg agreed: “For better or worse, this is going to fall squarely in your lap. We do see audit committees owning it.” Members generally agreed that the whole board needs to be involved in overseeing cybersecurity, but thoughts about what role the audit committee should play differed:

- **Audit committee adds value.** Some members said the audit committee does play a central role in overseeing the risk efforts: “Cybersecurity is part of the audit committee agenda; we need to monitor the risk.”

- **Audit committees are stretched thin already.** Some members agreed on the importance of the issue but said the audit committee is burdened with more than enough now: “The audit committee has to deal with this along with a whole range of other issues. I’m nervous, given the audit committee’s full load, about how to actually get our hands on this.”

- **Another committee’s responsibility.** Other members agreed and said the responsibility should lie with another board function: “Cybersecurity is here to stay. It’s a major issue and it has nothing to do with [the] audit committee. It should be dealt with in the risk committee or a specific committee,” a member said.

Members said that one of the hurdles is the lack of expertise on the board. “However capable boards are, it’s hard to have specialist knowledge on so many areas. I learn enough to ask the right questions, but we can’t make value judgments,” a member said. Ms. MacDermott said that while a specific cybersecurity committee could be an option, it would require finding the right talent that is in short-supply: “Someone who can put technical risks in the context of business risks.” She and an EY partner noted that a board director’s extensive business experience and understanding of the company’s business model is where audit committee members can offer the most value in overseeing cyberrisks: “It’s very easy to get dragged into technical issues. The audit committee can add a lot of value in terms of assessing business risk,” the EY partner said.

To supplement technical knowledge, some members suggested that boards turn to external sources: “It is up to us to ensure we have oversight over what management is doing. We do not have [that] competency on the board but we can get knowledge from the outside.” At a recent cybersecurity conference, directors and experts recommended such a tactic. Acknowledging that the “technical nature of cybersecurity can create a formidable barrier to effective board oversight … the board can invite experts to speak to the board on cyber issues and ask management to provide ‘de-jargoned’ reports in clear, actionable terms.”

Several members mentioned the ways in which their boards are addressing this issue without adding another member to the board. One member’s company has a specific committee to oversee some aspects of cybersecurity: “It consists of board members and non-board experts. There are people from audit and risk.

---

the chief technology officer of the firm, [who is] someone who used to run a [compliance business].” At the recent EACLN meeting, a member discussed how a board member with expertise in cybersecurity is brought in to the audit committee on an ad-hoc basis to help with the issue. Another member said having a variety of people on the audit committee, besides just those with financial expertise, helps as audit committees take on more of these types of issues: “We have a variety of people on the audit committee with a variety of experiences to ask different questions and have different points of view.” And members said directors can also share good practices across all the companies in which they serve.

Current efforts in cybersecurity standards setting

Members also discussed the need for standards as a means of holding management accountable through their oversight. “A consistent application of a standard from a baseline perspective would be very constructive,” a member said. However, while standards are beginning to take shape, members voiced frustration at the current lack of any generally accepted standards to turn to for that consistency. This problem is particularly pronounced in Europe, where standards are sometimes competing and contradictory across borders and where current standards-setting processes lack agility, such that rapid changes in the cybersecurity environment may quickly outpace standards that often take years to gain agreement.14

However, two standards have gained some traction among governments and industry: the International Organization of Standardization’s ISO 2700115 and the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework.16 The two standards are comparable and take similar risk-based approaches to the issue but also have some differences. The “Cybersecurity Framework is better when it comes to structuring the areas of security that are to be implemented and when it comes to defining exactly the security profiles that are to be achieved; ISO 27001 is better for making a holistic picture: for designing a system within which security can be managed in the long run,” one expert said, suggesting the two standards, which are designed to be compatible, can be combined to help demonstrate due diligence in the United States and in other jurisdictions.17

For now, adherence to either standard is voluntary, but experts warn that could change. In the United States, the Securities and Exchange Commission18 and the Federal Trade Commission19 have made public comments that if voluntary programs aren’t effectively used, then new laws and regulations may be put in place. Mr. Allport told members, “If there are standards that are becoming generally accepted and if you’re not using them and you have an incident, those standards are what you will be measured against in court.”

---

15 International Organization of Standardization, About the ISO27k standards (Geneva, Switzerland: International Organization of Standardization).
Create a cybersecurity dashboard

One way that boards and management can create open dialogue is to create a dashboard that everyone monitors for progress. Members agreed that management should track and report metrics that quantify the business impact of cyberrisk mitigation efforts and measure progress.20 “We need a dashboard structure so everyone knows all of the stops along the way,” a member said. According to the Internet Security Alliance, “Metrics can assist in making sure the mitigations and controls are headed in the right direction, … measure the degree to which various security measures have been implemented, … cover operational achievements, such as vulnerability detection and incident management, … and provide estimates of the actual financial losses due to past cyberattacks.”21

Experts recommended that the dashboard include information such as types of attacks experienced, severity, and responses; an analysis of where the company is compared with emerging standards; and threat assessments that could possibly predict future attacks.

Standards gap analysis

While no one standard has been decided upon internationally, the experts said that assessing company efforts against those that are emerging as generally accepted standards, particularly NIST Cybersecurity Framework or ISO 27001, will help companies meet their obligations. “What boards are doing is making sure management is assessing the [cyberrisks and mitigation efforts] against the standards and rating efforts. So what you are doing is a gap analysis and asking, ‘Why are we at a ‘two’ in everything? What should we aspire to?’” Mr. Friedberg suggested. A number of members said this will be a top priority for them: “I’d like to understand what standards the company is using and I’d like an external consultant’s view against those standards,” said one member.

Some members’ boards are hiring this external help directly as part of these efforts. “The newest thing we are doing is using third-parties who can provide assistance from an audit committee aspect. Internal audit are overseeing cybersecurity folks’ efforts and some third-parties are being used to teach internal audit how to oversee those cybersecurity efforts,” another member said.

Threat assessments and predictive analytics

As part of the dashboard, Mr. Friedberg recommended that boards ask for threat assessment reports from management that include not just what attacks the company has seen, but the types of attacks that an entire sector has undergone and what types of information attackers have sought. “In a sector, it could be specific types of attacks. But when we do these assessments for companies, the threats don’t make it to the [board],” he said. He recommended the attack information be aggregated and correlated through a governance, risk management, and compliance (GRC) approach and added to the dashboard.

---

21 Ibid.
Ms. MacDermott said these threat assessments should be overlaid with geopolitical risks and the economics of the business. She also advocated the use of predictive analytics: “The bad guys run businesses like any other. They have KPIs, they have campaigns. If we look and see where an organization falls in the cycle of an attack, [based on that information] we can start to make predictions.” For instance, a company may be operating or moving into a certain geography where attacks on foreign companies are on the rise in an effort to steal information to help boost local competitors. Predictive analytics can help pinpoint what information may be at risk or help internal teams locate an unknown attack already in progress.

Don’t shoot the messenger

Members and experts also discussed the importance of open and candid communication between the board and management. “Don’t shoot the messenger,” Mr. Friedberg told members about making sure management feels free to report honestly about inevitable bad news or shortcomings that may show up on the dashboard. Mr. Friedberg said that part of the issue is that many companies he sees “are wrestling with the question of how much detail and what security metrics management should present to the board in a cybersecurity dashboard. Truth telling is vital. In attempting to synopsize the company’s security posture into a high-level presentation for the board, the CIO may leave on the cutting room floor important negative factors.” He cited the example of presentations to boards he has seen in which “IT conducts third-party penetration testing but omit the fact that the company fared poorly in such testing.” Having a foundation of honest communication and board guidance to management can help make sure the right information makes it into the dashboard for an accurate assessment of the state of cybersecurity in the company, he said.

Review incident response plans

Experts and members said boards should ask about the roles for all functions of the company in the event of an incident, not just top management and the IT department but also general counsel, public relations (PR), and the board. “You need to bridge the gap between technology and response. Who gets attribution for statements released in the event of an attack? The CEO? The CISO? The board? This is not the same as a typical PR crisis. Companies are getting hit on slow – or lack of – response,” Ms. MacDermott said. She and other experts recommended that the plans be rehearsed to see where gaps might be and then followed up with status reports on how gaps are being closed. Mr. Allport told members that analyzing the cost of a response to a serious incident can also help management and boards assess their cybersecurity tolerance. He added that cybersecurity insurance often covers the response costs.

Get attestation on cybersecurity efforts

Among the questions the US National Association of Corporate Directors (NACD) suggests boards ask management are: Has the external auditor indicated any deficiencies in IT and is a framework like NIST used?22 Currently, external auditor responsibilities regarding cybersecurity are limited to financial reporting-related systems and data. “Accordingly, the financial statement and [internal controls of financial reporting] audit responsibilities do not encompass an evaluation of cybersecurity risks across a company’s entire IT

Experts said that a number of organizations are working on attestation standards for cybersecurity, including the American Institute of Certified Public Accountants (AICPA). “Audit committee attestation discussions are happening. The AICPA, the White House, the [Department of Justice], are all looking at this. So many bad things are happening that everyone is looking for someone to take this on,” Ms. MacDermott said. An EY partner added that the auditing profession as well as organizations like the US Center for Audit Quality are also exploring methods for using standards like NIST and ISO 27001 to help clients.

Conclusion

The risks associated with cybersecurity have grown in breadth and impact the past few years and boards are stepping up their oversight of cyberrisks in parallel. “Cybersecurity is a big, big risk that we need to get to get our heads around. It’s a matter for the board and a matter for subcommittees, be it risk or audit,” a member said. The dynamic nature of the risks mean boards and management need to keep constant vigilance over the issue and adjust their defenses and responses constantly to minimize the risks.

“Cybersecurity is a topic at every board and audit committee meeting I attend. It’s moving fast,” a member said. But members and experts agreed that generally accepted standards are needed to aid this work. Experts and members also stressed the need for executive ownership of cybersecurity efforts and boards need honest and business-based assessments of cybersecurity efforts. This information can feed a dashboard that can help management and boards keep in front of the ever-changing risks, experts and members agreed. They also said there is a much needed effort to have attestation on cybersecurity efforts, as well as an external assessment comparing companies with others in their industry and against accepted standards.

About this document

The European Audit Committee Leadership Network (EACLN) and Audit Committee Leadership Network (ACLN) are groups of audit committee chairs drawn from leading European and North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The networks are organized and led by Tapestry Networks with the support of EY as part of its continuing commitment to board effectiveness and good governance.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of ViewPoints lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive ViewPoints are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

Appendix 1: Participants

Members participating in the summit sit on the boards of nearly 50 large-, mid- and small-capitalization public companies:

- Werner Brandt, Audit Committee Chair, Lufthansa and RWE
- Ángel Durández, Audit Committee Chair, Mediaset España
- John Edwardson, Audit Committee Chair, FedEx
- Liz Hewitt, Audit Committee Chair, Novo Nordisk
- Judy Richards Hope, Board Member, General Mills and Union Pacific (alumna)
- Lou Hughes, Audit Committee Chair, ABB
- Shonaid Jemmett-Page, Audit Committee Chair, GKN
- Mike Losh, Audit Committee Chair, AON and TRW Automotive
- Heidi Miller, Audit Committee Chair, General Mills
- Pierre Rodocanachi, formerly Vice Chair and Audit Committee Member, Vivendi
- Guylaine Saucier, Audit Committee Chair, Wendel
- Erhard Schipporeit, Audit Committee Chair, SAP and Deutsche Börse AG
- Tom Schoewe, Audit Committee Chair, GM
- Martine Verluyten, Audit Committee Chair, STMicroelectronics and Thomas Cook

EY participants in all or part of the meeting included:

- Les Brorsen, Americas Vice Chair, Public Policy
- Steve Howe, Area Managing Partner, Americas
- Jean-Yves Jégourel, Assurance Leader, EMEIA
- Frank Mahoney, Americas Vice Chair of Assurance Services
- Christian Mouillon, Global Risk Managing Partner
- Mark Otty, Area Managing Partner, EMEIA
Appendix 2: Discussion questions for audit committees

? Who are your company’s most likely adversaries for cyberthreats and how might they go about an attack? What assets might they target? How are incidents reported to the board?

? How are information assets prioritized in your company? How is the security of those assets reported to the board? How do security teams know if an attack or a breach has occurred?

? What standards do you use? What additional standards would help you in your work overseeing cyberrisks?

? What is the role of the CEO in cybersecurity at your company? Is it a priority for leadership?

? How does your company work with industry associations on cybersecurity? What concerns do you have about sharing information?

? Does your company have metrics regarding cybersecurity? How are they reported to the board? Are those metrics monitored by internal audit?

? What has been your experience working with government? What kind of assistance would you like from the government? What kind of help could your company provide to the government?

? Does your company have cybersecurity insurance? What aspects of an attack does it cover?

? Where should cybersecurity oversight reside on the board?

? How is cybersecurity incorporated into risk management oversight?

? Are incident response plans in place in your companies should an intrusion occur? Do your companies practice responses? Under what circumstances will authorities be notified of a breach?

? What is the role of internal audit in cybersecurity? Are there cybersecurity experts in internal audit? Do outside experts advise internal audit, the board, or management?

? Do you receive attestation on cybersecurity from outside sources? Who provides this service? Does the external auditor play a role in assessing cybersecurity efforts?

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. 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. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc. and EY and the associated logos are trademarks of EYGM Ltd.

EYG no. C90269

For more questions directors can ask management about cybersecurity, see Clinton, Cyber-Risk Oversight, 21.