EUROPEAN
AUDIT COMMITTEE LEADERSHIP NETWORK
ViewPoints

8 May 2015

TAPESTRY NETWORKS, INC • WWW.TAPESTRYNETWORKS.COM • +1 781 290 2270

Cyberrisks and cybersecurity

On 8-9 April 2015, members of the European Audit Committee Leadership Network (EACLN) met in London to discuss cybersecurity, among other topics.[1] For the session on cybersecurity, members were joined by Helen Arnold, Chief Information Officer and Chief Process Officer at SAP SE; François Brisson, global head of Cyber & Technology for Swiss Re; and Chris Gibson, director of the United Kingdom's national Computer Emergency Response Team (CERT-UK).

The *ViewPoints* provides a summary of the key issues raised during the discussion, along with background information and insights that members shared before and during the meeting.[2] For further information on the networks, see "About this document," on page 9. For a full list of participants, see Appendix 1, on page 10.

Executive summary

Cybersecurity has become a top boardroom issue in recent years. Besides the economic cost of cybercrime, which is estimated at between $375 billion and $575 billion annually,[3] a breach can also damage a company brand or market value, factors that cybercriminals are now exploiting. "The cybercriminals are figuring out they can make more money by manipulating share prices and selling stocks than selling credit card numbers," said an EY cybersecurity expert.

At the EACLN meeting in London and in conversations with members before the meeting, discussion focused on several themes related to dealing with cyberrisks and cybersecurity:

- **Assessing cyberrisks** *(page 2)*

  Assessing cyberrisks is difficult due to the evolving nature of the risk, but good practices are surfacing. For example, experts recommend identifying the most important assets of the company and then making sure they are well protected. Knowing what type of attack the company might be at most risk for (such as IP theft, customer information theft or malicious shut down of operations) can also help a company understand its cyberrisk profile and put proper plans in place to mitigate those risks.

- **Mitigating cyberrisks** *(page 4)*

  Mitigating cyberrisks requires more than a technological approach. Making cybersecurity part of the company culture can help create a "human firewall" of protection for company assets. Such a plan would include the CEO taking a leading role in overseeing cybersecurity and the company providing training for all employees, not just on how to defend against attacks but also on how to respond should an attack occur.

- **Audit committee and board oversight of cyberrisks and cybersecurity** *(page 7)*

---

[1] In another session, EACLN members discussed activist investors. See European Audit Committee Leadership Network, *Activist Investors: a Dialogue with Harlan Zimmerman, Cevian Capital*, ViewPoints (Waltham, MA: Tapestry Networks, 2014).

[2] *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.

[3] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (Santa Clara, CA: McAfee, Inc. June 2014), page 2.

EACLN members agreed that cybersecurity needs to be a full-board[4] responsibility but said the audit committee can play a role, including evaluating controls and overseeing external and internal reporting on cybersecurity efforts. But members also said more standards are needed so boards can be sure they are providing the necessary oversight regarding cybersecurity.

Assessing cyberrisks

Experts say the growing sophistication of cybercrime requires a new mindset, one that is less about technology and more about the business. "You need to broaden your mind [beyond technology] to think about who would want to do damage to the company and why," said an EY expert. "It's only when you get your head around the fact that you are not protecting infrastructure, you are protecting assets, that you understand the issue."

The burgeoning cybersecurity insurance industry is also approaching risk assessment from a business perspective, looking at how a breach can impact a company. However, Mr Brisson told members the market is in its infancy, making it difficult to fully assess the aggregated risks: *"Insurers love figures, but right now we don't have any on cyberrisk. For now, we are using history from the past 10 years."* This history includes gathering information from customer claims and talking to customers about the risks they face, which differ by industry, region and company type.

Identify the most important assets to protect

The first step in assessing cyberrisk is to prioritize assets based on the severity of the impact if those assets were compromised. *"You are not going to be able to defend all your information. You need to know which assets are important and which are not. You need to know their criticality,"* Mr Gibson of CERT-UK told members.

To assess cyberrisks, Mr Gibson and other experts recommend boards ask management the following questions:

- What is the company's most sensitive information?
- How vulnerable is it and would the company know if it was under attack?
- What is being done to protect it?
- What would the impact be if high-priority assets were attacked?
- What is the company's response plan to contain and mitigate the impact from such an attack?

Assess the threat landscape

When hackers infiltrated Sony's systems in November 2014, the company not only suffered operational disruption and theft of digital assets, including employee records, personal emails and user account information, it also saw data erased, computers destroyed and its reputation damaged. The Sony incident serves as a prime example of the damage an attack can have on a company, such as the following corporate repercussions:

[4] Full board refers to the supervisory board for European companies that have supervisory and executive boards.

- **Operational disruption.** On 8 April 2015, French international broadcaster TV5Monde was taken off air by hackers claiming to be members of the Islamic State.[5] And in late February 2015, computer-maker Lenovo was attacked by activist hackers ("hacktivists") angry about a controversial software program on the company's branded laptops that left users vulnerable to their own cyberattacks.[6] The group used one of the most common types of operational disruption attacks, so-called DDoS (distributed denial-of-service), which is aimed at shutting down websites and Internet access by flooding servers with spam.

- **Physical destruction.** Government cybersecurity officials are also warning about the risk of physical damage from attacks on network-connected devices. As the Internet of Things (IoT) permeates more connected devices, from automobiles to medical devices to factory controls, hackers may cause real-world physical damage to devices that often fall outside IT control and its cybersecurity rigors. *"The Internet of Things brings a new dimension to this topic beyond the enterprise view. The risk is broad,"* said an EACLN member. For example, a December 2014 report revealed that hackers infiltrated a steel mill in Germany and manipulated and disrupted control systems "to such a degree that a blast furnace could not properly be shut down, resulting in 'massive' – though unspecified – damage."[7]

- **Extortion.** An attack on control systems can also be used to extort money from companies. A 2010 global study found that one in four power companies said they had been victims of extortion attacks after cybercriminals gained access to their control systems.[8] And while Sony's attackers used their access to try to stop the release of the film *The Interview*,[9] other companies experienced the rising use of ransomware, a malicious virus that encrypts data that attackers will only unlock if payment is made. In early June 2014, the U.S. Department of Justice unveiled its efforts to halt two highly destructive viruses aimed at holding businesses hostage by encrypting files and then demanding a ransom for the key to unlock them. Some 41% of the affected businesses had paid the ransom.

- **Data alteration.** Cybercriminals may also be altering a company's data without the company realizing it. For example, compliance risk auditors are now looking at the risk stemming from potential corruption of financial information. And the Center for Audit Quality recently stated: "The financial statement audit and, where applicable, the audit of [internal control over financial reporting], include procedures with respect to a company's financial reporting systems, including evaluating the risks of material misstatement to a company's financial statements resulting from unauthorized access to such systems."[10]

- **Intellectual property (IP) and digital asset theft.** Many companies are also dealing with the theft of protected IP and digital assets by other companies for competitive advantage or by state-actors on behalf of those competitors. One UK company told British officials that it has suffered losses of $1.3 billion due to intellectual property theft and resulting competitive disadvantages.[11]

- **Reputational damage.** While Target suffered financial damage from the theft of customer information in late 2013 – with a ripple effect that a security consulting firm estimates could cost Target, banks, and

[5] Adam Thomson, "Isis Hackers Cut Transmission of French Broadcaster," *Financial Times,* 9 April 2015.

[6] Gabriel Wildau and Patrick McGee, "Hackers Take Down Lenovo Website," *Financial Times*, 26 February 2015.

[7] Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired*, 8 January 2015.

[8] Arthur Neslen, "European Renewable Power Grid Rocked by Cyber-Attack," Euractiv.com, 12 October 2012

[9] Nicole Arce, "Sony Was Warned of Impending Cyber Attack in Extortion Email, Reveal Leaked Messages from Inboxes of Top Executives," *TechTimes,* 9 December 2014.

[10] Center for Audit Quality, "Cybersecurity and the External Audit," CAQ Alert #2014-3, 21 March 2014.

[11] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime,* page 16

retailers in excess of $18 billion[12] – it also suffered reputational damage on several fronts. Claims that the company was too slow to respond and report the breach to customers were followed by a 46% drop in profits in the fourth quarter of 2013, partly as a result of sales losses due to the breach.[13] The reputation of the board also suffered, prompting the proxy-advisor service Institutional Shareholder Services (ISS) to recommend against re-election of members of the board's audit and corporate responsibility committees for the "failure of the committees to ensure appropriate management of these risks …"[14] While the company was able to recover from much of this reputational damage because of improved responses in the weeks and months that followed,[15] and the directors were re-elected, one member said the case *"highlights the reputational risk to [audit committee members]."*

- **Compliance risk.** Governments at the country-level and the European Union (EU) are taking countermeasures and regulatory trends are emerging. Many countries and the European Commission (EC) have regulations covering three main obligations for companies: protect personal information that a company may have on individuals, allow regulatory authorities to audit those measures and notify regulators and affected individuals should a breach occur.[16] However, the strength and scope of these requirements have varied across member states as have the reporting requirements. For instance, previous laws applied to only a narrow scope of company types, such as Internet service providers, telecommunications companies and financial services firms. The newly proposed legislation would expand requirements to all businesses, inside and outside of the European Union, that either process personal information on EU citizens or collect information on EU citizens as part of business transactions. Moreover, the proposed fine for companies that fail to comply is up to 2% of a company's annual worldwide turnover.[17]

Mitigating cyberrisks

In addressing cyberrisks, the mind-set has shifted to being about response and managing intrusions from just being about defense, an EY expert said. "You should still be defensive, there are still things to defend. But they are only valid to a point. Attacks will still get through. The strategy needs to be to plan for the breach, which means extensive training and rehearsals, and knowing how to respond." The risk of a potentially damaging attack occurring may be brought down to an acceptable level, but it is vital that companies have an effective intrusion-management program and response strategy in place should hackers get through the defenses.

Enlist outside help

Several EACLN members advocated the use of third parties to assess risks and help establish mitigation efforts, including response strategies. *"A lot of this is beyond [the board's] collective expertise; one has to acknowledge that. So we bring in experts,"* one member said. Outside experts can also be used to simulate attacks to expose weaknesses and secure them and help teams form effective response plans. Mr Brisson said Swiss Re carefully reviews an insured's software infrastructure and compares it against its database of known

[12] Elizabeth A. Harris, et al., "A Sneaky Path into Target Customers' Wallets," *New York Times*, 17 January 2014.
[13] Paul Ziobro, "Target Earnings Slide 46% After Data Breach," *Wall Street Journal,* 26 February 2014.
[14] Paul Ziobro and Joann S. Lublin, "ISS's View on Target Directors Is a Signal on Cybersecurity," *Wall Street Journal*, 28 May 2014.
[15] Joel Berg, "Target as Target," *Risk & Insurance*, 3 February 2014.
[16] "EU and UK Push New Cyber-Security Regulations," Risk & Compliance, April-June 2014, page 9.
[17] European Commission, Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market, Fact Sheet, 28 January 2015.

vulnerabilities as a key part of their risk analysis: *"The only way we can deal with [aggregating risk] now is to take information from the insured about what software they use, which cloud provider they use, and similar information to give us some view of a unique event."* He also said insurers like Swiss Re can also be a source of help, with some now offering prebreach services to help companies assess their cybersecurity efforts and offer resources to address shortfalls.

Create a culture of security

Defensive technological tools will never be sufficient to prevent all cyberattacks. Good practice emphasizes the vital role that people – employees, vendors, partners and even customers – play in mitigating cyberrisk.

- **Lead from the top.** Members and experts emphasized the fact that senior executives must make cybersecurity a top priority and lead the charge. *"The CEO is the chief risk officer,"* said one audit committee chair. This was echoed by members at the recent Audit Committee Leadership Network (ACLN) in a discussion regarding risk management. "We weren't getting anywhere with cyber [risk]. We still had intrusions; we were still losing stuff we shouldn't. The CEO took charge and now has a group of five people meet with him monthly," said an ACLN member. "There is no one but the CEO who can make this a priority." Ms Arnold said responsibility at SAP lies mainly with the executive board, which comprises executive management, including the CEO, CFO, CIO, chief security officer, chief risk officer, and the data protection officer (DPO – a role mandated by law in a number of European countries and proposed in the new EC directive). *"We all meet to make sure we have a comprehensive view of the existing and potential risk issues."* She said the objective of the board is not to just go through a checklist but to make sure *"the company is ahead of attackers in understanding the risks"* and assessing *"what could potentially hit our company and what is our response to it?"*
- **Limit employee exposure.** Employees often present one of the biggest vulnerabilities. *"We would be naïve to think that some of our employees don't represent the biggest risk,"* said a member. Several experts recommended limiting access to sensitive information, a simple measure that is sometimes overlooked, particularly in an era in which bring-your-own-device (BYOD) policies for mobile devices are gaining acceptance. *"At one company, BYOD is only for top management, but they have access to the most important data and assets. Saying you are not giving it to all people is not good enough when you give it to top management [which may be the biggest risk],"* Mr Brisson said. He added that sophisticated hackers identify potential targets using social media profiles on platforms like LinkedIn and then target them using "social engineering" to trick them into revealing their passwords: *"The culture of the company [and individual behavior] may be out of touch with the real world. We are still adjusting to this new world."*
- **Build a human firewall.** With top management support, Ms Arnold said SAP conducts thorough training of employees to build *"a human firewall"* of defense: *"We realized cybersecurity may not be top of mind of everyone. So we thought about how do we get everyone emotionally attached to this topic, from the board to employees?"* Ms Arnold said companies need to make sure cybersecurity is a priority and becomes part of the culture: *"We drive our security awareness campaigns to make each individual understand it is everyone's job to ensure the company is secure. In cybersecurity, we can only be successful by combining aware and engaged people with the best technology. Internal and external audit are also involved, regularly testing that procedures are followed. Many times cyberattacks start with a combination of social engineering and taking advantage of technological weaknesses,"* Ms Arnold said.

Make cybersecurity a business issue, not just a technology issue

Experts and members said it is important not to think about cyberrisk as just an IT problem. *"This is a business problem that needs a business-driven incident response,"* Mr Gibson of CERT-UK said. *"You need processes in place, teams in place, and you need to run [company-wide] exercises frequently. You can't have an exercise and only the IT guy shows up. You need legal, HR, PR, IT … all of the pieces and then you need to run exercises across them."* SAP's Ms Arnold agreed, saying that *"when it comes to other crises, like an accident, everyone has a role. This is often missing [in cyberattack response plans]. At SAP, we have predefined crisis teams and crisis plan templates. And we regularly run emergency exercises. No matter if the crisis results from a flood, an earthquake or a severe cybersecurity attack."*

Engage internal audit

Experts noted that most cybersecurity measures are process-based and that internal audit should play a vital role in ensuring that those processes are consistently followed. "Cybersecurity is not unlike a lot of business issues in terms of how internal audit would address it."[18]

Among the issues internal audit can assess include:

- Is information security embedded throughout the organization, or is it an IT-only responsibility?
- How comprehensive is the existing threat-and-vulnerability management program and is it aligned with the business strategy and the risk appetite of the organization? How do the company's Enterprise Risk Management processes intersect with cyberrisk management processes?
- Do processes exist to ensure that identified issues are appropriately addressed and remediation is effective?
- What is the organization's response plan and response time when intrusion is detected?[19]

Assign cybersecurity responsibility to the CRO

Some experts recommended that cybersecurity fall under the jurisdiction of the chief risk officer (CRO) or another C-level executive on the business side rather than with IT. *"This is not a pure IT play; it's a business issue. It is the role of risk management to push the business to deal with it,"* said an EY partner. Experts warned that having cybersecurity fall under IT responsibility alone can lead to an overly technological focus in strategy.

Secure the supply chain

Securing the company's supply chain is an important issue, as the Target case illustrated, whereby the attackers gained access to Target customer data through a Target supplier. Also important is assessing the security of IT outsourcers, such as cloud-service providers, who either have access to data or are storing it. *"We live in a connected economy, all business processes travel around the globe now. So how do you make sure your entire supply chain is secure?"* Ms Arnold asked. *"In the end, it is not only about making your own company secure, you have to connect the dots and ensure that your whole business network has a certain level of security."* In much the same way that large companies often push good supply chain

[18] Tammy Whitehouse, "Where Internal Audit Can Help in Cyber-Security," *Compliance Week*, 24 February 2015.

[19] EY, *Ten Key IT Considerations for Internal Audit: Effective IT Risk Assessment and Audit Planning* (London: EYGM Ltd., February 2013), page 5.

efficiency practices down their supply chain, cybersecurity good practices can also be shared with suppliers, Mr Gibson said. And cybersecurity can also be integrated into scorecards to assess supplier readiness.

Tailor cybersecurity to specific threats

Similar to how government may change defense readiness based on threat intelligence, experts recommended companies implement agile cybersecurity strategies that can be adjusted to specific threats. An EY expert suggested companies subscribe to threat intelligence sources that offer intelligence specific to an industry or a company. SAP is using such intelligence and its own data analytics to help with this effort as part of technology it developed that scans its networks, in real-time, for keywords that may indicate attackers are in, or are trying to get into, its systems. Ms Arnold said the company has a full-time analytic investigation team analyzing the potential threats and working to understand patterns that they can feed into their network analysis system to head off breaches quickly should they occur.

Mr Brisson said the insurance industry is also analyzing threat patterns, such as an insured's activity that may increase its cyberrisks (such as launching a new online presence), and scanning for threats on the so-called "darknet," (Internet sites where cybercriminals often communicate or share intelligence). He also said insurers are monitoring public statements by companies, including the CEO, for comments that may put a company at heightened risk. "In the UK, there are a lot of headlines about corporate tax avoidance. That changes the threat profile of a company. [Hacktivists] might want to do something about that. Changing your level of security based on those sets of inputs is a good practice I've seen," an expert said in pre-meeting discussions.

Share information with the government and other companies

"There is no vaccine [for cybercrime] but what helps is talking, talking, taking and sharing," Ms Arnold said, adding that there needs to be more collaboration among companies and between private and public entities to *"align and combine forces and spread intelligence beyond industry and country lines."* Mr Gibson agreed that more work needs to be done to align threat intelligence and responses internationally and among government and private industry. For now, he recommended companies use platforms like the UK's CiSP (Cyber-security Information Sharing Partnership)[20] or similar platforms in other jurisdictions.

Audit committee and board oversight of cyberrisk

Boards have a critical role to play in providing leadership on cybersecurity, members and experts agreed. Boards can interact not only with the CEO of the company but with all the leaders who are ultimately responsible for cybersecurity, ensuring, as a first step in the oversight process, that the authorities and capabilities necessary for implementing cybersecurity measures are established and understood. Even without the technical knowledge, experts said boards can play a vital role to ensure that there is a clear structure of responsibilities, capabilities and accountability.[21]

Audit committee or board oversight?

EACLN members agreed that cyberrisk and cybersecurity is now a top priority for the (supervisory) board. However, members expressed mixed views on where oversight lies: with the full board, the audit committee

[20] For more information see CERT-UK's Cyber-Security Information Sharing Partnership (CiSP).

[21] Audit Committee Leadership Network, *Cybersecurity and the Board*, ViewPoints, (Waltham, MA: Tapestry Networks, 7 November 2014) pp 9-10.

or a separate committee. *"The CEO has responsibility on the business side, and it should be a full-board responsibility on the board side. The audit committee can facilitate, but it should not be their ultimate responsibility. It should lie with the full board,"* a member said, to general agreement.

Members and guests also discussed other board oversight concerns:

- **A need for standards.** One issue members raised is the lack of standards that boards can use to assess a company's cybersecurity readiness. *"There are no standards, so you can't check off [that everything is covered]. It's very dynamic. It would be helpful for me to understand what the best practices are for audit committees to use to say, 'We are covering the right things. We are doing the appropriate level of things,'"* a member said. A number of jurisdictions are working on standards for cybersecurity. Mr Gibson mentioned the UK's Cyber Essentials Scheme,[22] which covers basic technical protections for companies to use. The UK also offers guidance for boards with its *10 Steps: A Board Level Responsibility*,[23] which includes key questions for CEOs and boards. In the United States, resources such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework,[24] are also available. The American Institute of CPAs (AICPA) is also working with NIST and is expected to release standards soon to help internal and external auditors as well as boards assess cybersecurity readiness.
- **Oversight of internal controls.** Members also said they are seeking more help from their external auditor. One suggestion raised by members was for the external auditor to assess the internal controls around cybersecurity, similar to how they assess the internal controls around financial reporting. In discussing the audit committee's role in cybersecurity, one member suggested that the audit committee should *"make sure controls are in place. This is an issue audit committees don't understand."* The member added that audit committees need to be more proactive on getting feedback about how the organization is fairing. Another member agreed, saying that audit committees need to stick to these areas and avoid stepping over the line into management roles. *"It's one thing to be worried as an audit committee chair about controls and another [to worry about] software,"* the member said.
- **Tap board knowledge without adding to committee assignments.** Members recommended audit or risk committees engage with board members, who may have insights but are not serving on any committees charged with cybersecurity oversight. *"We'd like to understand and take advantage of [particular board member skills] without putting people on extra committee assignments. We want to make sure we're engaging all the talent and experience of the board members."*

Conclusion

Cybersecurity has moved from being a technology issue to being a business issue that needs to involve every level of the company. Ms Arnold told members that SAP approaches this issue by building a "*human firewall*" and making sure all employees are *"emotionally engaged"* in the issue. Members also said response plans need to be part of the training of all employees, including board members. Members agreed that creating this culture requires the CEO make cybersecurity a top priority. Members said that while the audit committee can provide support, the ultimate responsibility for a risk as large as cybersecurity needs to be

[22] Department for Business, Innovation and Skills (BIS), *Cyber Essentials Scheme: Requirements for Basic Technical Protection from Cyber Attacks* (London: Crown, June 2014).

[23] Department for Business, Innovation and Skills (BIS), Centre for the Protection of National Infrastructure, *10 Steps: A Board Level Responsibility* (London: Crown, January 2015).

[24] National Institute of Standards and Technology (NIST), Executive Order 13636, *Framework for Improving Critical Infrastructure Cybersecurity*, Cybersecurity Framework, last updated 9 December 2014.

with the full board. However, they also voiced frustration at the lack of standards and external guidance to help boards and audit committees understand what they need to be looking for and what they should be asking management about cybersecurity and cyberrisks.

About this document

The European Audit Committee Leadership Network is a group of audit committee chairs drawn from leading European companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is 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 advisors as they endeavor to fulfil 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, management and advisors who become systematically engaged in this dialogue, the more value will be created for all.

Appendix 1: Participants

Members participating in all or part of the meeting sit on the boards of nearly 40 public companies:

- Dr Werner Brandt, Audit Committee Chair, Lufthansa and RWE
- Mr Aldo Cardoso, Audit Committee Chair, GDF SUEZ
- Mr Ángel Durández, Audit Committee Chair, Mediaset España
- Dr Byron Grote, Audit Committee Chair, Unilever and Anglo American
- Ms Liz Hewitt, Audit Committee Chair, Novo Nordisk
- Mr Lou Hughes, Audit Committee Chair, ABB
- Ms Shonaid Jemmett-Page, Audit Committee Chair, GKN
- Dame DeAnne Julius, Audit Committee Chair, Roche Holdings
- Mr Chuck Noski, Audit Committee Chair, Microsoft*
- Mr Pierre Rodocanachi, Vice Chair and Audit Committee Member, Vivendi
- Ms Guylaine Saucier, Audit Committee Chair, Wendel

EY was represented by:

- Mr Jean-Yves Jégourel, EMEIA Assurance Leader
- Mr Christian Mouillon, Global Risk Management Leader
- Mr Steven Varley, UK Chairman and Managing Partner, UK and Ireland

* Member of the Audit Committee Leadership Network of North America

Appendix 2: Questions for audit committees

- What cybersecurity risks are you most worried about? What kinds of attacks do you see as the most dangerous and/or likely?
- Have your companies experienced any significant attacks? How did they play out? What types of data were targeted? What was the impact of these attacks?
- How are resources allocated for cybersecurity at your company? How is the budget allocated?
- Are information assets prioritized at your company? If so, how is the priority determined?
- What plans are in place should valued assets be attacked? Who is involved in response strategies?
- What kinds of strategies have your companies implemented to secure their systems and operations? How do your companies respond to attacks? Do you feel confident that your companies have cybersecurity under control?
- Is cybersecurity a top management issue? Does a senior executive have ownership of cybersecurity?
- What role does the CEO play in cybersecurity?
- How is cybersecurity communicated to employees? Is it part of the culture?
- What functions do you think government can effectively perform in the area of cybersecurity? What kind of help would your companies like from the government? Under what conditions would you be comfortable with your company sharing information with national or European-level government?
- Is cybersecurity thought of as a strategic risk management issue or an IT issue?
- How are responsibilities for prevention and responses defined, including those for top management? Who reports to the board from management? Is the role of the board defined in response plans?
- If responsibility for cybersecurity is shared among committees, how are issues delegated? How are efforts coordinated?
- Is your board seeking technical expertise to deal with cybersecurity?