AUDIT COMMITTEE LEADERSHIP NETWORK
IN NORTH AMERICA
ViewPoints

May 9, 2017

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

Dialogue with chief information security officers

With cyber threats ranking as a major risk for companies and their boards, directors believe it is more important than ever to have a strong leader managing cybersecurity efforts. Most large companies – over 70% of those with annual revenues over $1 billion, according to one survey – now have a chief information security officer (CISO).[1] The CISO's precise duties, position within the organization, and relationship with the board vary from company to company, however, and these elements remain the subject of debate among security, risk management, and governance experts.

On March 31, 2017, the Audit Committee Leadership Network (ACLN) met in New York to discuss these issues with three prominent security executives: Dr. Andy Ozment, co-CISO at Goldman Sachs; Frank Price, vice president and CISO at CVS Health; and Joe Sullivan, chief security officer (CSO) at Uber. For biographies of the guests, see Appendix 1, on page 9. For a complete list of participants, see Appendix 2, on page 10.

Executive summary

In conversations before and during the meeting, guests and ACLN members considered various aspects of the CISO's role and interactions with the board:[2]

- **The effectiveness of the CISO depends on how the role and scope are defined** *(page 2)*

  CISOs today have many potential responsibilities, though the role is still evolving at many companies. The security executives argued that it is important for CISOs to have a broader, more strategic role, which could include involvement in areas outside information technology (IT), such as mergers and acquisitions. The CISO role requires not only a range of skills and talents, but also a sufficient level of authority within the organization. The guests suggested that for a CISO to be most effective, the CEO and other senior leaders must embrace security as an important part of the company's mission.

- **Thoughtful, structured communication with the CISO enables better board oversight** *(page 4)*

  ACLN members and guests discussed several key issues that a board discusses with its CISO, starting with what framework – for example, the one developed by the National Institute of Standards and Technology – the company is using as a benchmark for its cybersecurity program. The CISO guests also recommended that boards and their CISOs track the top risks the company is facing over time to provide some insight into the performance of the CISO. Boards also have a role in ensuring that the budget for security is sufficient and that it is allocated effectively. Given the complexity of cybersecurity, both boards and CISOs rely on assistance from third-party service providers to help ensure that their companies have adequate protections. Members discussed the value of communicating directly with the

[1] The percentage is significantly lower for smaller companies. Society for Information Management, "CISOs in Only 46% of Organizations: IT Trends Study," news release, August 24, 2016.

[2] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from conversations with network members and guests in connection with the meeting.

CISO, usually at an audit committee meeting but sometimes as a full board, as opposed to hearing about information security from other executives.

For a list of discussion questions for audit committees, see Appendix 3, on page 11.

The effectiveness of the CISO depends on how the role and scope are defined

An overarching theme of the discussion between the audit chairs and the security executives was the issue of what questions directors should be asking their CISOs. Mr. Sullivan suggested a few basic questions for audit committee chairs to consider: *"Who is your CISO? What is their scope? Are they in the right place to be the eyes and ears of the board?"*

Effective CISOs tackle multiple responsibilities

A typical CISO is responsible for a range of technical and managerial tasks. The following outline of key CISO functions was developed by researchers at Carnegie Mellon University's Software Engineering Institute, based on discussions with CISOs and analyses of risk environments and security incidents:[3]

- **Protect, shield, defend, and prevent.** Ensure that the organization's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the enterprise from cyber threats and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization's risk tolerance.
- **Monitor, detect, and hunt.** Ensure that the organization's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries, and report instances of suspicious and unauthorized events as expeditiously as possible.
- **Respond, recover, and sustain.** Minimize [the impact of cyber incursions] and ensure that the organization's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible. Assets include, technologies, information, people, facilities, and supply chains.
- **Govern, manage, comply, educate, and manage risk.** Ensure that the organization … provide[s] ongoing oversight, management, performance measurement, and course correction of all cybersecurity activities. This function includes ensuring compliance with all external and internal requirements and mitigating risk commensurate with the organization's risk tolerance.

In practice, the CISO's responsibilities vary from company to company, depending in part on the company's industry and where the cyber risks reside. Incomplete or inaccurate understanding of where there is risk can also affect the breadth of the role. Mr. Sullivan noted that some CISOs have a narrower area of authority, focused on traditional IT systems that do not include, for example, new customer-facing applications. This means that they do not necessarily oversee all corporate data or have a view into the whole system.

[3] Julia Allen et al., *Structuring the Chief Information Security Officer Organization* (Pittsburgh: Carnegie Mellon University, 2015), 1.

At other companies, the role is broader. Mr. Sullivan said that at Uber, whose fundamental business is based upon consumer-facing digital applications, he has established his own team of engineers to manage application security issues, in some cases taking over security elements from units within the business: *"One example is user authentication. As a result of fast growth and fragmentation of work across engineering, we knew the fastest way to prioritize it would be to have our own engineers manage it."* Dr. Ozment mentioned a similar approach: *"Increasingly, companies believe that they are fundamentally technology firms, so they build a lot of applications themselves. A key part of the job is securing those applications from the get-go."*

Effective CISOs work beyond their formal boundaries. The guests cited examples of involvement with mergers and acquisitions (M&A). As one of his services to CVS Health's M&A due diligence team, Mr. Price assesses the security risk and maturity of target companies, and Dr. Ozment cited two situations at other companies in which a strong information security perspective would have added value in the due diligence process. In one instance, an acquiring company could not integrate the target company's systems because they were so compromised. In another case, the acquirer learned after the acquisition that a foreign government had hacked the target company and stolen its intellectual property.

CISOs need many skills and have diverse backgrounds

If they are to succeed, CISOs need an impressive array of skills and talents, particularly if their responsibilities require them to interact with a broad range of business units. Technical expertise is clearly a core qualification; CISOs must understand the full range of vulnerabilities in the company's IT systems, the techniques used by attackers, and the tools and strategies of defense. However, a CISO's more comprehensive responsibilities go beyond the technical: security decisions must be made in the broader context of the business. Thus, the CISO needs to understand more than just the technical security risks.

What is the career path to the CISO role? Mr. Sullivan remarked, *"We haven't decided as a business community what the right pedigree is for this role; it's all over the place. Until it's a true discipline, we'll continue to have these frustrating conversations. For example, I have a law degree, not a technical degree. On the other hand, people like [Dr. Ozment] have the technology background, but have had to learn the risk component."* The recruiting firm Korn Ferry identified several types of backgrounds among CISOs, though about half fell into the "techie turned executive" category.[4]

CISOs need to be positioned for success within the organization

The CISO also needs sufficient authority, which raises the issue of the CISO's position within the company. An ACLN member asked, *"Is the CISO at a high enough level to command the right interaction with senior leadership?"* Studies suggest that anywhere from 40% to just over 60% of CISOs report to the chief information officer (CIO), while 15% to 22% report to the CEO.[5] One member described a company in which the CISO reports to the general counsel because the legal function drives policy and compliance.

[4] Aileen Alexander and Jamey Cummings, "The Rise of the Chief Information Security Officer," *People + Strategy* 39, no. 1 (Winter 2016), 12.

[5] See Christophe Veltsos, "Is Your CISO out of Place?" *Security Intelligence,* March 1, 2016, and Jack Moore, "Most CISOs Lack Direct Line to the Boss," *Nextgov,* March 3, 2016.

Members and guests explored the drawbacks and alternatives to reporting to the CIO. Mr. Price noted that if the CIO and the CISO do not approach security with the same sense of priority, there will be tension. *"It can't be a relationship where the CISO is asking the CIO to do things that the CIO views as an imposition. It has to be a dialogue about how best to execute,"* he said. Mr. Sullivan mentioned a specific case in which this tension was a problem: *"One peer at a nearby company had an issue with reporting to the CIO, where the CISO didn't have the ear of the CEO and security objectives were not reached because CIO priorities allocated budget elsewhere."* He noted that he reports directly to Uber's CEO: *"I wanted a closer relationship to be able to engage directly with my CEO on a shared vision for security."*

However, Mr. Sullivan also noted that the tone from the CEO about the importance of cybersecurity is ultimately more important than formal reporting lines. The tone from the CIO also makes a difference, Mr. Price added: *"The tension can come when the CIO doesn't perceive security as part of the mission. If security is just tacked on to the technology agenda, there is a strong tension, but if the CIO believes security to be integrated into the mission, then it works to the organization's benefit."* A member also remarked on the importance of harmony across the organization: *"I'm less interested in to whom the CISO reports and more in how those around the CISO are working with them, like audit and compliance. Are they operating like they are on the same team? I don't want to see turf wars."*

Thoughtful, structured communication with the CISO enables better board oversight

Although boards are limited in how deeply they can delve into the technical details of cybersecurity, they have a clear responsibility to oversee and, if necessary, influence what the company – and specifically the CISO – does to protect the company and its assets. Interactions with the CISO are crucial to this effort, but there is evidence that these interactions are not achieving sufficient results. A 2015–2016 survey of IT and security executives at large companies found that only 37% believed that their interactions with the board reduced organizational risk, and only 34% believed that board members understood the cybersecurity information provided to them.[6]

ACLN members and guests discussed how boards and CISOs could improve these interactions, outlining the issues that are most important for boards to discuss with CISOs and identifying the types of interactions – in terms of modes and methods – that are most helpful.

The board should ask CISOs about frameworks, risks, and resources

The CISO guests and ACLN members raised several questions that come up in discussions between the board and the CISO:

- **Which security framework is the company applying?** The CISO guests emphasized the importance of using a standard to track cyber risk and countermeasures, citing as examples the frameworks from the National Institute of Standards and Technology and the International Organization for Standardization. However, there are some cases in which a custom framework may be better suited

[6] Bay Dynamics and Osterman Research, Reporting to the Board: Where CISOs and the Board Are Missing the Mark (Black Diamond, WA: Osterman Research, 2016), 1, 3.

for tracking and managing risk. Mr. Sullivan described an approach he developed for categorizing cyber risks at Uber, in which he built a framework based not only on the standard frameworks but on what it means to be world-class in addressing cyber-related risks: *"This framework forces us to think about what other companies are doing and whether we are improving."* Dr. Ozment noted that a CISO *"needs to flag what is not covered under the frameworks and what is not within the CISO's remit."*

- **What are the biggest risks?** Mr. Sullivan suggested asking the CISO to list the *"five biggest risks in rank order. This can tell the audit committee about the CISO's judgment and priorities, and by comparing risks over time, the audit committee can gain insight into the CISO's performance."* Mr. Price said that audit chairs should ask how CISOs know that the risks within their sights are the most important ones. *"Make sure that the CISO is not focused [solely] on what is easy or what is generally happening in the industry,"* he advised.

- **Are sufficient resources available, and are they being used wisely?** Mr. Sullivan also recommended asking the CISO, *"Do you have sufficient budget, and are you spending it well?"* He said that asking the CISO to measure return on investment (ROI) *"forces the CISO to articulate risk in a concrete way. For example, it may generate better ROI to spend money on forcing everyone to use randomly generated passwords via a password manager and a multifactor authentication approach than on training them to avoid phishing attacks."* He suggested asking how an extra $100 million would be spent, and, conversely, what would be cut if the budget was 20% smaller. Dr. Ozment added, *"It's important to ask, 'What were we not able to do? Describe a project that is a marginal project, possibly because of a lack of resource.'"*

- **How can third parties improve risk assessment?** The CISOs and members found value in engaging third parties to assess a company's cybersecurity program. In some cases, these outsiders review systems and defenses to offer a fresh perspective; in others, they test the systems through friendly hacking. Dr. Ozment noted that these assessments are *"helpful when there's a leadership change and the new leaders need to develop confidence and trust in CISO."* Mr. Price said that *"you want make sure that they assess the entire program from end to end."* Mr. Sullivan added that he always engages outside firms to assess or test his systems. *"I don't want my team to become defensive or complacent by not constantly engaging outsiders,"* he noted.

  One member suggested that high-level access for third parties might be beneficial: *"As an outside firm, it's difficult to get the CIO to see that a problem exists."* Dr. Ozment noted that using third parties for penetration testing requires care, as the third party will gain access to highly sensitive information: *"There is concern with the data security around the data that is collected in that process. We have to really scrutinize both the process and the third party."*

As the board weighs all these issues, participants suggested, it should consider the broader context of the business and the broader costs and benefits. The whole point of security – protecting the business – is lost if the measures implemented hinder the conduct of business too much. As Mr. Price explained, *"I can put you in a suit of armor, but that's not a great idea if your job is to swim quickly across the river."*

Direct and clear communication is key to a successful relationship

The guests and ACLN members brought up two major considerations for improving interactions between CISOs and boards in order to ensure that they derive more value from each other:

- **Who joins the discussion?** Though CISOs sometimes provide input to other executives who then speak to the board, several ACLN members underscored that they want to meet specifically with the CISO: *"We hear directly from the CISO on my boards. Sometimes the CIO tries to jump in, but we want to hear directly from the CISO. We have a regular relationship with the CISO; it's good to have regular communication."*

  All three security executive said that they interact with the board through the audit committee, either annually or at every meeting. In some cases, however, interactions include other members of the board, as one member explained: *"We have found it beneficial to have a joint committee sit with the CISO and CEO to discuss these issues. We get a much richer conversation by broadening the group beyond the audit committee – it's about half of the board three times a year, then the full board twice a year. It's a fundamental issue for the company, so it's important for the full board to hear and discuss."* EY's Center for Board Matters has noted that, "[g]iven the pervasive impact that cybersecurity can have on all facets of company operations, the full board should govern cybersecurity."[7]

- **How is information conveyed?** ACLN members emphasized that they derive the most value from their interactions when their CISOs present technical information in language they can understand. A member said, *"We've been doing a lot of work to develop a risk dashboard to show what the risks are, who manages them, and the timing on mitigating them. It's a way of getting non-technologists to understand these information security issues. We will dive into specific issues, but then pull back to see the fuller landscape."*

  In advance of the meeting, Mr. Price explained his communication technique: *"We stay focused on the level that provides enough information to make decisions … We speak 'geek' only when spoken to, and we use a lot of analogies – that's helpful."* Dr. Ozment mentioned an approach for teaching board members how they can help CISOs communicate effectively with them: *"I know of a company that brought in two CISOs to role-play and demonstrate for the audit committee how to question and engage with their CISO."*

[7] EY Center for Board Matters, *Taking charge: How boards can activate, adapt and anticipate to get ahead of cybersecurity risk* (New York: Ernst & Young LLP, 2015), 3.

What are the top risks?

The security executives shared the risks they are currently most worried about. They mentioned specific threats, and one brought up the readiness to respond to them:

- **State-sponsored adversaries.** The speakers mentioned potential attackers like North Korea and Iran, and in particular their demonstrated willingness to conduct data destruction attacks. China, on the other hand, might steal data, but they have not yet shown a willingness to destroy it.
- **Weaponization of data.** Mr. Price brought up not only the theft of data from the company, but the use of this data to harm the company's customers. A paramount concern for him is *"maintaining the privacy of our customer information across the business."*
- **Company readiness to respond.** For Mr. Sullivan, the biggest worry was not a specific threat, but the ability of the company to defend itself in the event of an attack. Has the company thought through all the steps it would need to take? Mr. Sullivan noted that *"a company can survive a massive breach if they have the right procedures for communicating and managing the attack."*

Conclusion

Mr. Price compared a company's cybersecurity effort to a fluid and fast-moving sport: *"Security is like a soccer game – you are all on the field, not in exact spots but free to move in order to solve issues."* To exercise effective oversight of this effort, the board needs a strong relationship with the person in charge, the CISO. One element is an understanding of how the CISO is positioned within the company, in terms of their responsibilities and authority, and making adjustments as needed. The board should ask the CISO about several key issues, including the security framework the team is applying, the top risks the company is facing, and the resources available and how effectively they are being used. Participants also noted that direct communication between the CISO and the board is helpful, using language and dashboards that convey information clearly for non-technical directors.

About this document

The Audit Committee Leadership Network is a group of audit committee chairs drawn from leading North American 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 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: Guest biographies

Andy Ozment

Andy Ozment is co-chief information security officer at Goldman Sachs. He joined Goldman Sachs as a managing director in 2016. Dr. Ozment has worked in cybersecurity and information security as an operator, programmer, national policymaker, and executive. Prior to joining Goldman Sachs, he served as assistant secretary for cybersecurity at the Department of Homeland Security. There, he led a billion-dollar organization that protected the government against cyber attacks and helped the private sector protect itself. He also spent four years at the White House, where he served as the president's senior director for cybersecurity policy. Prior to that, Dr. Ozment served in cybersecurity and technical roles with the Office of the Secretary of Defense, National Security Agency, Massachusetts Institute of Technology Lincoln Laboratory, Merrill Lynch, and Nortel Networks. Dr. Ozment earned a bachelor of science degree in computer science from the Georgia Institute of Technology. While studying in the United Kingdom on a Marshall Scholarship, he earned a master of science degree in international relations from the London School of Economics and a PhD in computer science from the University of Cambridge.

Frank Price

Frank Price serves as vice president and chief information security officer of CVS Health, the largest pharmacy healthcare provider in the United States, and is responsible for the company's enterprise information security program. Prior to joining CVS Health in 2013, Mr. Price worked in the telecommunications sector as chief information security officer of Alcatel-Lucent and in the healthcare sector as vice president of global information security at Medco Health Solutions (now Express Scripts). Mr. Price has also held information security roles in the banking sector at Dai-Ichi Kangyo Bank and Long Island Savings Bank. He obtained his bachelor of science degree in information systems management from New York University.

Joe Sullivan

Joe Sullivan is the chief security officer at Uber, where he is responsible for all aspects of safety and security. Before joining Uber last year, Mr. Sullivan was the CSO at Facebook, where he led the company's information security, product security, investigations, and law enforcement relationship teams for six years. Prior to joining Facebook, Mr. Sullivan spent six years working in a number of security and legal roles at eBay and PayPal, including, at different times, overseeing user safety policies, coordinating law enforcement relationships, guiding eBay's regulatory compliance efforts, and managing PayPal's North America legal team. Before entering the private sector, Mr. Sullivan spent eight years with the US Department of Justice. As a prosecutor in the US Attorney's Office for the Northern District of California, he was a founding member of a unit dedicated to full-time investigation and prosecution of technology-related crimes. Mr. Sullivan has been active with a number of organizations that promote Internet safety and security, including the National Cyber Security Alliance, the Action Alliance for Suicide Prevention, and the Bay Area CSO Council. He has also served on the advisory boards of a number of start-ups, including Airbnb, BlueCava, Gurucul, and RiskIQ.

Appendix 2: Participants

Members participating in all or part of the meeting sit on the boards of 38 public companies:

- Ron Allen, Audit Committee Chair, The Coca-Cola Company
- Alan Bennett, Audit Committee Chair, Halliburton
- Aldo Cardoso, Audit Committee Chair, ENGIE[8]
- Mary Anne Citrino, Audit Committee Chair, HP
- Pam Craig, Audit Committee Chair, Merck & Co.
- Pam Daley, Audit Committee Chair, BlackRock
- Lou Hughes, Audit Committee Chair, ABB[9]
- Blythe McGarvie, Board Member, LKQ
- Chuck Noski, Audit Committee Chair, Microsoft
- Jim Turley, Audit Committee Chair, Citigroup
- David Vitale, Audit Committee Chair, United Continental
- Maggie Wilderotter, Audit Committee Chair, Hewlett Packard Enterprise

EY was represented in all or part of the meeting by the following:

- Steve Howe, US Chairman and Americas Managing Partner
- Frank Mahoney, Americas Vice Chair of Assurance Services

[8] Member of the European Audit Committee Leadership Network
[9] Member of the European Audit Committee Leadership Network

Appendix 3: Discussion questions for audit committees

- What does the CISO do in your company? What skills and qualities does they need to be successful?
- How is the CISO positioned in your company? To whom do they report?
- What is the relationship between the CISO and the enterprise risk management system?
- What issues should the CISO and the board discuss? What kinds of questions should the board ask the CISO?
- Who takes the lead on the board in discussions about cybersecurity? Which members of management are involved?
- What kinds of communication work best, and at what frequency? At what level of detail should discussions be conducted? How can information be summarized effectively?
- How do the modes and methods of interaction vary depending on the issue at hand?
- Should the board seek external validation of the cybersecurity program?