European Audit Committee
Leadership Network

January 2018

EACLN

VIEWPOINTS

CISOs and the board

Cybersecurity is a critical concern for companies and their boards, which is why it is important to have a strong leader overseeing cybersecurity efforts. Although their precise responsibilities may vary, chief information security officers (CISOs) typically oversee security related to information technology (IT) and may also oversee security relating to production systems and third-party cyber risk. The role continues to evolve to keep up with evolving cyber threats and new regulations. The CISO has been elevated at many companies in recent years, according to a 2017 survey of European CISOs.[1] But just as CISOs' responsibilities differ from organization to organization, so too do their status and relationship with the board. *For guest biographies, see Appendix 1, on page 11. For a full list of participants, see Appendix 2, on page 12.*

Executive summary

On November 15, 2017, members of the European Audit Committee Leadership Network (EACLN) met in London to discuss the CISO and the board with Robert Coles, CISO and head of information protection at GlaxoSmithKline (GSK); Mike Maddison, partner at EY; and Emma Smith, group technology security director at Vodafone. This *ViewPoints* includes background information and synthesizes the perspectives that members shared before and during the meeting on the following topics.[2]

- **The CISO's evolving role and function** (page 1)

  One way that companies are addressing cyber risk is to empower a CISO with broad authority to work across the enterprise in order to protect data and physical assets, monitor for deficiencies, respond to attacks, and educate the workforce. In many cases, this means delving into areas that are not traditionally within the scope of IT. As a result, the role requires an individual with deep technical expertise, strong business acumen, and access to appropriate resources, supported by a team with diverse skills.

- **The CISO's relationship with the board** (page 5)

  Cybersecurity is at the forefront of the board's agenda, with many directors reporting it as the top risk at their companies. Audit committee chairs reported that they benefit from having an open and direct relationship with their company's CISO, which includes communicating at a regular cadence using a consistent framework and common language. They said that a strong relationship makes it easier for boards and CISOs to agree upon adequate resourcing and ensure sufficient oversight of the controls in place to mitigate cyber threats.

For a list of discussion questions for audit committees, see Appendix 3, on page 13.

The CISO's evolving role and function

Large organizations are constantly under threat of a cyberattack from a wide range of actors. To combat this threat, companies are empowering strong, experienced leaders with broad mandates to oversee their cyber defenses. EACLN members and guests discussed the evolution of the CISO role, with a focus on how to position a CISO for success. Mr. Maddison described how the role is changing: *"The role used to be technical, embedded in the organization serving as a compliance function. That profile has changed, along with the level of responsibility and accountability. The role is much broader now, and the expectations far higher."*

The CISO's skills and qualifications

CISOs need an impressive array of skills and talents to succeed, particularly if their responsibilities are comprehensive. Technical expertise is a core qualification. While not all CISOs have IT backgrounds, members said that a CISO needs to understand the full range of vulnerabilities in the company's IT systems, the techniques used by attackers, and the tools and strategies of defense. Because security decisions must be made in the broader context of the business, the CISO also needs business acumen.

One member shared an example of a CISO with a background in human resources (HR): *"One CISO is not a technical expert. He has a background in HR but has a team of experts. There are two main reasons for this choice: his thorough knowledge of the organization and his expertise in human behavior, which is a major issue for cybersecurity."* Dr. Coles and Ms. Smith were receptive to the idea of CISOs without a traditional IT background so long as they have developed technical expertise. Ms. Smith observed that *"the risk of having someone non-technical in the CISO role is that they may not have enough technical knowledge to make quick decisions."* Mr. Maddison noted, *"There's a lack of talent in the marketplace, so many organizations are promoting from within to the CISO role, which can be beneficial since they know the organization. There's also a need for appropriate technical depth within the team. A CISO needs the ability to understand what is a dynamic and quickly changing environment, while also being able to communicate a balanced story to senior management."*

A Russell Reynolds study of the CISO role found that the best CISOs complement their technical capabilities with softer skills: a deep understanding of the company's key strategies, creativity and innovation, the ability to communicate in a way that business executives can understand, the ability to build strong relationships across the company, and the talent to lead and inspire, including acquiring, developing, and retaining top employees.[3] A member noted, *"The role requires a multidimensional individual. While nominally responsible for network security, the CISO is now having a role in product and service security. The role is absolutely fundamental because the risk is existential to the enterprise."*

The CISO's team

As the mandate of the CISO expands, it becomes critical for a CISO to create a strong supporting team of people with diverse skill sets who are enthusiastic about the work. CISOs look at talent from a broad perspective. Ms. Smith said, *"Diversity of experience makes the* *team strong. We look for security experience, but there's no fixed view because we also hire those who are passionate and we can train."*

Mr. Maddison said that it is becoming more common for CISOs to recruit from other parts of the business. As an example, he pointed out that *"internal audit is central to business operations and has been an incubator for developing talent, and the security function should be seen the same way."* Dr. Coles noted that because security of the manufacturing process is so important at GSK, he has prioritized recruiting people with engineering backgrounds and operational expertise for certain key roles.

The CISO's key responsibilities

The CISO typically has both technical and managerial responsibilities. The following outline of CISO functions was developed by researchers from the Software Engineering Institute at Carnegie Mellon University, based on discussions with CISOs and analyses of risk environments and security incidents:[4]

- **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." A member noted that by defining the *"crown jewels,"* or the assets that are essential for business continuity, the member's company was able to identify access points and then mitigate those fundamental risks.

- **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." An example of monitoring identified by members and guests was the use of penetration tests to identify gaps in the program. But Mr. Maddison said that companies need to go beyond penetration testing: *"The level of assurance gained from penetration testing can be fundamentally flawed. It can provide a false sense of security. We are starting to see more companies test from the attacker's perspective by giving ethical hackers a target and timeline instead of just using a risk-based perspective to test."*

- **Respond, recover, and sustain.** "Minimize [the impact of cybersecurity incidents] 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." EACLN members and guests discussed the importance of running simulations. *"Scenario planning is very important. I've taken executive teams through three-hour simulations, even testing the team without the CEO present. This* *process is hugely insightful because it shows how they react in the moment,"* said Mr. Maddison. Ms. Smith said, *"We educate our executives and board because they are a huge target for outside attackers; we need to give them extra protection. We work with them on using social media safely, ethical phishing testing, and a 'Doing What's Right' campaign across the organization to model right behaviors."*

The CISO's partners within and outside the company

The CISO role can encompass systems-related security, including production systems that are not typically considered part of the IT environment. Dr. Coles, for example, has overall responsibility for security at GSK, and he leads on issues including security policy and third-party oversight. Ms. Smith leads both first-line defenses—functional elements of the cybersecurity platform—and second line: information security policy and oversight. Responsibility for security relating to third parties is relevant given that a recent survey of IT and security professionals found that 63% of cybersecurity breaches were linked to third parties with access to corporate applications.[5]

Members and guests described ways CISOs can work with those both within and outside the company to increase security:

- **Coordinating with HR.** It is important for the CISO to work closely with their HR teams, principally to mitigate insider threats. Through careful vetting during the hiring process and proper training of employees, the HR team can reduce inadvertent but dangerous misuses of personal email or social media. Additionally, by being alert to early-warning signs, the team can ward off potentially malicious acts by disgruntled employees.[6] *"I work closely with the director of HR, reviewing issues like user access and acceptable use in order to build the right boundaries,"* noted Ms. Smith.

- **Protecting the company's physical assets.** One member said, *"We should have the CISO cover physical attacks, helping to understand penetration vulnerabilities. It's an underestimated issue; we had checked and believed that we were protected from an IT perspective, yet physically we were not."* In pre-meeting conversations, a member mentioned that the CISO can also be responsible for security related to technology embedded in a company's products: *"Even with packaging, we actually have smart technologies that fall under the CISO."*

- **Working with outside advisers.** One member asked the guests, *"How are you balancing your team's capabilities between in-house employees and third-party contractors?"* While the CISO's teams have grown in recent years, Ms. Smith noted the importance of maintaining strong relationships with external advisers: *"At one time our team was third-party reliant. Now, depending on when or what the problem is, I make sure to have external expertise to lean on when needed."* Working with consultants can be an effective way of educating the CISO's team, said Dr. Coles. Guest CISOs also observed greater coordination between experts in the field, with Ms. Smith noting, *"Inter-sector communication is good and increasingly growing across geographies and sectors. We are starting to see networks* *share more information. We don't see other security teams as competitors; we all have shared foes."*

The CISO's position in the company

In order to carry out their broad mandates, CISOs need adequate authority and access to the appropriate stakeholders. CISOs often report to chief information officers (CIOs), since the CISO role involves managing information technology. EACLN members described varying reporting lines for their CISOs, with most reporting to the CIO or chief technology officer, a few reporting directly to the CEO, and one reporting to the chief operating officer.

Given the growing importance of information security, some security experts suggest that the CISO should report directly to the CEO, arguing that putting the CISO under the CIO results in security concerns competing with—and potentially losing out to—other IT objectives.[7] The technology research firm IDC has predicted that by 2018, 75% of CISOs and chief security officers will report directly to the CEO.[8] However, studies suggest that currently 40% to 50% of CISOs still report to the CIO, while only 15% to 22% report to the CEO.[9]

Dr. Coles stressed that the CISO's stature in the organization, and access to the board are more important than official reporting lines: *"What matters is the CISO's relationship with the CEO and the ability to access the board directly."* Ms. Smith agreed: *"I'm not layered in the organization and have direct access to the CEO and the board. I don't think I could completely make the company secure if I was only focused on compliance; however, quick execution is essential and being closely aligned with technology makes that easy."* Mr. Maddison said that it is important for the CISO to be viewed as a peer and a key resource across senior management.

The CISO's relationship with the board

Boards have clear oversight responsibility for risk in general and cybersecurity specifically, but they are limited in terms of how deeply they can delve into the technical details of cybersecurity. The board's interactions with the CISO are part of this effort, but there is evidence that these interactions are not always achieving the desired results. A recent global EY survey found that 52% of the IT and security executives surveyed consider their boards not fully knowledgeable on cyber risk or the measures in place to mitigate the risk at their companies.[10] Similarly, another survey of IT and security executives 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.[11]

Presenting key issues to the board

Members and guests outlined the issues that are most important for boards to discuss with CISOs:

- **Threats and incidents.** Boards want to know about actual incidents, especially the most significant ones, to understand their impact and how to neutralize the effects. Members said that it was not realistic for them to hear about all incidents; some mentioned seeing aggregated information, such as data on the frequency of attacks. As the cybersecurity program matures, more incidents will be reported to the board, Ms. Smith said: *"The board needs to know how many incidents occurred, including what happened, who did it, and why. I make sure to use the same language and same type of report each time that I present."*

- **Organizational maturity.** Guests noted that the International Organization for Standardization's (ISO's) 27001 standard and other frameworks are helpful guides for both building and assessing an organization's cybersecurity program.[12] To create a common language and a common set of risks for management and the board to review, Ms. Smith highlights key controls from those standards when she presents to the audit committee: *"I then measure and report on how effective we are in working on these controls and risks—a controls effectiveness score. I profile those risks into a program and budget."* In a pre-meeting conversation, a member said, *"It's the audit committee's responsibility to understand where the company stands in terms of a maturity scale. I ask what the CISO's plan for the cyber program is. How are we getting better? You have to understand in terms of timeline."*
- **Independent assessment.** The high stakes associated with cybersecurity, which may include legal risks for the board itself,[13] also raise the question of whether the board should supplement communication from the CISO with input from independent advisers to help assess the threats and evaluate the CISO and the cybersecurity program.[14] Some members mentioned that their boards rely on outside consultants for assistance, including penetration testing and other services.
- **Budget.** Members and guests agreed that the board plays an essential role in ensuring that the CISO's team has adequate resources. Spending needs to align with the level of risk the organization is willing to incur, noted one member: *"If you wanted to prevent all cyber threats, you'd have to spend three times capex [capital expenditure]. Instead, you need to define the company's risk appetite and determine what is non-negotiable."* Direct contact with the CISO allows directors to better gauge whether the CISO's program has what it needs. Ms. Smith described an additional benefit of the board's role in cybersecurity budgeting: *"Communication between the CISO and the board helps the CEO hear what we are up against."*
- **Industry trends and benchmarking.** Some CISOs also provide information about broader trends in the industry, such as what other companies are doing or what regulators are demanding. Knowing how the company's cybersecurity compares to competitors is also important. One member found it valuable for the CISO to benchmark the number of cyber incidents against those suffered by competitors, a common practice in some sectors. Another member said, *"It's a journey, and despite inadequacies, by benchmarking we've discovered that we're actually ahead of the curve."* Dr. Coles agreed that this practice is beneficial: *"I make sure to show where we are in relation to our peers, showing the impact of key risks and how we're mitigating those threats."* Mr. Maddison noted that recent advances in benchmarking mean that the company can gain more quantitative insights:

"Now, there are quite technical ways to benchmark and measure how controls are working and feed into a dashboard that shows where the organization stands."

CISOs identify top cybersecurity threats

Guest CISOs shared their perspectives on the most significant cyber threats currently faced by large companies.

- **Rogue actions of nation-states.** The CISOs said that nation-state actors pose the most serious risk to companies. Dr. Coles said, *"The biggest risk is collateral damage from the actions of a nation-state or other political actors, such as terrorist organizations, or states stealing intellectual property."*
- **Failure to take basic precautions.** Guests also emphasized the importance of security hygiene—applying security patches and updating legacy systems. One attendee observed, *"Everyone is very nervous of service outages, so patching can be delayed. Patching is often seen as routine and doesn't get the attention it deserves. But companies need to make bold decisions."* Dr. Coles agreed: *"We used to do major testing of patches, but that takes time. Now, we test patches over a smaller sample size and take some risks."* Mr. Maddison added, *"The greatest risk is a failure to address hygiene. You can't always think about the sexy, high-tech issues while forgetting those fundamental elements."*
- **The intersection of physical and digital security.** Guests highlighted the importance of considering how cyber and physical security interconnect. *"The biggest long-term threat is the defense of where physical and cyber come together,"* said Ms. Smith. *"The weaponization of a physical asset's digital capabilities is real; this issue is on the radar of both the military and terrorist groups,"* noted Mr. Maddison.

Fostering productive communication

Some members expressed frustration over the technical jargon used by security professionals and said that their own lack of fluency in this area can complicate communication when working with CISOs. In pre-meeting conversations, one member said, *"Boards understand the problems associated with cyber risk, but there's a knowledge gap between non-executive directors and CISOs, which makes it difficult to have a sensible discussion."* With limited time to present to the board, communicating enough detail in a concise manner can be difficult for a CISO. Steve Holt, EY's financial services cybersecurity leader for Europe, the Middle East, India, and Africa, noted, *"Level setting is essential when speaking to the audit committee. One should define cyber for them, because some organizations have a narrow view. It's important* *for the committee to know the scope of the CISO's role, to understand the purpose of communicating with them, and to hear the full story of cyber risk for the organization."*

There are a number of considerations for improving communication between CISOs and boards to ensure that both parties derive more value from the interaction:

- **Level of detail.** Board members are generally not experts on cybersecurity, so CISOs need to consider the technical detail of their presentations to the board. *"The amount of information can be overwhelming; it is a lot to present in a single presentation to the audit committee,"* noted Dr. Coles, who also observed, *"There are two key ways of measuring: showing where we are today and then where we need to get to."* A member expressed frustration with the number of presentations on cybersecurity: *"I'm seeking a method out of madness. We have too many presentations on cyber. It seems that we're constantly talking about random occurrences. Is there a framework that is comprehensive, so that we know we're not missing elements?"* Dr. Coles described most methods of reporting on cyber as *"home grown,"* and attributed this to fact that every organization is unique.
- **Frequency of communications.** One survey of security executives found that a plurality of respondents, 44%, reported on the status of the organization's cybersecurity program on a quarterly basis, while 26% reported monthly, 18% reported less than quarterly, and just 12% reported weekly.[15] Members reported routinely receiving briefings from their CISOs when major incidents occur; additionally, dedicated cybersecurity discussions take place in the audit committee about twice a year. Guests emphasized the need for an open line of communication with the board, as well as one-on-one time with the audit chair, and noted the importance of the audit committee listening, supporting, and challenging the CISO.
- **Venue.** Some EACLN members noted that while the audit committee often takes the lead on cybersecurity, the full board is also briefed at least once a year and also receives a briefing in the event of a serious cybersecurity incident. Some boards delegate aspects of cybersecurity to a risk committee, if there is one. Several members said that although the CISO may not present or attend all board meetings, cybersecurity almost always comes up as a topic.

The seriousness of matters under discussion affect all three considerations: a serious security breach, for example, will likely be covered in greater detail, with more frequent updates, and at the board level, and it will likely involve an expanded group of executives, including the CEO.

Members agreed that more needs to be done to educate the board on cybersecurity so directors can work more effectively with the CISO. *"Most audit committee members are on a steep learning curve, far behind the attackers,"* said one member. In pre-meeting conversations, another member said, *"As audit committee members, our knowledge needs to increase in order to understand what the CISO does. Honestly, the CISO could give the audit committee whatever they wanted, but if we could make recommendations to them about how to present, it would be helpful."*

Conclusion

Cybersecurity remains a top concern for nearly every major company and its board. One way that many companies are addressing this risk is by empowering a CISO to coordinate the company's preparation and defense in a much broader way than before, with a reach across the organization that goes well beyond IT. Members and guests emphasized the importance of an open line of communication between the board and the CISO and use of defined frameworks and a common language to discuss the company's preparedness and plans. As businesses become more digital, the stakes will only increase. *"We are all grappling with how organizations will change; this change will be constant,"* said Ms. Smith.

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 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, management, and advisors who become systematically engaged in this dialogue, the more value will be created for all.*

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 counsellors 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.

Appendix 1: Guest biographies

Emma Smith

Emma Smith joined Vodafone in 2015 as Group Technology Security Director, responsible for all aspects of information and cyber security. The global security teams in Vodafone are responsible for setting security policy in line with local laws and regulations, implementing new security technologies and controls, securing new products and services and 24x7 cyber defense capabilities. Emma is passionate about security. Specifically, about evolving security to protect customers against changing threats and the opportunity to contribute to improving the safety of the communities we operate in. Prior to joining Vodafone, Emma was Security Director at the Royal Bank of Scotland for seven years. In her role, she was responsible for fraud prevention, information & cyber security, intelligence, physical security, business resilience and records management. Before that, she held a number of leadership positions within the Group Internal Audit team and RBS and Royal Mail.

Mike Maddison

Mike Maddison is a Partner and the leader of Cyber Security Services for EY across Europe, Middle East, India and Africa. Mike has almost 30 years of experience in the field of technology risk, cyber and physical security. Mike has delivered significant transformation programs within end user environments as well as developing cyber risk mitigation strategies and appropriate organizational designs. Prior to joining EY Mike was based in the Middle East leading Risk Assurance Services across the region for another Big4 firm. These services include enterprise risk management, internal audit, cyber and information security, technology risk, corporate governance as well as operational and finance controls assurance and consulting. Prior to working in the Middle East, Mike was based in London, with responsibility for all assurance and advisory services relating to cyber security, business resilience, testing and privacy in the UK and EMEA. He has regularly contributed to broadsheets as well as radio and television and industry publications. In addition, Mike has spoken at conferences globally on the topic of cyber security and provided briefings at the highest level of government on security and intelligence issues. Before moving into management consultancy Mike held a number of senior risk roles in end user environments.

Dr. Robert Coles

Dr. Robert Coles joined GSK in October 2013 as their first Chief Information Security Officer. Robert owns the information security risk and is responsible for providing global leadership across GSK. He is accountable for establishing information security strategy and direction, building a global information security capability and overseeing all of the information security initiatives across the company. Prior to GSK, Robert was CISO and head of digital risk and security at National Grid (a major US/UK power utility) where he created and lead the function since 2009. He has also held CISO positions at Merrill Lynch and interim Head of Group Information Security at Royal Bank of Scotland, and was the lead partner in KPMG's Information Security Services for EMEA. Robert has extensive links with several major industry information security networking groups and government security agencies. He also has links with a number of universities and participates in leading edge research, particularly with Royal Holloway where he is a visiting professor. He undertook his PhD in psychology at the University of Leeds in the perceptions of information and IT risk and has published on this topic.

Appendix 2: Participants

Members participating in all or part of the meeting sit on the boards of over 50 public companies:

Mr. Aldo Cardoso, ENGIE

Ms. Carolyn Dittmeier, Generali

Mr. Ángel Durández, Repsol

Mr. Eric Elzvik, Ericsson

Mr. Byron Grote, Tesco, Akzo Nobel, and Anglo American

Ms. Siân Herbert-Jones, Air Liquide

Mr. Lou Hughes, ABB

Mr. Arne Karlsson, Maersk

Ms. Dagmar Kollmann, Deutsche Telekom

Mr. Richard Meddings, Deutsche Bank

Mr. Nasser Munjee, Tata Motors

Ms. Guylaine Saucier, Wendel

Mr. François Thomazeau, Bolloré

Ms. Martine Verluyten, STMicroelectronics and Thomas Cook

Mr. Lars Westerberg, Volvo

EY was represented in all or parts of the meeting by:

Mr. Jean-Yves Jégourel, EMEIA Assurance Leader

Mr. Hywel Ball, Managing Partner, Assurance, United Kingdom & Ireland

Appendix 3: Discussion questions for audit committees

- What does the CISO do in your company? What skills and qualities do they need to be successful?
- What is the professional background of your CISO? How does that background make them well suited for the role?
- How is the CISO positioned within 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?
- Should the board seek external validation of the cybersecurity program?

Endnotes

[1] Mark Lueck, "2017: The Year of the CISO," 2017.

[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. Quotations in italics are drawn directly from conversations with network members in connection with the meeting.

[3] Matt Comyns, Tim Cook, and Jesse Reich, *New Threats, New Leadership Requirements: Rethinking the Role and Capabilities of the Chief Information Security Officer* (Russell Reynolds Associates, 2014), 5.

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

[5] Carin Hughes, "Why Third Party Cybersecurity Matters," *CSO*, December 7, 2016.

[6] Andie Burjek, "HR and IT: The Dynamic Duo in Fighting Cybersecurity Risks," *Workforce*, May 4, 2016.

[7] CIO staff and CSO staff, "Eight Reasons the CISO Should Report to the CEO and Not the CIO," *CIO UK*, January 6, 2017.

[8] CIO staff and CSO staff, "Eight Reasons the CISO Should Report to the CEO and Not the CIO."

[9] Christophe Veltsos, "Is Your CISO out of Place?" *Security Intelligence*, March 1, 2016.

[10] EY, *Path to Cyber Resilience: Sense, Resist, React* (London: EYGM Limited, 2016), 16.

[11] Bay Dynamics and Osterman Research, *Reporting to the Board: Where CISOs and the Board Are Missing the Mark* (Black Diamond, WA: Osterman Research, 2016), 2–3.

[12] For more information, see "ISO/IEC 27001:2013(en)," International Organization for Standardization, 2013, and "Cybersecurity Framework," National Institute of Standards and Technology, accessed October 18, 2017.

[13] Bob Barker, "Ignoring Board Liability for Cyber Risk Is Unwise," *Cybergovernance Journal*, May 2, 2016.

[14] 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), 5.

[15] Bay Dynamics and Osterman Research, *Reporting to the Board: Where CISOs and the Board Are Missing the Mark,* 5.