Audit Committee Leadership Summit

August 2022

ACLS

VIEWPOINTS

The future of cyber risk

While cybersecurity has been a well-established topic on board and audit committee agendas for several years, constant vigilance is required to keep pace with an ever-changing and intensifying risk landscape. Companies are experiencing ongoing nation-state and ransomware attacks, increased exposure fueled by digital transformation efforts, and risks stemming from emerging technologies such as artificial intelligence (AI) and machine learning.

On June 29–30, 2022, members of the North American and European Audit Committee Leadership Networks (ACLN and EACLN, respectively) held a discussion on the future of cyber risk with three guest experts: General (Ret.) Keith Alexander, founder, chairman, and co-CEO of IronNet, Inc. and former director of the National Security Agency; Tim McKnight, executive vice president and chief security officer of SAP; and Lee Foster, senior vice president of Alethea Group.[1]

This *ViewPoints* summarizes three key themes that emerged from the discussion:

- **Cyber threats are fueling a growing and complex risk landscape**
- **Boards should prepare for emerging cyber risks**
- **Disinformation is an emerging risk for companies**

For guest biographies, see Appendix 1 (page 7); for a list of network members and other participants, see Appendix 2 (page 9); and for a list of reflection questions, see Appendix 3 (page 10).

Cyber threats are fueling a growing and complex risk landscape

General Alexander and Mr. McKnight provided an overview of the evolving cyber risk landscape and emerging technologies that are important for boards to keep on their radar.

Companies are on the front lines of geopolitical cyber threats

Increased tensions between the United States and nation-states like China and Russia are fueling cyber threats that directly impact companies, General Alexander said, and he underscored the need to stay on high alert. His guidance closely aligned with recommendations made earlier in the meeting by US Federal Bureau of Investigation Director Christopher Wray.[2] Today, military conflict frequently involves cyberattacks, either to disrupt command and control or to damage critical infrastructure; nation-states, cybercriminals—and sometimes a blend of the two—often target companies.

China is particularly concerning in this regard, as General Alexander explained: *"China has said in its military doctrine that they will use cyber as part of their campaign in the event of a war. In addition to stealing intellectual property, they also would destroy data … creating a near-term risk for small and mid-sized companies in your supply chains."* He stressed the importance of a collective defense, with the private and public sectors working together to effectively combat cyber threats.

Technology advancements create new types of risks

Mr. McKnight discussed how technologies like AI and machine learning can create opportunities for companies but also bring new cybersecurity and ethical risks. Transparency and integrity are key to risk management. *"You need to retain the ability for humans to override automated processes if an outcome is being driven by bias or inaccurate models,"* he explained. He recommended that boards ask questions about what checks and balances are in place as new technologies are developed and deployed at their companies. Criminals can quietly modify the data that trains a machine learning system, leading to misclassifications and operational damage that may take many months to detect.[3]

Quantum computing could significantly disrupt cybersecurity

Quantum computing is a fundamentally different and more powerful computing model that experts believe will bring substantial value creation opportunities. But it also presents significant security risks because existing encryption methods rely on limits to the processing speed of modern computers. Quantum technology could vastly increase this speed, making today's encrypted data vulnerable.

While audit chairs reported limited knowledge about the risks associated with this emerging technology, EY's *Quantum Readiness Survey 2022* highlighted several: "The prospect of quantum being used to break existing encryption protocols cannot be discounted. Perhaps of greater significance, however, is the prospect of 'store now, hack later' attacks—in which bad actors intercept valuable encrypted data now, because they believe that it can be decrypted within a few years, once sufficiently powerful quantum computers emerge."[4] The report noted, however, that advances in quantum encryption should help alleviate the potential for damage. The question of when quantum will more fully emerge is debatable, said Mr. McKnight, but he emphasized that boards should begin preparing now. *"Security will be significantly challenged when quantum arrives,"* he said.

Boards should prepare for emerging cyber risks

As boards look at future threats and vulnerabilities, Mr. McKnight highlighted several important considerations.

Audit committees can drill down to understand and prepare for future vulnerabilities

"Given the threat landscape, what is missing from our audit and risk committee agendas?" one member asked. Mr. McKnight recommended that audit committees ask management about near misses, not just the big breaches. He also advised members to *"bring in business unit leaders on a rotating basis to explain their cybersecurity practices. It's an important way to change the pair of glasses you are wearing on the topic."* A member pointed out that *"audit committees need good information and effective dashboards."* Mr. McKnight agreed, noting that such tools can be especially important when assessing preparedness for oversight of future risks and technologies.

Members and guests also discussed security risks associated with the cloud. *"Security is now multilayered and includes 'on premises' and 'on the cloud.' It is increasingly complex but provides resilience beyond what was available in the past,"* General Alexander said. Mr. McKnight advised members to confirm that their companies have strong cloud security teams.

Talent management is a top cyber concern

The global cybersecurity workforce has some 2.72 million unfilled positions, according to the 2021 (ISC)^2 Cybersecurity Workforce Study, and cybersecurity leaders believe that a lack of skilled talent is the topmost barrier to meeting corporate security needs.[5] More cybersecurity professionals and expanded expertise are needed, said Mr. McKnight. He underscored that it is *"very competitive to land talent,"* and boards should ask their chief information security officers about how they develop and retain talent for their cyber and technology programs. Mr. McKnight shared good practices that companies can implement, such as working closely with human resources teams and universities to develop talent early. He also advised investing in automation to perform *"lower value-add services"* where possible.

Organizations need to become crypto agile

Data security is a high priority for companies amid the current threat environment, where data is continuously targeted by a myriad of bad actors. AI, machine learning, and quantum capabilities used for malicious purposes bring even more urgency to this issue. As existing encryption methods become ineffective, companies should stay abreast of new technologies and prioritize protecting sensitive data and assets. Mr. McKnight noted that his team is *"very focused on crypto agility right now,"* and he advised members to make it a priority and to ensure that their companies are prepared to rapidly respond to any changes in cryptographic standards.

Disinformation is an emerging risk for companies

Quantum attacks on encryption may be in the future, but disinformation is a current reality. Companies are facing targeted disinformation—the intentional spread of false or manipulated information to harm an organization, brand, or person—at growing rates. Members were interested to learn more about the scope of risk and good practices to strengthen their oversight efforts.

The scope of disinformation risk

Mr. Foster described the current state of disinformation threats for companies and its overlap with cybersecurity, including several key themes:

- **Disinformation creates a wide range of risks for businesses.** While typically seen as a threat in the political realm, disinformation has increasingly been recognized as a risk to companies. *"Companies are just as much a target as any political entity,"* emphasized Mr. Foster. Disinformation can include false press releases, fake social media accounts, deepfakes, and other types of falsified information. All can cause significant damage, explained Mr. Foster, citing diminished consumer trust, brand and reputational damage, stock price and/or financial market manipulation, and even physical security risks as examples. Mr. Foster described a recent instance of disinformation where a vaccine company, Ocugen, experienced bot-like accounts coordinating to manipulate its stock performance. *"Stock price manipulation is just one of the many elements companies should be thinking about when it comes to disinformation,"* said Mr. Foster.

- **Types of attackers vary and have different motivations.** Nation-states are one type of offender and have significant resources to put behind disinformation campaigns. Others include for-hire contractors, ideological individuals, or disgruntled former employees, customers, or stakeholders. Conspiracy theorists also may target a company, as was the case in a disinformation campaign against Wayfair, which involved conspiracy theorists falsely claiming the company was trafficking children. Attacker motives range widely and may include financial or political gain or a desire to disrupt companies or markets.

- **Disinformation is easy to create and spreads quickly, making it particularly dangerous.** Unlike traditional cyber threats, targeted disinformation events have a low barrier to entry, requiring less sophistication and very little technical acumen, said Mr. Foster. *"It doesn't take much to stand up a network of inauthentic accounts and push out a false narrative around a company,"* he explained. Disinformation also spreads quickly. Social media platforms can easily amplify disinformation, causing it to go viral and have even more harmful effects. *"An attacker can seed a misleading narrative into a legitimate online community, which can then unknowingly spread false content,"* Mr. Foster explained.

- **Deepfakes are a growing concern.** All three guests agreed that deepfakes are rising in prevalence and pose unique disinformation risks. Deepfakes use AI to alter video, images, and recordings to create new footage of events that did not actually occur. Mr. McKnight explained that *"deepfake technology is quickly getting to the point where it will be very hard to tell what is real versus fake."* People in leadership positions, such as politicians and celebrities, are frequent targets, and the technology could also be used to impersonate corporate executives.

Good practices in risk oversight

Most members reported that disinformation is a new risk area that is not on their boards' current agendas, but it should be. One said, *"It is not really part of the dialogue at my company yet, but it is clearly a growing trend, and I think audit chairs should get more explicit about it."* Another pointed out that *"as directors of large public companies, we are used to activists putting out extreme statements, but this raises it to another level."* Mr. Foster reiterated that large companies face heightened risks because they may be more likely to be swept into geopolitical conflicts given their global footprints.

Because being prepared is critical to effectively respond to targeted disinformation, boards must ensure that management proactively monitors for disinformation and that incident response plans are in place. Mr. Foster advised that companies should *"watch for disinformation and try and catch it early—before it creates a crisis. Stay ahead of what can otherwise suddenly spin out of control."* General Alexander agreed and underscored the point: *"You have to get ahead of the narrative. If you're behind, it's very difficult to get in front again."*

Mr. Foster provided members with actionable recommendations for their companies:

- **Identify relevant stakeholders and assign responsibility.** Boards should ensure that responsibility for disinformation risk is clearly assigned to the appropriate stakeholders within their companies, starting with the internal threat response team, if there is one. Aspects of disinformation could be relevant for legal, HR, communications, cyber, IT, and physical security functions. Several members suggested investor relations should be included as well.

- **Train employees to recognize disinformation.** The nature of disinformation makes it difficult to distinguish. Companies should continuously monitor for disinformation and provide training to employees, especially those responsible for disinformation risk. *"Make sure they understand the disinformation threat space and how to work within it,"* advised Mr. Foster. *"It's not just what is being said—it's the indications that show it is part of a larger, orchestrated campaign targeting the company."* One member remarked that disinformation-specific monitoring could be strengthened at his company: *"Our marketing group tracks social media constantly, but the disinformation angle needs to be beefed up."*

- **Create an incident response plan and hold practice drills.** Similar to ransomware and cyber risk planning, boards should ensure a crisis response plan is in place that outlines key processes and decision makers in the event of a disinformation incident. Boards should be involved in practice exercises with management, Mr. Foster advised, which will *"allow you to better react should an incident arise."*

About this document

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

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

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc., and EY and the associated logos are trademarks of EYGM Ltd.

Appendix 1: Guest biographies

General (Ret) Keith Alexander, founder, chairman, and co-CEO of IronNet, Inc., is one of the foremost authorities on cybersecurity in the world. A four-star Army general, he was previously the highest-ranked military official of USCYBERCOM, National Security Agency/Central Security Service, where he led these US Department of Defense agencies during the conflicts in Afghanistan and Iraq when attempted cyberattacks against the US were on the rise.

In recognition of cyber's increasing importance, President Barack Obama and Defense Secretary Robert Gates appointed General Alexander as the first commander of USCYBERCOM, a newly created military institution charged with defending the nation's security in cyberspace against sophisticated cyber threats to businesses and government operations in an increasingly interconnected world.

A leader with vision and a pragmatic approach to tackling the ever-changing cyber-threat landscape, General Alexander built IronNet to bring this knowledge and experience to the private sector and fill in a critical gap between cyber threats and available security technology. IronNet provides best-in-class cyber defense based on complex behavioral analytics based on artificial intelligence and machine learning models and a Collective Defense platform that allows organizations to exchange anonymized attack intelligence in real time.

General Alexander holds a bachelor of science degree from the US Military Academy, a master of science degree in business administration from Boston University and master of science degrees in systems technology, physics, and national security strategy.

Tim McKnight is executive vice president and chief security officer at SAP. He heads SAP's global security unit in the office of the CEO board area, reporting directly to Christian Klein, CEO and member of the executive board of SAP SE. He is responsible for SAP's overall security strategy, ensuring that SAP and its customers have a consistent and convenient security experience, establishing SAP as a recognized and trusted leader in the industry. In his role, Mr. McKnight develops, implements, and manages SAP's overall security policies, standards, and guidelines in accordance with ongoing security initiatives and worldwide IT, physical and personnel security, cybersecurity activities, data protection, and privacy laws.

Before joining SAP in December 2018, Mr. McKnight was chief information security officer for Thomson Reuters, responsible for all aspects of the company's global information-security risk management program. Prior to that, he served as chief information and product security officer for General Electric, executing its information security and IT risk strategy. Previously, Mr. McKnight was executive vice president of Fidelity Investments' information security and technology risk. He also served in various IT security leadership roles at Northrop Grumman, BAE Systems, and Cisco Systems. Mr. McKnight began his career at the Federal Bureau of Investigation as lead investigator of National Infrastructure Protection Center matters, including high-tech crimes, corporate espionage, foreign counterintelligence, and telecommunications fraud.

In addition to these roles, Mr. McKnight has held the roles of chairman of the Internet Security Alliance and taught undergraduate courses in digital forensics as an adjunct professor at Georgetown University. He is also a member of the board of advisors for Google Cloud, Amazon Web Services, ClearSky Security Fund, and Tenable.

Lee Foster is senior vice president at Alethea Group, where he oversees the company's disinformation and research analysis team and data science research and development efforts. Mr. Foster joined Alethea Group in September 2021 after nearly seven years at cybersecurity company FireEye's Mandiant Intelligence division, where he most recently held the title of director of information operations analysis. At Mandiant, Mr. Foster founded and led an internationally recognized team of intelligence analysts specializing in identifying and tracking cyber-enabled disinformation campaigns. In that role, he oversaw the team's groundbreaking investigations exposing notable state-sponsored influence activity, including the first public exposure of Iran's extensive online influence activity and its attempts to manipulate the domestic politics of the US and elsewhere, and the NATO/Eastern Europe-focused "Ghostwriter" campaign. He has a particular passion for advancing analytic tradecraft and integrating data analytics practices with traditional intelligence investigations and analysis.

Over the years, Mr. Foster has briefed numerous government entities and corporations on disinformation and cyber threats around the world and is a frequently sought-out voice by media on disinformation and information operations. He has appeared on CNN and MSNBC and provided dozens of print and radio interviews to media outlets including the Washington Post, BBC, Reuters, and numerous others. He holds a master of arts degree in intelligence and international security and a master of arts degree in political science, and he is currently completing his master of science in analytics.

Appendix 2: Participants

The following ACLN members participated in all or part of the meeting:

- Joan Amble, Booz Allen Hamilton
- Judy Bruner, Applied Materials and Seagate Technology
- Jeff Campbell, Aon
- Janet Clark, Texas Instruments
- Pam Craig, Merck
- Ted Craver, Wells Fargo
- Dan Dickinson, Caterpillar
- Bill Easter, Delta Air Lines
- Lynn Elsenhans, Saudi Aramco
- Tom Freyman, AbbVie
- Gretchen Haggerty, Johnson Controls
- Bob Herz, Fannie Mae and Morgan Stanley
- Akhil Johri, Boeing and Cardinal Health
- Lori Lee, Emerson Electric
- Arjun Murti, ConocoPhillips
- Louise Parent, FIS
- Ann Marie Petach, Jones Lang LaSalle
- Peter Porrino, AIG
- Kimberly Ross, Cigna
- Tom Schoewe, General Motors
- Leslie Seidman, GE
- Cindy Taylor, AT&T
- Fred Terrell, Bank of New York Mellon
- Tracey Travis, Meta
- Jim Turley, Citigroup

The following EACLN members participated in all or part of the meeting:

- Julie Brown, Roche
- Marion Helmes, Heineken
- Pilar Lopez, Inditex
- Benoît Maes, Bouygues
- John Maltby, Nordea
- Marie-José Nadeau, ENGIE
- Karyn Ovelmen, ArcelorMittal
- Ana de Pro Gonzalo, STMicroelectronics
- Jon Erik Reinhardsen, Telenor Group
- Guylaine Saucier, Wendel
- Maria van der Hoeven, TotalEnergies

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

- Julie Boland, EY US Chair and Managing Partner, and Americas Managing Partner
- John King, EY Americas Vice Chair—Assurance
- Patrick Niemann, EY Americas Leader, EY Audit Committee Forum

Appendix 3: Reflection questions for audit committees

- ? How confident are you that your company's existing processes for cyber risk management are adequate to address the heightened threat landscape and emerging risks like artificial intelligence, machine learning, and quantum computing?
- ? As data migrates to the cloud and device connectivity increases, are you receiving new or different information around cyber risks? What is most useful?
- ? How effective are the questions you ask management related to understanding cyber risks?
    - ○ When discussing cybersecurity with management, do you ask about near misses in addition to prevented breaches?
    - ○ Do you hear from multiple levels of management, such as business unit leaders, about cybersecurity?
- ? How does your board provide oversight of talent management related to cybersecurity? How comfortable are you with how cybersecurity talent is being developed and retained?
- ? Is your board aware of the potential risks that quantum computing poses to your company's cybersecurity (such as to current encryption systems)? Do you know the status of your company's crypto agility?
- ? Has your company been the target of targeted disinformation? What factors could put your organization at particular risk for disinformation?
- ? How is your company working to prevent, detect, and mitigate disinformation?
    - ○ Does your company monitor specifically for disinformation?
    - ○ Is disinformation risk currently addressed as part of your board conversations?
    - ○ Do you have a disinformation incident response plan in place?

Endnotes

[1] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from members and guests in connection with the meeting but may be edited for clarity.

[2] See Audit Committee Leadership Summit, *Dialogue with FBI Director Christopher Wray,* ViewPoints (Waltham, MA: Tapestry Networks, 2022).

[3] Cyber Risk Director Network, *Emerging Cyber Risks,* ViewPoints (Waltham, MA: Tapestry Networks, 2020), 6.

[4] EY, *How Can You Prepare Now for the Quantum Computing Future: EY Quantum Readiness Survey 2022* (London, Ernst & Young LLP, 2022), 17.

[5] (ISC)^2, *A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)^2 Cybersecurity Workforce Study, 2021* (Alexandria, VA: (ISC)^2, 2021), 20–24.