Audit Committee Networks

ACN VIEWPOINTS

Today’s Cybersecurity Front

December 2024

The cybersecurity threat landscape is ever-changing, with increasingly sophisticated attacks targeting organizations of all sizes. As threats grow in both scope and complexity, detection, defense, and response become more challenging, requiring boards and audit committees to continually reassess their approach to oversight.

On October 16, 2024, members of all six of Tapestry Networks’ regional Audit Committee Networks met with Shawn Henry, chief security officer at CrowdStrike, who shared insights on the current state of cyber threats, their trajectory, and how audit committees can prepare for future cyber risks.

For a list of reflection questions for audit committees, see page 8. For lists of participating audit chairs, see Appendix 1 (pages 9–10), and for the guest’s biography, see Appendix 2 (page 11).

This *ViewPoints*[1] covers key themes that emerged from the meeting and related conversations:

Threat actors are more sophisticated than ever

The current cyber threat landscape is characterized by the accelerating speed, scope, and sophistication of attacks. CrowdStrike's 2024 Global Threat Report and similar briefings highlight new threats: compressed time between initial entry and breach, artificial intelligence lowering the barrier to entry for low-skilled attackers to launch sophisticated attacks, and the use of social engineering, malicious insiders, and other human-centered attack modes.[2] Members observed similar trends, with one noting, *"Every day, there is something new. What used to be easily detectable now proves very challenging due to the sophistication of these attacks."*

Mr. Henry briefed audit chairs on the threat landscape, focusing on three elements: threats, vulnerabilities, and consequences. *"The variables involved may change over time, but those three essential elements will not."*

On threats, he noted, *"It is critical to understand who is targeting you, how, and why."* He described different types of threat actors and highlighted how their motivations and strategies have evolved:

- **Nation-states.** The main actors continue to be China, Russia, North Korea, and Iran— "the Big Four"—which fund cyberattacks for their strategic advantage. While their attacks have historically pursued objectives like stealing sensitive information or espionage in support of national interests, Mr. Henry noted that the attackers' focus has changed in recent years. For example, Russia used cyberattacks against Ukraine to instill fear, weaken targets, and sow confusion in support of military objectives, and China targeted Taiwan to spread criticism of the country's presidential candidates.[3] *"There are many nations building or enhancing these capabilities; it is not just the Big Four. For companies, this means there are more threat actors on the field,"* Mr. Henry said.
- **Hacktivists.** Often loosely organized, hacktivists are motivated by specific political or social agendas. For example, hacktivists based in Russia have targeted Ukraine in support of Russian geopolitical interests.[4]
- **Organized crime groups.** These highly structured groups pursue cybercrime primarily for financial gain. Ransomware attacks have transformed the landscape in recent years, increasing the number of crime groups and exposing companies of all sizes and sectors to greater risk. *"The number of cyber criminals has surged due to the high return on investment and low risk of being caught,"* Mr. Henry said.

- **Insider threats.** Mr. Henry said that malicious insiders are a growing risk. While the stereotypical insider threat came from a disgruntled employee, it now includes employees planted by nation-state actors. *"We've seen adversarial governments place operatives in US companies and attempt to co-opt existing employees,"* Mr. Henry said. He noted recent examples of major companies unwittingly hiring North Korean foreign intelligence officers into their IT departments.

READ MORE »

Audit Committee Leadership Network ***ViewPoints—Cybersecurity and Data Privacy: A Dialogue with Chief Information Security Officers and Data Privacy Leaders***

New technologies increase organizational vulnerability

Companies must prioritize technological innovation to maintain competitiveness, but tech advances can also widen the scope of vulnerability. *"New technologies enhance a company's effectiveness, and we should adopt them, but we must do so thoughtfully and with careful consideration,"* Mr. Henry said.

He highlighted several areas of vulnerability:

- **Personnel.** Employee identities and credentials need robust protection. EY's recent cybersecurity disclosures report revealed that attackers targeted employees in over two-thirds of known breaches.[5] Adversaries may start with phishing and then leverage compromised credentials to move through systems undetected. Remote work increases vulnerability by making breaches harder to prevent in less controlled settings.
- **Operational technology (OT).** Where IT systems manage information and data, OT systems typically control physical devices in areas such as manufacturing, energy production, transportation, and HVAC (heating, ventilation, and air conditioning). As the "Internet of things" becomes a reality, millions of devices, large and small, are being connected to networks. Each creates a new potential attack point. When IT and OT teams work independently, they can leave exploitable gaps, giving attackers access to the network. Compounding this risk, outdated technology—often still in use in OT systems that lack modern security or support—creates additional vulnerabilities. *"Companies keep using it, but it might not provide security anymore because nobody is supporting it,"* Mr. Henry said.
- **The cloud.** Cloud computing can be safer than on-premises computing, but it has its own vulnerabilities, which have to be managed as companies rapidly shift business activities and data to the cloud. CrowdStrike reported that cloud environment intrusions increased by 75% from 2022 to 2023 as adversaries learned to abuse features unique to the cloud.[6] Mr. Henry noted that many organizations overlook the

importance of understanding their cloud provider's security capabilities and reliability. *"You put your data in the cloud, but adversaries might be able to gain access to it,"* he cautioned*. "You can't just adopt a technology without understanding the security implications."*

- **Artificial intelligence (AI).** *"Many companies have adopted AI across their organizations for its value, and it will become a significant component of the economy,"* Mr. Henry said. *"However, this adoption comes with vulnerabilities. Companies must thoughtfully assess the risks and establish guardrails around AI."* Members discussed the risks posed by AI: *"There are so many ways the bad guy can get in. We've all seen the Zoom calls generated with AI, and that's a mess,"* one audit chair observed. Echoing this sentiment, another member added, *"It's getting worse over time, even just taking a video and being able to put words in someone's mouth."* Mr. Henry further cautioned members that entering data into large language models can expose sensitive information to unauthorized parties, and that AI models may generate plausible but factually incorrect responses, raising the risk of spreading misinformation alongside the increased threat of a security breach.

Successful attacks can result in significant consequences

"When a vulnerability gets exploited by an adversary, it turns into a consequence," Mr. Henry said, underscoring the need for companies to proactively recognize and address threats before they become serious. Consequences can include major operational disruptions, financial losses, and reputational damage. He highlighted several disturbing trends:

- **Ransomware remains a persistent threat.** Ransomware attacks continue to increase in frequency and sophistication, Mr. Henry reported. High-value sectors like critical infrastructure and healthcare remain targets, but businesses of all sizes and sectors are at risk. One member observed, *"Big companies are targets, but smaller companies are also becoming frequent targets*.*"* Mr. Henry noted that ransomware tactics have become more advanced: *"With companies improving their backup strategies, some attackers*

Should companies pay ransoms?

Mr. Henry generally advises clients against paying ransoms. However, he acknowledged that the decision is fraught with complexity. For instance, one company targeted by ransomware would have faced collapse if it did not recover its data and intellectual property, and therefore decided to pay. Companies should consult internal and external counsel, communications professionals, and other key advisors when making such decisions.

Should companies involve the FBI?

Members asked for Mr. Henry's perspective on engaging the FBI in the event of a cyberattack. *"Every company should have a contact at the FBI,"* Mr. Henry said. Even if immediate contact is not needed, having an established relationship enables faster response if and when an incident occurs. The FBI can help identify threat actors, initiate law enforcement actions, and possibly coordinate with regulators to manage disclosure timelines. He noted that companies should still consider potential liability and regulatory issues even when involving law enforcement.

not only steal and encrypt data but also start leaking and selling it, which creates a whole new dynamic."

- **Destructive attacks can render physical equipment inoperable.** These attacks render computers, servers, and other devices essentially inoperable. *"Malware can be used to prevent devices from connecting to a network,"* Mr. Henry told members. *"It could impact tens of thousands of computers. In that case, remediation is not just reconstituting or decrypting data—it is bringing in new physical infrastructure."* He noted that nation-states have launched destructive attacks of late: Russia employed such attacks against Ukraine, and Iran did so in targeting entities in the Middle East.
- **Misinformation and disinformation can cause reputational damage.** Misinformation and disinformation also pose risks for companies. Mr. Henry cautioned members about the damage that organizations can suffer from targeted misinformation and disinformation campaigns: *"There are foreign governments that are actively trying to cause unrest and division in the US. From a corporate perspective, it's a risk. We've seen organizations that have been falsely maligned."* Disinformation campaigns lean heavily on the use of bots, generative AI, and geofencing, among other tools.[7]

Responding to the growing risk of insider threats

"We experienced an insider attack," one member recounted. *"We believe our employee was paid by the group known as Lapsus, resulting in leaked client information and damaged customer relationships."* The member noted a need for better indicators to detect insider threats: *"The cost of taking certain actions like limiting access across the company or deploying tools seems prohibitive. If insider threats are becoming more prevalent, what indicators should we look for? How do we identify them?"*

Mr. Henry responded with the following guidance:

- **Screen for threats during hiring.** *"It starts with the vetting process. HR and legal teams should be involved. There are characteristics you can look for during the hiring process that could be indicative of potential issues."*
- **Build awareness across the company.** Educate management and employees about red flags. *"I send reminders to our employees a couple of times a year; there needs to be awareness,"* Mr. Henry said. Managers can be taught indicators to look for—for example, an employee who begins making rash statements or who comes into the office at strange times.
- **Consider external resources.** Some cybersecurity companies offer solutions specifically designed to address insider threat risks.

Effective oversight requires constant vigilance

The current threat landscape makes it increasingly difficult for audit committees and other governance bodies to oversee cyber risk. *"This year, I've dealt with every type of vulnerability mentioned,"* a member noted. *"One company I'm involved with faced a ransomware attack but chose not to pay the ransom. Another encountered cyber-hygiene issues as our team failed to deploy a critical patch, and it caused operational challenges. Another company was targeted by an organized crime group and had issues with vendors. As audit committee members, we really can't control a number of these issues, but there is a tremendous amount of pressure placed on boards to conduct oversight, and sometimes we are not successful."*

Despite the challenge, directors remain committed to enhancing oversight, and members were eager to discuss good practices. Mr. Henry shared several:

- **Prioritize tone at the top and culture.** Cybersecurity is a *"whole-of-company responsibility,"* Mr. Henry said, noting that *"every person is a potential entry point and must take cybersecurity seriously."* This mindset is especially important for encouraging good cyber hygiene, whether that extends to regular software updates, strong passwords, or the willingness to raise the alarm about any situation that seems out of the ordinary. As one member put it, *"You can never do too much."* Mr. Henry stressed that leadership sets the tone for a security-aware culture. He advised audit chairs to create an environment where the chief information security officer and cybersecurity team feel comfortable raising concerns, stressing the importance of taking cybersecurity seriously while being realistic in recognizing that incidents will happen.

- **Know the company's technology footprint and mitigation timing.** A clear understanding of a company's entire technology footprint is essential, especially in light of the increasing number of vulnerabilities. Mr. Henry advised audit chairs to ask their cybersecurity teams: *"What are the assets most in need of protection? When we find something that is vulnerable, how quickly can it be patched before it gets exploited?"*

- **Focus on building resilience.** *"No matter how good your team is, incidents will happen,"* Mr. Henry said. He advised members to ensure that their companies have a business continuity plan, to ask what it entails and verify that it has been tested, and to confirm that team members understand their roles.

- **Conduct tabletop exercises.** Tabletop exercises are helpful for building resilience. They can be held at the operational level (e.g., with the chief information security officer, general counsel, head of communications, and their teams), at the C-suite level, or with board involvement. They allow a company to identify key players, clarify roles, involve necessary external partners, and prepare for many of the questions that can arise during a cyber event. Mr. Henry highlighted the value of conducting these exercises while there is the *"benefit of time to make thoughtful decisions."* Several members noted their experiences with simulations. *"I can attest to the incredible value they can bring,"* one said. EY reported that in 2024, 47% of Fortune 100 companies disclosed conducting simulations, tabletop exercises, or readiness tests, up from 3% in 2018.[8]

- **Ensure processes are in place to determine materiality.** One member highlighted the difficulties that come with establishing materiality, especially with the US Securities and Exchange Commission's rule requiring disclosure of cybersecurity incidents within four business days of a materiality determination. *"When you get caught in a cyberattack, there's a strong tendency for management to avoid reporting,"* the member said. *"I see a lot of discussions where they're unsure if it's material, and that's a real issue audit committees face today."* Mr. Henry advised audit chairs to ensure that clear processes are in place to determine materiality: *"Well before any attack, sit down with your general counsel, outside counsel and determine which situations would clearly be material. Others are more case-specific and fall into a gray area."* Tabletop exercises can be invaluable for practicing materiality determination, he added.

- **View cybersecurity as an investment, not a cost.** *"People who make decisions solely on cost are short-sighted. Cost is an important consideration, but not the only one,"* Mr. Henry cautioned. He underscored that companies and boards should view cybersecurity as an investment *"in your people, in your intellectual property, in your company, and in the resilience and longevity of your organization."*

- **Use external advisors and third-party assessments.** EY reported that 87% of Fortune 100 companies disclosed using an external independent advisor on cybersecurity matters in 2024, and 10% of boards engaged with one.[9] These advisors can help guide leadership as they provide specialized expertise, unbiased assessments, and effective incident-response strategies.

Approaches to board oversight of cyber risk

Cyber-risk oversight is a priority for all boards, with most delegating the task to audit committees. According to EY's cybersecurity disclosures report, "81% of Fortune 100 companies now assign cybersecurity oversight to the audit committee, up from 61% in 2018."[9] Other approaches include assigning oversight to a risk or technology committee or to the full board.

One member noted the importance of coordination when multiple committees are involved. Another emphasized customization: *"It should be tailored to your business. There is no one-size-fits-all solution."* Another brought the question of dedicating one board seat to a technology expert or "digital director." While the SEC does not mandate disclosure of board members' cyber expertise, according to the EY report, 72% of companies seek it and 71% include cybersecurity in at least one director biography, a rise from 34% in 2018.

Reflection questions for audit committees

? What parts of your business are most vulnerable to cybersecurity disruptions?

? What information has management provided to help the board assess which critical business assets and partners, including third parties and suppliers, are most vulnerable to cyber-attacks?

? How is your company addressing the influence of generative AI on cybersecurity, both in terms of increased risk and potential benefit?

? Do cyber threats manifest as physical risks for your company, whether to people, equipment, or real property? How is this connection between information security and physical security addressed?

? How would you characterize your company's cybersecurity culture? Do you believe it is adequately prioritized, communicated, and understood across the company? How does your company ensure that employees practice good cyber hygiene?

About this document

The Regional Audit Committee Networks are 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 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, members of 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 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: Participants

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

Central Audit Committee Network

Jeff Boromisa, Wolverine Worldwide

Candy Duncan, Discover Financial Services and Teleflex

Sandy Helton, OptiNose

Frank Jaehnert, Nordson

Phoebe Wood, Invesco and Leggett & Platt

East Audit Committee Network

Bert Alfonso, Eastman Chemical Company

Karen Golz, Analog Devices

Simon Lorne, Teledyne Technologies

Leslie Seidman, Janus Henderson Group

Southeast Audit Committee Network

Bill Creekmuir, Flexsteel Industries

Juan Figuereo, Deckers Outdoor and Western Alliance Bancorp

Joe Householder, Advanced Micro Devices

Jim Hunt, Brown & Brown

Mercedes Johnson, Synopsys and Teradyne

Maria Pinelli, International Game Technology

Karin Teglia, Wintrust Financial

Darrell Thomas, British American Tobacco

Mary Winston, Acuity Brands

Carol Yancey, BlueLinx Holdings

Bryan Yokley, Rayonier Advanced Materials

Southwest Audit Committee Network

Marcela Donadio, Norfolk Southern and NOV

Barbara Duganier, CenterPoint Energy

Teri Fontenot, AMN Healthcare Services

Don Kendall, Talos Energy

Teresa Madden, Cooper Companies and Enbridge

Brenda Schroer, Antero Resources

Laura Wright, CMS Energy

West Audit Committee Network–North

Carol Hayles, eBay

Bala Iyer, Power Integrations

West Audit Committee Network–South

Jim Morris, Edison International

EY was represented by the following:

Ted Acosta, Head of the Office of Strategic Relationships
Kevin Brower, US-Central Region Audit Leader
Scott Hefner, Senior Global Client Service Partner
Jennifer Lee, Managing Director, Americas Center for Board Matters
Molly Tucker McCue, US East Audit Leader
Pat Niemann, Partner, Americas Center for Board Matters
Anthony Sgammato, Assurance Partner and Office Managing Partner Iselin, NJ

Tapestry Networks was represented by the following:

Kate Cady, Project and Event Manager
Jonathan Day, Chief Executive Officer
Kelly Gillen, Senior Associate
Ginevra Rollo, Associate
Todd Schwartz, Executive Director
Ashley Vannoy, Project and Event Manager
Jason Watkins, Managing Director

Appendix 2: Guest biography

Shawn Henry serves as chief security officer of global cybersecurity firm CrowdStrike. In his role, Mr. Henry has responsibility for all facets of digital and physical security and risk, including global security, information security, business resilience & continuity, insider threat, and crisis response. Mr. Henry previously held the position of president of services, leading a world-class team of security professionals on large-scale, global security efforts, aggressively and effectively investigating and mitigating targeted attacks on computer networks.

Prior to CrowdStrike, Mr. Henry had a 24-year career at the FBI, finishing as executive assistant director, where he oversaw half of the FBI's investigative operations, including all FBI criminal and cyber investigations worldwide, international operations, and the FBI's critical incident response to major investigations and disasters. During his 24-year career, he held a wide range of operational and leadership roles and oversaw major computer crime and cyber investigations spanning the globe. Mr. Henry led the establishment of the National Cyber Investigative Joint Task Force (NCIJTF), a multi-agency center led by the FBI, and forged partnerships domestically and internationally within governments and the private sector. He was an original member of, and key contributor to, the National Cyber Study Group, under the direction of the office of the director of national intelligence. This organization developed the Comprehensive National Cybersecurity Initiative (CNCI), the U.S. government's then-national strategy to mitigate threats and secure cyberspace. Early in his cyber career, Shawn served on the US delegation to the G8 as a member of the High-Tech Crimes Subgroup.

Mr. Henry serves on the faculty and is a board leadership fellow at the National Association of Corporate Directors (NACD) where he educates corporate boards and directors about complex cybersecurity issues. He currently serves on the board of directors of public companies CLEAR and ShoulderUp; on the non-profit BOD for the Global Cyber Alliance; as well as on the Advisory Board of the Hofstra DeMatteis School of Engineering, the ADL's Center for Technology and Society, and cybersecurity startup DoControl. He served previously on the cyber advisory board to the Governor of New York.

Mr. Henry earned a bachelor of business administration from Hofstra University and a master of science in criminal justice administration from Virginia Commonwealth University. He is a graduate of the Homeland Security Executive Leadership Program of the Naval Postgraduate School's Center for Homeland Defense and Security.

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. Italicized quotations reflect comments made in connection with the meeting by network members and other meeting participants.

[2] CrowdStrike, *2024 Global Threat Report* (Austin, TX: CrowdStrike, Inc., 2024).

[3] CrowdStrike, *2024 Global Threat Report,* 5, 37.

[4] CrowdStrike, *2024 Global Threat Report,* 53.

[5] Barton Edgerton and Pat Niemann, "Cyber Oversight Disclosures: What Companies Shared in 2024," EY, October 15, 2024.

[6] CrowdStrike, *2024 Global Threat Report.*

[7] Bart Lenaerts-Bergmans, "Disinformation Campaign," CrowdStrike, March 19, 2024.

[8] Edgerton and Niemann, "Cyber Oversight Disclosures: What Companies Shared in 2024."

[9] Edgerton and Niemann, "Cyber Oversight Disclosures: What Companies Shared in 2024."