tapestry NETWORKS

FSLN VIEWPOINTS

Responding to a heightened technology risk landscape

May 2025

Cybersecurity has been among the top risks facing financial institutions for many years. *"The first risk most boards worry about is cyber—because it's not a matter of if you're going to be attacked but when,"* observed an executive. Today, however, large financial institutions are grappling with a widening range of technology risks, including dependence on an expanding number of third-party providers and partners, rapid advances in technology that are challenging traditional risk management, and growing volume, speed, and sophistication of cyberattacks. At the same time, international regulators and customers continue to emphasize operational and technical resiliency. As managing technology risk becomes increasingly urgent and complex, financial institutions are prioritizing efforts to mitigate cyber risk and build resilience across their operations.

On March 4 in New York and April 10 in London, board directors and senior executives from leading financial institutions gathered to discuss cybersecurity and technology risk, exploring how the risk environment continues to evolve, the strategies firms are adopting to mitigate those risks and build more resilient institutions, and boards' shifting approaches to oversight.

For a list of participants, please see page 12.

This *ViewPoints*[1] highlights the following themes that emerged from the meetings and related conversations:

EY Building a better working world

Technology and cybersecurity remain among the top risks facing financial institutions

The latest global risk management survey from Ernst & Young LLP (EY) and the Institute of International Finance (IIF) identified the cybersecurity threat landscape as the foremost concern for chief risk officers (CROs) over the next three years, followed by other technology-related risks, including data availability and AI. In the words of the report, "CROs say their top priorities for enhancing operational resilience for the next three years involve cyber, data and technology risk."[2]

Over the past 20 years, the financial sector has experienced more than 20,000 cyberattacks, leading to $12 billion in losses.[3] The frequency and complexity of these attacks pose a risk to the global financial system. A single cyber incident can ripple across markets, disrupt payment systems, undermine trust, and potentially trigger widespread financial instability. An executive warned, *"A disruptive attack against the financial services sector would be devastating to the world economy, and I think it's an area we need to make sure we are clearly focused on."* Threats to financial stability could materialize from outside large systemically important institutions. An executive observed, *"Most large financial institutions have their data protected, so disruption is more likely to happen at a smaller bank. I am much more worried about a smaller bank being taken out and taking the rest of us all down with it, because if depositors don't know how much money they have, the panic will affect all of us."*

"A disruptive attack against the financial services sector would be devastating to the world economy, and I think it's an area we need to make sure we are clearly focused on."

— Executive

Fallout from recent technology disruptions underscores the risks financial institutions face, both financially and reputationally. Nine of the top banks and building societies operating in the UK experienced at least 803 hours (over 33 days) of unplanned technology and systems outages over the past two years.[4] These outages affected millions of customers and resulted in significant financial consequences, including £12.5 million in compensation payments by Barclays.[5] A flawed update in August 2024 from one of the world's largest cybersecurity companies, CrowdStrike, caused outages that led to estimated losses exceeding $5 billion.[6] According to the EY/IIF report, "The high-profile IT disruptions of summer 2024 illustrated just how important it is for resilience strategies to be embedded across all parts of the business."[7]

The cybersecurity threat landscape is growing ever more complex

The cybersecurity threat landscape continues to evolve as geopolitics reshape the threat from nation-states, AI and other advanced technologies enable bad actors, ransomware becomes even more profitable, and partner and provider ecosystems create new vulnerabilities.

Nation-states, including the US, remain a top concern as geopolitical tensions shift the threat landscape

"Nation-states are always a risk. China, North Korea, Russia, and Iran are working together in a collaborative way and sharing tactics. Their ability to impact a nation is substantial, complex, and existential to certain organizations. We've been fighting these nation-states for three decades. As they align it becomes more challenging," said an executive.

The shift in American politics is also causing consternation. Heavy dependence on large US-headquartered technology companies, including cloud providers, has been a concern for some time for firms in other markets. And the current political landscape has exacerbated anxieties. One director said, *"A state actor we haven't talked about yet is the US ... We have to consider the potential for Donald Trump to have access to Amazon or Microsoft and to use that as a source of political pressure. I don't think it's a fantasy; I think it's a very real concern."*

> *"A state actor we haven't talked about yet is the US ... We have to consider the potential for Donald Trump to have access to Amazon or Microsoft and to use that as a source of political pressure."*
>
> — Director

Gen AI is empowering a broader range of bad actors

AI is increasing the volume, speed, and sophistication of cyber activity. *"What's changed from last year to this year is the pace of technology. The bad guys are getting worse, and they're now [using] … Gen AI–enhanced attacks,"* noted an executive. This executive continued, *"[Generative AI] puts power into the hands of those previously not powerful by allowing nontechnical actors to create tools being used in identity attacks, better phishing emails, phishing voicemail. Generative AI has been a huge boon for adversaries."* Participants also worry about the success of deepfakes and the potential for their use for all sorts of harmful purposes, including fraud, theft, or to damage firms' reputations.

Quantum computing looms on the horizon

Quantum computing has not yet arrived in a meaningful way for financial institutions, but when it does, it has the potential to challenge traditional cyber risk management techniques. Quantum computers' ability to defeat encryption is a key concern: *"It will destroy all encryption systems,"* one participant predicted. Another agreed, noting that previously stolen encrypted data, which was once thought to be secure, could be accessible: *"There's a good chance they're going to decrypt it with quantum, and it will come back and be incredibly painful."* Another participant warned, *"When quantum becomes more accessible, that's when bad actors will also get access and become more dangerous."* Regulators' expectations of firms are developing in tandem with quantum computing. An EY executive reported, *"The expectation from regulators is that you understand where cryptography is [currently being] used to protect your data and [that you] understand the nature of the algorithms used. When quantum is ready, bad actors will be able to hack existing encrypted data. So, consider whether work is being done to protect against quantum decryption, and when is the right time to invest."*

> *"When quantum becomes more accessible, that's when bad actors will also get access and become more dangerous."*
>
> — Participant

Ultimately, several participants said that quantum's relatively limited availability, high cost, and narrow use cases meant it was unlikely to be a threat for years. But some also agreed that they had to ensure their institutions were taking appropriate steps to become *"quantum ready"* now.

Ransomware is an increasingly pernicious threat

"The first thing most clients have to worry about is ransomware—you have to plan for the worst," said an EY expert. Bad actors are becoming more technically sophisticated and increasingly savvy in identifying and taking advantage of vulnerabilities. *"They find everything: your insurance policy, your coverage tower, what your limits look like. And they leverage every bit of that,"* commented an executive. A director shared what this looked like in practice: *"They set the ransom price at our insurance limit, and we paid it. They were so 'kind' that as a parting gift, they gave us a list of all our vulnerabilities. They know what to say, what to do, and how to deal with our negotiators."* Midsize companies are particularly vulnerable: *"Large financial institutions are vulnerable but have large budgets. Midsize companies don't have budget or resources for cyberattacks. This middle group is getting targeted the most. And they pay the [ransom] because they don't have an option."*

> *"They set the ransom price at our insurance limit, and we paid it. They were so 'kind' that as a parting gift, they gave us a list of all our vulnerabilities. They know what to say, what to do, and how to deal with our negotiators."*
>
> — Director

Many firms are predisposed to pay ransom, but some authorities are contemplating prohibiting organizations from doing so. *"Last year a senior Biden administration official suggested making it illegal for companies to pay [ransom],"* one director said. *"I think that would be a great thing because it makes it very clear that US companies aren't just going to pay."* said another. The UK government is similarly exploring legislation that would forbid certain industries from making ransomware payments.[8] However, one participant challenged such policies, noting that without the ability to pay the ransoms, companies would have no means to get their data back from hackers: *"I would be totally horrified if any government made that action illegal."* Another participant added that if the UK government forbids firms from paying ransoms, and thus retrieving their stolen data, *"they do need to be ready and able to help when that day comes. But do they have the resources they need?"*

Third parties create a complex set of vulnerabilities

An EY expert observed, *"Financial services organizations are investing significant money in cyber. Unfortunately, some third parties aren't doing the same. And that's often where the attackers are focused."* Some senior financial services leaders feel that working with the major tech providers mitigates third-party risk since those providers have the financial resources required to invest in security. But a participant cautioned that the large-scale cloud providers limit financial institutions' influence over and visibility into their cyber practices: *"We've found that you can dictate security standards with smaller organizations, but it's more difficult with larger companies. And with larger providers there is systemic risk. How do we ensure the overall financial system is protected and risks are understood, if, as an individual firm, you can't get the answers from the larger providers? I'm a lot more in the dark about [a major technology provider] than I am about my smaller providers."*

"Financial services organizations are investing significant money in cyber. Unfortunately, some third parties aren't doing the same. And that's often where the attackers are focused."

— EY Expert

Insider risk remains among the hardest to combat

One participant stated, *"Insider risk is a huge threat. A disgruntled employee or someone compromised by an adversary is one of the most significant and most dangerous threats because of the difficulty in detection. The amount of time between initiation and boom is very quick."* The participant continued, *"The ability to identify and detect is critical. Risk can come from someone who is a gambler, abusive, et*

cetera—anything you can look at beyond the digital realm, since you're dealing with human beings. Having a team look at risks in both the physical world and the virtual world is crucial."

Managing technology risks requires adapting to the new risk environment

Participants stressed two aspects of managing technology risk: making an organization less vulnerable to disruptions and cyberattacks, and improving its ability to respond to adverse incidents.

Reduce organizational vulnerability

Approaches to minimizing an organization's exposure to technology risk are many and varied, but participants at the March and April meetings focused on reducing third-party vulnerability and segmenting organizational computer networks. Participants noted the following strategies for mitigating weaknesses in their organizations:

- **Optimize the number of third-party relationships.** Some financial institutions are reducing the number of vendors and partners with which they work to mitigate third-party risks. A director said, *"We are reducing the number of external third-party suppliers and concentrating ever more in those few large companies, but making sure that the large companies have their back ends buttoned up."* Another agreed on the benefits of rationalization: *"You used to have two vendors for anything critical. Fast-forward to now, and companies are basically starting to have just one vendor because it came back that it's not so easy to have multiple vendors, and it's not a cost advantage to have to pay two vendors."*

  Reducing the number of providers and partners too much can create different risks, however, including vulnerability through overreliance on a small number of key providers. Finding the right balance is critical. A director said, *"By limiting who we do business with, I think we overcomplicate life by having proprietary systems which cannot be efficiently maintained. So, I tend to support using off-the-shelf systems from really good companies that are continuing to invest and enhance their offerings."*

- **Establish protocols around automatic updates.** Staying up-to-date on software patches is a basic aspect of cyber hygiene, but implementing automatic updates from third-party vendors can represent a key source of risk. An executive observed, *"It's really*

"By limiting who we do business with, I think we overcomplicate life by having proprietary systems which cannot be efficiently maintained."

— Director

hard to manage third parties that bring their own updates into your environment, but it's also really important to do so." A recent disruption caused by a faulty automatic update led some to reconsider their approach: *"No good crisis should go to waste, so we looked at our process for accepting and implementing software updates. What's the rigor we put behind that? Are there additional steps we should be taking? We reviewed that process and then took the opportunity to do a deeper dive on vendor dependency overall."* An executive suggested inserting processes to delay automatic vendor updates: *"It is a matter of inserting a delay of your choice. For different types of updates, consider how critical do I think they are as a class and how long of a delay do I want to insert? Then if something breaks, it breaks at someone else's company first."*

- **Segment networks to limit the impact of attacks.** Network segmentation divides computer networks into smaller parts to control traffic moving through different areas.[9] A participant observed, *"Network segmentation is one of the best practices often neglected by organizations."* A director agreed: *"Network segmentation was a key takeaway from our tabletop exercise. Creating internal barriers within the network limits access and contains threats."*

Build organizational resilience

An organization's resilience—its ability to recover from a severe setback, such as a cyberattack—depends on having systems and processes in place before they are needed. *"Resiliency needs to be foundational in the organization. Everything you do from code development to deployment needs to be part of this resiliency methodology. Resiliency needs to be cultural, and it needs to be indoctrinated,"* stated a director. Recognizing the inevitability of cyberattacks and technology disruptions, participants identified several approaches to enhancing resilience:

> *"Resiliency needs to be cultural, and it needs to be indoctrinated."*
>
> — Director

- **Identify assets and prioritize key systems for recovery**. *"You can't protect what you don't know,"* observed one director. Another noted, *"A huge issue is whether a company has an asset inventory and whether people have access to that asset inventory. Then you have to prioritize those systems. If everything is down, what do you want to get back up first? When you're bailing water, it's usually the big ones that get attention."*

  One way to prioritize is to identify the essential services the

organization provides and ensure they can be restored quickly following an outage or cyberattack. A key question, one director said, is *"What is the minimum viable service we have to provide? Whatever those minimum services are, [they] have to sit on another cloud than that of the main bank."* A regulator agreed: *"Minimum viable service is a very important point. There's a clear example of a bank that identified its core service as enabling payments and displaying balances. They have a live, alternative cloud-based solution to support their core service. That idea is well worth thinking about."*

- **Run detailed tabletop exercises frequently and conduct real tests.** Participants see value in tabletop exercises that enable management and the board to prepare for possible scenarios. One participant advocated doing them as frequently as once a month. A regulator encouraged participants to make these exercises as robust and lifelike as possible: *"Tabletops tend to be based on one type of event scenario, but there's a high likelihood there will probably be multiple things occurring at once. Build scenarios that include multiple things. For example, if small banks have something happen, who might want to take advantage of the chaos? How would you put those together and respond?"*

  Part of an effective scenario exercise is understanding and improving the speed of recovery. *"Something we all need to think about is uncovering the elapsed time to do a full-stack recovery,"* one director opined. *"You have got to not only practice it through tabletop exercises, but you've got to actually do it to know what the levers for reduction in cycle time can be."*

- **Implement alternative forms of internal communication.** An executive said, *"Out-of-band communications are so important. If an adversary attacks you, you can't communicate where they can see or have access."* A director echoed this sentiment: *"Technical staff need to have alternate means of communication. If email systems go down and technical teams are unable to communicate or collaborate to resolve the issue, it can significantly hinder response efforts."*

- **Develop an external communication strategy in advance.** Communicating with transparency and clarity is paramount during an incident. An executive reflected on their own experience in the face of a significant disruption: *"Open communication helped us*

"Out-of-band communications are so important. If an adversary attacks you, you can't communicate where they can see or have access."

— Executive

restore trust. We weren't standing behind lawyers. Having trust and customer confidence was so important."

The organization's legal counsel, business team, and law enforcement will often have differing objectives during a crisis. Communicating with law enforcement requires a deliberate approach. A director stated, *"Companies must determine their objectives when communicating with the government, whether for operational or compliance reasons. The government's goal is to identify and arrest bad actors, not to remediate systems ... Each situation is unique, so it's crucial to consult with outside counsel and make informed decisions internally. It's not a one-size-fits-all approach."*

Technology risk oversight is maturing

Technology risks present evolving oversight challenges for financial institutions, so boards must continue to adapt their governance approaches.

Defining technology risk appetite more clearly

Financial institutions and their boards must accept a certain degree of technology risk, but it should be aligned with the institution's overall risk appetite. An EY executive noted, *"Before risk acceptance, there's risk appetite. You can see examples of boards following a perfect process to set risk appetite, yet the organization has been outside of appetite for long periods of time. Big banks in the UK have had 30-plus days of outages, but the appetite for outages is always zero, so risk appetite is clearly not being met."* Boards must also understand that risk acceptance does not represent fulfillment of duty; additional action steps are required. A director said, *"Risk acceptance is not risk abdication. Risk acceptance just means you have a risk you don't know how to stop, but that means you need a plan and to know what your response will be."*

> *"Before risk acceptance, there's risk appetite. You can see examples of boards following a perfect process to set risk appetite, yet the organization has been outside of appetite for long periods of time."*
>
> — EY Executive

Rethinking committee oversight of technology risk

Without dedicated technology committees, already overloaded risk and audit committees often take on responsibility for tech risk oversight. A participant commented, *"We're in an industry where risk committees are so full already, and there isn't sufficient capacity or a fair burden for*

those committees to take on oversight responsibility for something like this." In response, some boards have decided to establish a dedicated tech committee. One director said, *"The tech committee is able to dive deep … It's a fork-in-the-road decision whether to create a tech committee. It's a pain, it's inconvenient, but it's an important decision."*

Some participants expressed concern that compartmentalizing risk across so many committees could mean that the full board misses something at the enterprise level, or that it could overly defer to specialized committees. A director asked, *"Is the board really understanding the conflation of the risks? I'm not sure we are spending enough time understanding these are conflated, when they start piggybacking."* Another director stated, *"There is not one solution that is perfect, but we make sure every board member is on either the audit or risk committee. We also have some overlap of tech and risk for when something needs both breadth and depth.*"

"We're in an industry where risk committees are so full already, and there isn't sufficient capacity or a fair burden for those committees to take on oversight responsibility for something like this."

— Participant

Recognizing the limitations of third-party assessments

Third-party assessments of an organization's cybersecurity and tech environment can provide useful insights, but participants expressed concerns that boards may not get a full picture from those reports. One participant suggested the board or executive management team should be responsible for hiring the assessor to ensure appropriate reporting and accountability: *"If it's the [chief information officer] or the [chief information security officer], the board will not get what it wants in the report. So, the client has to be the board or someone higher up in management."* Another participant emphasized the importance of thorough validation: *"We have learned to have some healthy skepticism and ask a lot more challenging questions. When it comes to cybersecurity maturity assessments, you really have to drill down. How deep did they go? Did they actually validate or just ask management questions?"*

Working with management to improve reporting

The quantity of information boards receive can make it difficult for directors to focus on the most important issues. A director said, *"As a board member, I often hear that the information was in the packet, but I have to read* War and Peace *to get to the information."* This director noted that excessive information can allow management to avoid taking responsibility for identifying key issues. *"I want them to tell me, 'These*

"As board members, we don't run the business. We need executives to take ownership."

— Director

are the five things I am worried about, and this is how I am working on it.' As board members, we don't run the business. We need executives to take ownership." But another director suggested the board must proactively inform management of the level of depth and detail it's looking for: *"I really do think it's one of the board's jobs to make sure it has appropriate information in the right degree of granularity to oversee the company and challenge executives. If you're getting* War and Peace, *then it's up to the board to make that right. Getting that balance right is really important."*

Questions boards should ask about tech risk

- **What are your institution's critical business services? What constitutes your organization's "minimum viable business," and how quickly can you get that up and running in a crisis?**
- **How much do you spend on cyber relative to the IT budget, and how does that compare to your peers? If you received significantly more budget, what would you spend it on, and what business risk would you be reducing?**
- **What sources of potential disruption could most significantly impact operations, and how are you preparing for them?**
- **How are you ensuring you have the right mix of cybersecurity expertise across leadership, operations, and technical teams? How does your current staffing level compare to industry standards and peer organizations?**
- **What guidance on cybersecurity regulation are you currently receiving from regulatory authorities?**

Meeting Participants

The following individuals participated in the meetings or related conversations:

Participants

Homaira Akbari, Non-Executive Director, Santander

Giles Andrews, Transformation Oversight Committee Chair, Bank of Ireland

Nora Aufreiter, Human Capital and Compensation Committee Chair, Scotiabank

Sarah Beshar, Non-Executive Director, Invesco

Paul Bishop, Audit Committee Chair, AXA XL and Zurich Assurance, Chair of the Board MetLife UK

Craig Broderick, Risk Review Committee Chair, BMO Financial Group

Agnes Bundy Scanlan, Nominating and Governance Committee Chair, Truist Financial

Kathy Byrne, Non-Executive Director, Just Group

Marta Chaffee, Senior Associate Director, Supervision and Regulation, Federal Reserve Board

Andrew Chisholm, Risk Committee Chair, RBC

Michael Cole-Fontayn, Non-Executive Director, JPMorgan Securities

Alec Cramsie, Head of London Market Wholesale Cyber & Technology, Beazley

Martha Cummings, Nominating and Corporate Governance Committee Chair, Marqeta

Andrew Dapre, Former Global Partnerships, Microsoft Cloud for Financial Services

Andrew DeBerry, Chief Operating Officer, Costa Security

Pierre-Olivier Desaulle, Senior Independent Director, Beazley

Andrea Doss, Senior Vice President and Chief Risk Officer, State Farm

Beth Dugan, Deputy Comptroller for Large Bank Supervision, Office of the Comptroller of the Currency

Terri Duhon, Risk Committee Chair, Morgan Stanley International

Harriet Edelman, Independent Director, Technology Committee Chair, Assurant

Alessia Falsarone, Non-Executive Director, Assicurazioni Generali

Karen Fawcett, Non-Executive Director, Aegon

Tim Gallagher, Large Risk Underwriter - Cyber & Technology, Beazley

Karen Gavan, Audit Committee Chair, Swiss Re

Jill Goodman, Non-Executive Director, Genworth Financial

Heather Gottehrer, Senior Vice President, Cyber Security Assurance, Bank of America

Tobias Guldimann, Risk Committee Chair, Edmond de Rothschild

Ashok Gupta, Risk Committee Chair, Sun Life Financial

Margarete Haase, Audit Committee Chair, ING

Shawn Henry, Chief Security Officer, CrowdStrike

Sheila Hooda, Nominating & Governance Chair, Enact Holdings and AGL Private Credit Income Fund; Non-Executive Director, Alera Group

Mark Hughes, Risk Committee Chair, UBS

Joe Hurd, Non-Executive Director, Lloyd's of London

Arlene Isaacs- Lowe, Non-Executive Director, Equitable Holdings

Jim Islam, Chief Executive Officer, OneFamily

Giedrimas Jeglinskas, Chair of the Committee on National Security and Defence, Lithuanian Parliament

Shonaid Jemmett-Page, Senior Independent Director, ClearBank, Customer and Sustainability Committee Chair, Aviva

Kevin Kajiwara, Co-President, Political Risk Advisory, Teneo

Malik Karim, Founder and Chief Executive Officer, Fenchurch Advisory Partners

Phil Kenworthy, Non-Executive Director, ClearBank

Joan Lamm-Tennant, Chair of the Board, Equitable Holdings and AllianceBernstein

Rob Lelieveld, Audit Committee Chair, NN Group

Stuart Lewis, Risk Committee Chair, NatWest

John Lister, Actuarial Committee and Risk Committee Chair, Old Mutual; Risk Committee Chair, Phoenix Life

Duncan Mackinnon, Executive Director for Supervisory Risk Specialists, Prudential Regulation Authority

John Maltby, Audit Committee Chair, Nordea

Trevor Manuel, Chair of the Board and Corporate Governance and Nominations Committee Chair, Old Mutual

Liz Mitchell, Non-Executive Director, Principal Financial

Tom Murphy, Senior Managing Director, Fenchurch Advisory Partners

Diane Nordin, Audit Committee Chair, Principal Financial; Compensation and Human Capital Committee Chair, Fannie Mae

Ed Ocampo, Risk Committee Chair, JPMorgan Securities

Lewis O'Donald, Non-Executive Director, HSBC

Andy Ozment, Executive Vice President, Chief Technology Risk Officer, Capital One

Doina Palici-Chehab, Non-Executive Director of several AXA Entities

Jane Pearce, Non-Executive Director, Morgan Stanley International

Marvin Pestcoe, Underwriting and Risk Committee Chair, Hamilton Insurance Group

Lisa Pollina, Non-Executive Director, Munich Re America

Bruce Richards, Non-Executive Director, RBC Bank

James Rosenthal, Chief Executive Officer and Co-Founder, BlueVoyant

Gavin Smyth, Chief Risk Officer, Nationwide Building Society

Scott Stoll, Audit Committee Chair, Farmers Group and Farmers New World Life Insurance Company

John Sutherland, Observer to the Audit Committee, European Investment Bank

Patrick Tannock, Non-Executive Director, Fidelity International

Nick Turner, Group Chief Executive, NFU Mutual

Grace Vandecruze, Audit Committee Chair, PIMCO

Betsy Ward, Non-Executive Director, Hanover Insurance Group

David Wildermuth, Managing Director and President, UBS Americas Holdings

Al Zollar, Technology Committee Chair, BNY

EY

Omar Ali, Global Financial Services Leader; EMEIA Financial Services Regional Managing Partner

Cindy Doe, EY Americas Consulting Risk Leader, EY

Stuart Doyle, EY Risk Principal, EY

Jeff Gill, Americas Insurance Leader

Adam Girling, EY Americas Banking and Capital Markets Deputy Leader, EY

Steve Holt, Partner, EY

Jun Li, Global and Americas Wealth and Asset Management Leader, EY

Nigel Moden, EY Global Banking and Capital Markets Leader; EY EMEIA Banking and Capital Markets Leader, EY

Bridget Neill, Americas Deputy Vice Chair – Public Policy, EY

Isabelle Santenac, Global Insurance Leader

Phil Vermeulen, EMEIA Financial Services Insurance Leader

Tapestry Networks

Dennis Andrade, Managing Director

Eric Baldwin, Executive Director

Tiffany Luehrs, Senior Associate

Brenna McNeill, Senior Associate

Tucker Nielsen, Managing Director

About this document

The Financial Services Leadership Network (FSLN) is a group of financial services board members, executives, stakeholders, and other subject matter experts committed to addressing pressing problems 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.

About Tapestry Networks

Since 2004, Tapestry has been the premier firm for building collaboration platforms with leaders of the world's foremost organizations. Tapestry Networks brings senior leaders together to learn and to shape solutions to today's most pressing challenges. We are a trusted convener of board directors, executives, policymakers, and other stakeholders, connecting them with information, insight, and each other. Top experts join our discussions to learn from the leaders we convene and to share their knowledge. Our platforms help educate the market, identify good practices, and develop shared solutions. We call this the power of connected thinking.

About EY

EY is a global leader in assurance, tax, transaction, and advisory services to the financial services industry. The insights and quality services it delivers help build trust and confidence in the capital markets and in economies the world over. EY develops outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, EY plays a critical role in building a better working world for its people, for its clients, and for its communities. EY supports the networks as part of its continuing commitment to board effectiveness and good governance in the financial services sector.

Endnotes

[1] *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 from conversations with participants in connection with the meeting.

[2] Ernst & Young LLP and the Institute of International Finance, *Agility in Volatility: Rebalancing CRO Priorities in a Shifting Risk Matrix* (EYGM, 2025), 23.

[3] Spencer Feingold and Johnny Wood, "Global Financial Stability at Risk Due to Cyber Threats, IMF Warns. Here's What to Know," World Economic Forum, May 15, 2024.

[4] "More Than One Month's Worth of IT Failures at Major Banks and Building Societies in the Last Two Years," UK Parliament, March 6, 2025.

[5] Graham Fraser, "Barclays to Pay Customers Millions as Banks See Month's Worth of IT Outages," BBC, March 6, 2025.

[6] Raphael Yahalom, "What the 2024 CrowdStrike Glitch Can Teach Us About Cyber Risk," *Harvard Business Review,* January 10, 2025.

[7] Ernst & Young LLP and the Institute of International Finance, *Agility in Volatility: Rebalancing CRO Priorities in a Shifting Risk Matrix,* 23.

[8] John Timmons and Joe Devine, "Ransomware Payments: New Legislative Proposals in the UK," White & Case, February 4, 2025.

[9] "What Is Network Segmentation?" Cisco. Accessed May 13, 2025.