Cyber risk management: the focus shifts to governance

Bank Governance Leadership Network

April 2017

Tapestry Networks

EY

Building a better working world

Bank Governance Leadership Network
ViewPoints

April 2017 TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM · +1 781 290 2270

Cyber risk management: the focus shifts to governance

> *"The adversaries relevant to your firm come and go, but somebody is always trying to hurt you. They range from hacktivists to organized crime to nation-states playing a long game. This is a dynamic, asymmetric risk."*
>
> – Participant

Cyber risk has attracted a great deal of attention in recent years, and banks have made substantial investments in cybersecurity. Despite this, cyber risk and data security are still the top operational risk concerns in 2017, according to a recent survey of risk professionals.[1] *"The cyber threat is increasing by the day. All you have to do is pick up a paper and you see the impact. It is a moving target that can only get worse,"* said one director. Indeed, media headlines are dominated by state actors hacking elections and nefarious groups attacking a wide range of companies, with banks among the most targeted.[2] Customers, investors, and regulators all want assurances that boards understand the risks and are doing the utmost to ensure banks are managing them.

Over several months, culminating with meetings on February 23 in New York and March 16 in London, Bank Governance Leadership Network (BGLN) participants shared perspectives on the practical challenges that boards and risk management teams face in the oversight of cybersecurity. This *ViewPoints*[3] synthesizes the perspectives and ideas raised in the meetings, as well as in nearly 30 conversations beforehand with directors, executives, supervisors, and banking professionals. A list of individuals who participated in discussions can be found in Appendix 1. A companion *ViewPoints* entitled Banking in transition: overseeing non-financial risk in the midst of technological and business model transformation captures content relating to other non-financial risks and managing the transformation agenda. Themes, insights, and observations from those discussions are summarized in the following sections:

- **Cyber vulnerability presents unique challenges for risk management and oversight**
- **Regulatory authorities are becoming more prescriptive in defining cyber risk expectations**

Cyber vulnerability presents unique challenges for risk management and oversight

Cybersecurity continues to be a particular challenge for board risk oversight, due to the dynamic nature of the risk and the increasing vulnerabilities created by digital banking. A participant observed, *"All big financial institutions feel the vulnerability and are devoting serious resources. We are plugged into different national and international agencies. I get the sense we are doing as well as we can."* But how do boards know whether they are

doing enough? An executive warned, *"Your patience will be exhausted before cyber risk is effectively managed … We are not yet on top of it."*

"Your patience will be exhausted before cyber risk is effectively managed."

– Executive

Setting tolerances

Leaders of financial institutions generally acknowledge that it is impossible to make an organization 100% invulnerable to cyber breaches. Many are now trying to determine their risk appetite, or tolerance, for various aspects of cyber risk. This task is challenging. One director acknowledged, *"We are in breach of our risk appetite given the state of our information security. [Our] ability to deal with threats that continually adjust is unclear. We have done some things, but we are in breach, and we know it."* Some directors questioned how they can ensure that appropriate steps are being taken to address cyber risk. One conceded, *"There is nothing else you can do except say you are looking into remediation projects."* The particular challenge in setting a tolerance for cyber risk, according to one participant, is that *"cyber is an asymmetric risk. The bad guys only need to be successful once. You have to be perfect all the time."* Furthermore, as one participant observed, *"Certain types of threats you cannot mitigate against. If a nation-state uses previously unknown tactics specifically against you, you have to accept it."* This challenge only highlights how important it is for boards and executive management teams to understand the scope of the risks they are facing, the specific steps they should take to mitigate them, and how the risk and mitigation efforts align with their risk appetite.

"The bad guys only need to be successful once. You have to be perfect all the time."

– Participant

Understanding the investment needed

"If you recognize there will be cyber attacks, that your tolerance can never be zero, then the question is how much are you willing to spend? The investment is massive," said one participant. Another shared some historical context: *"If you go back five years, a lot of large banks acquired major capabilities in cybersecurity. They spent a lot of money. Yet, there are still a lot of data breaches. Why? The capabilities were not mature, and they were implemented in silos. A lot of the interconnectivity is where we see weaknesses. It created new avenues for attackers."* The result of this continued vulnerability is that many boards have the impression that their chief information security officer (CISO) is *"always telling us that cyber is a disaster and we need all this money,"* reported one participant. An executive acknowledged, *"As risk professionals, we have to give the board a better way to measure progress, or they will lose patience,"* but added, *"At the moment, we do need a surge in investment, and that CISO who keeps asking for more money really does need it."* Increasingly, many large banks are investing heavily in tools like automated correlation engines, which collect and digest large amounts of data from many different sources to predict, identify, and respond to cyber attacks.[4]

"… That CISO who keeps asking for more money really does need it."

– Executive

Although directors expressed frustration at their inability to measure the effectiveness of cyber expenditures, one director cautioned against an excessive focus on precise measurement, saying, *"We need to keep in mind the overall purpose of the exercise, rather than get caught up in 'Can I attach X dollar amount to managing it better?'"*

Identifying threats and addressing vulnerabilities

Keeping up with the constantly evolving cyber threat remains a formidable challenge. Directors do not need to become experts in cybersecurity, but they do need to understand the risk to their firms and the appropriate responses. Experts distinguish threats originating with vandals or hacktivists looking to cause disruption; criminals seeking money, often through ransomware; spies seeking intellectual property; saboteurs looking to cause real damage; and slackers – employees who are simply lazy and do not follow security protocols. A participant noted, *"Each attacker's motivation leads you down different defensive paths."*

Adding to the complexity, a participant noted, *"Cyber attacks are not binary in their success. It takes a long time to be successful."* Because eventual breaches are inevitable, managing cyber risk is not just about protecting the perimeter but also about *"how you defend, respond, and recover. It is the full cycle."* That involves reviewing practices like how system backups are structured and where backup data is stored. A participant noted, *"Most networks were built to encourage cross selling and easy navigation, so it is easy to get in."* This means that firms have to consider ways to *"box in the risk"* – for example, by *"changing the economics so it is more expensive for the attacker to be successful"* once inside. They might also use fake servers as decoys, or think about how firewalls are used between servers. A participant warned, *"Attackers are smart; they watch the process. They might even attack the backup first."* Participants were also concerned about where and how data is being stored. A director said, *"As we encourage more innovation, more people are putting data in places the [chief information officer] doesn't even know."* As more banks move data to the cloud, directors should consider whether the cloud is private or public and what jurisdiction the cloud is in.

> *"As we encourage more innovation, more people are putting data in places the [chief information officer] doesn't even know."*
>
> – Director

Perhaps more worrying than individual bank vulnerabilities are threats to the system. A participant observed, *"We haven't seen many major cyber attacks yet because terrorists haven't really moved to cyber. Nation-states have, but it is easier to deter nation-states. Terrorists' goal is to induce terror. You can induce disruption, but it is hard to induce terror through cyber attacks. But it is only a matter of time."* The market for advanced cyber tools is growing, and some organizations are advertising sophisticated hacking tools available to the highest bidder. The same participant observed, *"It is not a lack of tools or ability. It is a lack of motivation and sophistication."* One participant warned that criminals are *"becoming more interested in attacking the Internet infrastructure itself."*

Improving governance and oversight

Firms have adopted different approaches for handling oversight of cyber risk. Some are sharing primary board responsibility among technology and risk committees. Others have established special subcommittees focused specifically on cyber. Most have a single accountable officer responsible for cyber resilience, often a CISO. The reporting structure for this officer, however, remains a source of disagreement. *"Some say the CISO should report to the chief risk officer. I'm thinking, what are you doing? The risk exists because of IT. If it were me, I would want to be sure cyber remained a responsibility with reporting to the CIO,"* argued one director.

Participants highlighted the following ways in which boards can make meaningful contributions to good governance:

- **Encouraging an organization-wide culture of cyber-awareness.** A recent article in *The Economist* describes why improving cybersecurity can pose a cultural challenge: "It is tempting to believe that the security problem can be solved with yet more technical wizardry and a call for heightened vigilance … That requires a kind of cultivated paranoia which does not come naturally to non-tech firms."[5] This is particularly critical as recent data suggests that employee negligence or malicious acts account for nearly two-thirds of cyber breaches.[6] A participant asked, *"How can you create resilience in the DNA of the culture so that everybody knows the consequences of their actions? Eventually people have to think about cyber as a fundamental skill set. Not that they need to be an expert, but that they need to have situational awareness."* Another said, *"Security is always a trade-off … The goal is to change the mind-set from one focused on not making any mistakes to instead thinking about turning all of your employees into sensors. You don't need 100% of employees to avoid clicking on a phishing link; you just need one person to report it."* Another focused on controls and broadening risk management responsibility: *"One of the challenges is the translation of these risks to an effective control strategy. The drive is toward giving responsibilities across the three lines of defense. That was not previously the case."*

> *"You don't need 100% of employees to avoid clicking on a phishing link; you just need one person to report it."*
>
> – Participant

- **Increasing access to cyber expertise.** Most boards are experimenting with new governance structures, such as special committees, and bringing cybersecurity advisers into those committees or adding an advisory committee, and considering how best to divide oversight responsibility among committees and the full board. Other boards are adding directors with cyber expertise. One director commented, *"We have a cyber expert who has no financial institutions experience, so there is a back and forth on understanding how the business works. The value is the ability to interface with the CISO. They speak the same language and can convey that to the board."* Directors cautioned against too much reliance on specialists on the board, however. One asserted, *"You can't have a board member to understand every technological development. It is more about having access to experts."*

- **Ensuring accountability and prioritization at senior executive level.** One participant advised, *"Keep the pressure on. I know there is a CISO at every bank. Everybody thinks they are paying attention to cyber, but where the rubber meets the road, they often fail the test, especially if cybersecurity conflicts with a business priority."* Another participant noted, *"One of the hardest groups to manage are top executives. Are there exceptions for them on security? If so, push on whether they are needed … The CEO doesn't need superuser access."*

- **Developing robust response and recovery plans.** Participants agreed that banks should focus on reducing the impact of inevitable cyber incidents, by developing appropriate response plans and using scenarios to prepare. A director elaborated: *"Often, we at the board hear about what might have happened in terms of a cyber*

breach, and you go into your 'what happened?!' moment. But it might be six months before you really know what happened and how and why. Spending resources is really about reducing that period." Scenario planning and "war-gaming" can help, though the specifics will rarely align with real events. Part of the priority for a board is to understand their role in an incident. For example, how long should the board wait before alerting the public of a significant breach or loss of data? One asked, *"Assume there is a significant breach, maybe a ransomware attack. Do you pay the ransom, and when do you tell the customer?"* Another complained of mixed messages: *"You have regulators saying, 'Tell the customers,' and police saying, 'Don't say anything.'"* A regulator clarified, *"Feedback to the outside world is complex, and people will make assumptions. Banks are different. It is all about trust and safety. We err on the side of safety. If we say something and it turns out to be untrue, we lose the confidence of the wider system. We think about our role in the response. We do think we have to work together."*

"If we say something and it turns out to be untrue, we lose the confidence of the wider system."

– Regulator

Regulatory authorities are becoming more prescriptive in defining cyber risk expectations

Some analysis suggests that the financial sector outpaces other sectors in cybersecurity preparedness, owing to dramatically increased investments in defensive measures.[7] Nevertheless, many policymakers are concerned that the sector is not going far enough. Sarah Bloom Raskin, former US Treasury Deputy Secretary, noted that while the financial services industry may be ahead of other sectors, it still has a long way to go, and said that "there are well-documented best practices out there" that have not been universally adopted.[8] Certainly there is no shortage of frameworks and guidelines: a recent report suggested that regulators at the various levels, along with industry bodies, have "issued or proposed 43 differing cybersecurity frameworks, questionnaires, rules, and requirements applicable to the financial services sector."[9] Apart from regulatory guidance, many firms are already implementing norms, such as the National Institute of Standards and Technology (NIST) framework.[10] A supervisor reported that banks still have to improve to meet the NIST standards: *"We have done exam work relative to the NIST framework. We have not seen any systemic firm where we saw something that we really liked. The average bank is not where we would like it to be. They are struggling on some foundational issues."*

New cyber regulations in the United States shift the focus to governance and controls

In the United States, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Federal Reserve have jointly proposed enhanced cyber risk management standards for financial institutions in the form of an advance notice of proposed rulemaking (ANPR). According to an EY briefing report, the proposed rules require the development of a board-approved cyber risk management strategy, as well as a board-approved cyber risk appetite. In addition, firms will be obliged to take an inventory of all business assets and their criticality, along with the ability to monitor in real-time all external dependencies.[11] Some directors criticized the ANPR as further

reaching and more prescriptive than prior guidance from regulators, but one participant noted that as the first step in a multi-phase consultative process, the initial proposal was deliberately designed to be very broad in order to garner feedback, whereas the final rules were likely to be more limited. Most directors agreed that the proposed standards do not create new or vastly expanded expectations beyond what boards are already doing so much as clarify specific responsibilities. The standards do demonstrate a new focus for regulators: a participant noted, *"Previously, cyber regulation was all about prevention. This is about governance models."*

"Previously, cyber regulation was all about prevention. This is about governance models."

– Participant

A participant went into more detail: *"In the ANPR, there are descriptions about the three lines of defense and the second line getting access to the board. It is all about getting the first and second line working together. Then you have internal audit validating that the cyber risk framework is complying with the regulations … ANPR is clear on the board keeping management on top of it … A lot of it is quite reasonable, but it is the scope that is the issue. They are really pushing you to understand the supply chain, for example."* Another summarized, *"The ANPR is setting clear lines to push cyber throughout the organization. For example, if you make an acquisition, how are you thinking about its cyber risk implications? They want to make sure cyber risk is managed, not accepted. It is about enlightening people to think about cyber from an end-to-end perspective."*

The ANPR is a by-product of discussions among G7 regulators and policymakers. As a result, it is likely other national regulators will follow with similar requirements – perhaps not as prescriptive, but based on a similar set of agreed principles.

Data regulations are coming in Europe

In Europe, the new European General Data Protection Regulation will come into force in May of 2018. A participant commented, *"This is the really scary one because of the fines. It is all about protecting EU citizens' data. If you operate in the EU, you need the right processes in place. Depending on the type of breach, it could cost you up to 4% of your annual revenue."* Participants were warned not to underestimate the significance of these requirements: *"At most companies, legal is pushing the response. But the strategic challenges are so broad. If you don't go about it the right way, you could be in trouble … It will affect everyone,"* warned one participant.

"… You need to constantly be state-of-the-art, and the state of the art is constantly changing."

– Director

Directors accept heightened expectations, but encourage regulators to avoid duplication

Some participants submitted that regulators have no choice but to load accountability onto banks and their boards. One director remarked, *"I don't think the regulators know enough about the technical aspects of the issue. I think they hide behind the rigors of regulatory structure to call for monitoring, governance, and accountability as opposed to focusing on the nuts and bolts. But I do think it is right to force financial institutions to have this discussion themselves."* Another said, *"We all know the regulatory expectations are vastly up, even before these new rules are finalized. The general expectation is that you need to constantly be state-of-the-art, and the state of the art is constantly changing … We are told a whole new generation of things need to happen."*

Despite this general acceptance, participants advised regulators to focus on efforts that can make a positive impact and raise standards. One director cautioned, *"Most of us use NIST as a starting point. If the guidance moves away from that, then they would need to be clear on why they are doing so. There are like 65 regulators around the world coming out with guidance on this. It is a pretty complicated tapestry."*

***

A subject matter expert predicts that cybersecurity is becoming the "master problem" of the era – an existential challenge similar to climate change in its significance and consequence, which will require massive resource commitments in the next few years.[12] In the past, cybersecurity was often viewed as a technical problem to be addressed primarily by technology, rather than as a strategic threat to be addressed by the board. Those days are over. As technology is increasingly embedded in all aspects of banking, cyber risk is expanding, requiring more and more board attention. A participant outlined the significance of cybersecurity and related issues for bank leaders: *"Can the chairman or CEO stand up to investors and say, 'We are not going to focus on protecting against this risk or that,' or that they decided to slow down customer innovation because it is increasing the cyber risk profile? Or take a stance on data collection? Do our boards take real business ownership of the deep implications of cyber risk? Or are we just, as one participant suggested, being 'updated at' by the technology community? It impacts really big strategic choices."*

"Do our boards take real business ownership of the deep implications of cyber risk? … It impacts really big strategic choices."

– Participant

About the Bank Governance Leadership Network (BGLN)

The BGLN addresses key issues facing complex global banks. Its primary focus is the non-executive director, but it also engages members of senior management, regulators, and other key stakeholders committed to outstanding governance and supervision in support of building strong, enduring, and trustworthy banking institutions. The BGLN is organized and led by Tapestry Networks, with the support of EY. *ViewPoints* is produced by Tapestry Networks and aims to capture the essence of the BGLN discussion and associated research. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of senior management, advisers, and stakeholders who become engaged in this leading-edge dialogue, the more value will be created for all.

About Tapestry Networks

Tapestry Networks is a privately held professional services firm. Its mission is to advance society's ability to govern and lead across the borders of sector, geography, and constituency. To do this, Tapestry forms multistakeholder collaborations that embrace the public and private sector, as well as civil society. The participants in these initiatives are leaders drawn from key stakeholder organizations who realize the status quo is neither desirable nor sustainable, and are seeking a goal that transcends their own interests and benefits everyone. Tapestry has used this approach to address critical and complex challenges in corporate governance, financial services, and healthcare.

About EY

EY is a global leader in assurance, tax, transaction, and advisory services to the banking 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 BGLN as part of its continuing commitment to board effectiveness and good governance in the financial services sector.

Appendix: discussion participants

In February and March of this year, Tapestry and EY hosted two BGLN meetings on the challenges in overseeing non-financial risk in a period of rapid technological, business model, and operating model change, and had over 50 conversations with directors, executives, regulators, supervisors, and other thought leaders. Insights from these discussions informed this *ViewPoints* and unattributed quotes from these discussions appear throughout.

The following individuals participated in BGLN discussions on the changing nature of non-financial risk:

Bank directors and executives

- Clare Beale, Global Head of Independent Model Review, HSBC
- Bill Bennett, Risk Committee Chair, TD Bank
- Win Bischoff, Chairman, JP Morgan Securities
- Lord Norman Blackwell, Chairman of the Board and Nomination & Governance Committee Chair, Lloyds Banking Group
- Jonathan Bloomer, Non-Executive Director, Morgan Stanley International
- Chantal Bray, Global Head of Pension Risk, HSBC
- Juan Colombás, Executive Director and Chief Risk Officer, Lloyds Banking Group
- David Conner, Risk Committee Chair, Standard Chartered
- Sir Sandy Crombie, Senior Independent Director and Performance and Remuneration Committee Chair, RBS
- Sir Howard Davies, Chair of the Board and Nominations and Governance Committee Chair, RBS
- Nick Donofrio, Non-Executive Director, BNY Mellon
- Noreen Doyle, Vice-Chair of the Board and Lead Independent Director, Credit Suisse
- Dina Dublon, Risk Committee Chair, Deutsche Bank
- Betsy Duke, Independent Vice Chair, Wells Fargo
- Douglas Flint, Chair of the Board, HSBC
- Tom Glocer, Operations and Technology Committee Chair, Morgan Stanley
- Nick Godfrey, Managing Director and Co-Chief Information Security Officer, Goldman Sachs
- Byron Grote, Non-Executive Director, Standard Chartered
- Mike Hawker, Remuneration Committee Chair, Macquarie
- Bob Herz, Audit Committee Chair, Morgan Stanley
- Olivia Kirtley, Risk Management Committee Chair, US Bancorp
- Axel P. Lehmann, Group Chief Operating Officer, UBS
- John Lipsky, Non-Executive Director, HSBC
- Rachel Lomax, Senior Independent Director and Conduct & Values Committee Chair, HSBC
- Douglas Lyons, Chief Credit Officer, Nomura International
- Deborah McWhinney, Non-Executive Director, Lloyds Banking Group

- Scott Moeller, Risk Committee Chair, JPMorgan Securities
- Andy Ozment, Co-Chief Information Security Officer, Goldman Sachs
- Bill Parker, Vice Chair and Chief Risk Officer, US Bancorp
- Kevin Parry, Audit Committee Chair, Nationwide Building Society
- Nathalie Rachou, Risk Committee Chair, Société Générale
- Susan Segal, Corporate Governance Committee Chair, Scotiabank
- Alexandra Schaapveld, Audit and Internal Control Committee Chair, Société Générale
- David Sidwell, Senior Independent Director and Risk Committee Chair, UBS
- Tim Tookey, Risk Committee Chair, Nationwide Building Society
- Jasmine Whitbread, Brand, Values & Conduct Committee Chair, Standard Chartered

Regulators, supervisors, and others

- Jonathan Davidson, Director of Supervision, Retail & Authorizations Division, UK Financial Conduct Authority
- Harald Heide, Head of Section in DG-MS1/6a, European Central Bank
- Lyndon Nelson, Deputy CEO & Executive Director, Regulatory Operations and Supervisory Risk Specialists, Bank of England Prudential Regulation Authority
- Stephen Page, Non-Executive Director, BSI Group and the National Crime Agency
- Bruce Richards, Senior Vice President and Head of the Complex Financial Institutions, Federal Reserve Bank of New York
- Molly Scherf, Deputy Comptroller, Large Bank Supervision, Office of the Comptroller of the Currency
- Todd Vermilyea, Senior Associate Director, Division of Supervision and Regulation, Federal Reserve System

EY

- Omar Ali, Managing Partner, UK Financial Services
- Peter Davis, Americas Financial Services Advisory Leader
- Marie-Laure Delarue, EMEIA Banking and Capital Markets Leader
- John Doherty, Partner, Governance Risk and Compliance
- Steve Holt, Partner, FS Advisory
- Ertem Osmanoglu, Americas Deputy Cybersecurity Leader
- Isabelle Santenac, EMEIA FSO Assurance Managing Partner
- Bill Schlich, Global Banking and Capital Markets Leader

Tapestry Networks

- Dennis Andrade, Partner
- Jonathan Day, Vice Chairman
- Colin Erhardt, Associate

Endnotes

[1] "Top 10 Operational Risks for 2017," *Risk.net*, January 23, 2017.

[2] Emma Dunkley, Caroline Binham, and Sam Jones, "Overseas Cyber Attackers Targeted Lloyds," *Financial Times*, January 22, 2017.

[3] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby comments are not attributed to individuals, corporations, or institutions. Network participants' comments appear in italics.

[4] Steven Norton, "Wells Fargo CISO Says Cyber Investments Pointing Way to Better Risk Management," *CIO Journal* (blog), *Wall Street Journal,* March 13, 2017.

[5] "How to Manage the Computer Security Threat," *Economist,* April 8, 2017.

[6] "Effective Cybersecurity Strategy Rests on People, Not Just Technology," *Insurance Journal,* March 1, 2017.

[7] Jonathan Cedarbaum and Sean Reilly, "Cybersecurity Collaboration: Routes to Stronger Defenses," *Banking Perspective* 3, no. 1 (2015), 66.

[8] Martin Arnold, "Finance Sector Urged to Ramp up Cyber Defences," *Financial Times*, December 8, 2016.

[9] Lalita Clozel, "Big Banks to Regulators: Don't Tread on Our Cybersecurity Efforts," *American Banker,* March 1, 2017.

[10] National Institute of Standards and Technology, "NIST Releases Update to Cybersecurity Framework," news release, January 10, 2017.

[11] EY, "Enhanced Cyber Risk Management Standards for Financial Institutions," Financial Services regulatory alert, October 2016.

[12] Eli Sugarman, "Four Questions for Steven Weber on Cybersecurity Futures 2020," Hewlett Foundation, May 23, 2016.