Bank Governance Leadership Network
ViewPoints

December 13, 2013 TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM · +1 781 290 2270

Addressing cybersecurity as a human problem

Cybersecurity has been a prominent topic within the Bank Governance Leadership Network (BGLN) for more than two years. As the economic impact of cybersecurity has steadily grown, the BGLN has engaged with non-executive directors and executives of global banks and other major financial service firms, along with representatives from supervisory institutions, governments, security authorities, and technology experts to address the issue. This engagement culminated in a June 2012 meeting entirely dedicated to cybersecurity.[1]

The importance of cybersecurity for banks continues to increase, as does the frequency and severity of attacks. Today, there are almost daily reports of cyberattacks on banks. These include distributed denial-of-service attacks – designed to overwhelm bank web servers – as well as theft of customer data and intellectual property. Consequently, various stakeholders have initiated efforts to improve banks' defenses against cyberrisks; such efforts include governments increasing efforts to protect critical infrastructure, legislatures working on new laws to enable more information sharing, regulators conducting war-gaming exercises, and banks increasing their investments and protections, individually and through industry bodies. Despite these attempts, cyberattack remains a growing threat, necessitating increased attention, understanding, and collaboration both in individual banks and system wide.

On November 19, BGLN participants gathered in London to discuss cybersecurity, including its evolving threats, the systemic risk it poses, and the ways that boards should deal with cybersecurity issues. Participants also discussed innovative tactics for improving bank and system defenses. Given the systemic nature of the threat, the meeting brought together critical stakeholders to discuss the issue, including government officials, regulators, bank non-executive directors and executives, and subject-matter experts. For a list of participants, see Appendix on page 11.

This *ViewPoints*[2] captures the essence of those conversations, in which five key themes were discussed:

- Knowing your adversaries
- Focusing on internal systems
- Defending an ever-growing security perimeter
- Responding systemically
- Strengthening the board's role in cybersecurity

[1] See Bank Governance Leadership Network, "Cybersecurity: an Emerging Risk for Global Banks and the Financial System," *ViewPoints*, August 13, 2012.

[2] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants and their corporate or institutional affiliations are a matter of public record, but comments are not attributed to individuals, corporations, or institutions. Network participants' comments appear in italics.

Knowing your adversaries

Prior to the November meeting, several bank information technology (IT) executives questioned why cybersecurity should be treated distinctly from other forms of data or IT security. Similarly, a regulator at the meeting said, *“We ask ourselves, ‘Is cybersecurity different? And if it is, what should we be doing differently?’”* Meeting participants were in agreement that cybersecurity is different for many reasons, notably the scale, rapid evolution, and potency of the threat.

One director said, *“The challenge is that our systems are vast – they are processing thousands, hundreds of thousands, sometimes millions of items a day.”* Noting the rapid evolution of attacks, one regulator stated, *“This is a continuously mutating risk.”* Another said, *“There has been an exponential increase in the scale of the threat and its fast-evolving nature. Each evolution of the attacks gets faster.”* One regulator said before the meeting, *“Every time you repel [attackers], [they] come back smarter.”*

Collaboration among adversaries makes cyberattacks ever more difficult to repel. As one IT security expert put it before the meeting, *“The criminals are sharing information between themselves, and joining forces online.”* At the meeting, participants agreed, with one expert noting, *“Some groups of adversaries work together. There have been instances of sophisticated adversaries selling their technologies and intelligence on the black market once they are done with it.”* A regulator added, *“The barriers to entry [into cybercrime] have gone down, and we are seeing coalitions among the cyberattackers.”*

Experts at the meeting recommended the “80–20 rule” for understanding cyberthreats. According to one security expert, *“Eighty percent of the threats are broad based, not highly targeted or necessarily sophisticated … Hacktivists tell you what they’re going to do. If you look in the right places, they broadcast it.”* However, one director noted that the existence of a large number of small actors presents a collective challenge: *“Often, this is not about someone stealing a lot of money, but instead, the question is, can you catch a lot of small criminals going after small sums.”*

Nonetheless, the largest financial risk to banks comes from the 20% of threats generated by serious criminal organizations. The adversaries in question are economically rational, more interested in stealing money than in disrupting banks. These critical adversaries run global businesses that target other global businesses; they are not activists or vandals, but organized criminals with significant budgets. At the meeting, one participant said, *“The 20% threat – from the adversaries who present advanced persistent threats – is the most worrisome.”* The participant elaborated, *“You really need to understand the adversary. Their tactics, techniques and procedures … The adversary has a multibillion-dollar budget, and they want a return on their investment. These are multiyear campaigns. When their success rate fails, they develop new approaches … The reality is one campaign often involves multiple attacks – it could include 20,000 attacks. The trick is knowing the adversary’s approach so that you can use the same course of action to repel all 20,000 attacks.”*

Understanding that the most potent threats derive from economically rational actors provides one notable technique for defense: make cybercrime less economically rewarding. As one participant noted, *“If their return on investment isn’t good [when] attacking our company, they will go somewhere else.”* For banks, this approach is far more cost effective than completely trying to shut out adversaries from their systems.

Focusing on internal systems

Although cyberattacks threaten not only an individual institution's systems but also many external networks, banks must begin by protecting their own internal IT systems. Most banks operate through a collection of different systems, some commercial off-the-shelf systems and some custom made. Many legacy systems have been inherited through mergers over the past several decades, and the resulting internal systems are therefore difficult to protect. A key mindset change for many banks is moving from a focus on building bigger walls around the perimeter to accepting that systems will be breached no matter what technological barriers are present. This means that banks need to attend to keeping the data that really matters from leaving their systems.

BGLN dialogues during and leading up to the meeting identified several important steps that banks can take in this regard:

- **Getting the basics right.** Though it is tempting to focus attention on the latest technologies, several BGLN participants have urged banks to focus on a more basic approach. Many banks buy expensive protection software and equipment but fail on simpler and more fundamental measures. One participant said, *"The reality is, still, in large firms that the basic security hygiene is missing – say, the most recent patches. Firms have to get the basics done first."* Systems can also be simplified. Another participant added, *"We have reduced the number of internet 'pipes' into our firm to two, and reduced the number of data centers from over 40 to five. This has greatly enhanced our ability to protect ourselves, and it's cheaper."*
- **Developing capabilities, not just technology.** One meeting participant stated, *"Technology doesn't solve this problem."* Rather, as one director observed, *"It is about processes, technology, and the culture within the organization."* Rather than focusing almost exclusively on technological fixes, a participant said, it is more important to develop people with the skills to respond, calling it the *"tradecraft."*
- **Improving system resiliency to prevent data corruption or destruction.** Banks have long had off-site backup systems in place; however, recent events have underscored new challenges. One regulator said sharply, *"The Stuxnet attack*[3] *was a game changer. What do you do if your systems become inoperable? Or if your data is completely corrupted? Standard backup systems don't help, as they have the same corrupt data."* A participant at the meeting also admitted, *"We do tend to focus on the robustness and resiliency of our systems, but we are less attuned to data being destroyed or corrupted."* Moreover, a director said, *"Our firm is looking into additional backups. If our main system's information is corrupt, by definition so is our backup. So do we need a third system that's backed up differently?"*
- **Focusing on how physical factors can enhance the risk of cyberattack.** An important point highlighted during the meeting was that cyberrisks are not simply technological in nature. Several BGLN participants pointed to the recent attack on Santander in the UK, in which criminals posed as engineers. Entering a branch, they installed a KVM (keyboard, video, and mouse) switch, a device that enables one computer to remotely control many others by manipulating their keyboards, mice, and video screens.

[3] Stuxnet is a computer worm discovered in June 2010 that is believed to have been created by United States and Israel agencies to attack Iran's nuclear facilities.

The particular incident was notable because it combined both high-tech and more traditional elements of low-tech crime, showing that, in the words of a *Financial Times* story, it is "not just IT security methods that needed to be scrutinised, but also people's [physical] access to computers."[4] In discussing this incident before the meeting, one participant predicted that protecting internal systems would become more challenging: *"Given the high level of outsourcing of maintenance and cleaning staff, and high turnover among the contractors, it is easy to get into buildings."*

- **Identifying and protecting the *"crown jewels."*** Before the meeting, several subject-matter experts noted that few banks have identified the core data that they absolutely must protect, what several referred to as the *"crown jewels"* or *"trophies."* At the meeting, a participant commented, *"Firms need to know where their critical information and systems are. Are they protected? What happens if it is compromised [or] destroyed?"* Institutions must accept that their systems *will* be infiltrated and that they therefore need to shift their focus to the core systems that most need protecting. In many cases, it is more important to keep attackers from getting valuable information out than to try to stop them from getting in. As one BGLN participant put it before the meeting, *"The bottom-line message is you can't stop everything. There must be multiple layers of defense. Intrusion will happen. The point is that the adversary can't get your critical information."* Another participant recommended the following: *"Firms need to know their businesses first in order to know what to protect. In investment banking, there is important intellectual property. In retail, it's financial crime, customer data."* Intellectual property could include information on how markets work or on specific trades.

- **Testing system vulnerability more routinely.** Banks are stepping up the frequency and depth of their vulnerability testing. One director said, *"We launch our own unauthorized trades to assess where they get caught."* Another noted, *"We have vulnerability assessments done, and the results are shared with the board and risk committee."* Using what is often referred to as a red-team approach, some firms have in-house teams attacking their own systems in order to spot vulnerabilities. One participant said, *"We have a red attack team, which uses the same tactics as our adversaries to attack our systems and those of our supply chain."* Further testing should also be completed whenever major IT upgrades are undertaken. One regulator advised before the meeting, *"If I were a non-executive director, I would have vulnerability tests done after every major change – you don't know what new doors it opens."* Last year, RBS became a notable example of such risks when a software upgrade to the payments system led to nearly 12 million people losing access to their accounts for a prolonged time period.

- **Improving human counterintelligence.** Cybercriminals increasingly rely on "HUMINT" (human intelligence), such as sending spurious employees into a target company or creating fake vendors. Banks must therefore sharpen their skills in human counterintelligence. One expert described the creation of *"honey traps,"* apparently attractive systems that criminals can penetrate. The honey traps are not, for the most part, used to identify criminals to law enforcement authorities, but to silently observe the attackers at work and gather intelligence on their methods. *"Once you use a honey trap to bait an adversary,"* he said, *"it may prove useful; you can't learn from criminals you have shut out."*

[4] Caroline Binham and Patrick Jenkins, "Cyber Raiders Foiled in Attempt to Steal Millions from Santander," *Financial Times*, September 13, 2013.

Defending an ever-growing security perimeter

Recent trends in banking, notably the increasing adoption of new technologies and digitalization of financial services, have greatly expanded the perimeter that requires protection from cyberattacks. This perimeter is difficult to define, monitor, and defend because it is rapidly expanding and includes employees, customers, and suppliers. Humans, rather than machines or data networks, play a major role in extending the perimeter; securing it is primarily a human challenge.

Employees are creating new risks for cybersecurity

The risks created by employees come in three major forms:

- **Lack of knowledge.** Despite training and communication, many employees are still unaware of how their actions – for example, opening a phishing e-mail or an attachment from a suspicious party – can assist adversaries. One director commented on the difficulty, saying, *"At one level, it is easy to understand; it is analogous to physical security. But we know from our staff that they are less focused on this security risk than they are on physical risks."* It can be challenging to communicate and engage employees effectively, given the range of risks employees are being asked to consider. Prior to the meeting, one IT executive observed, *"It's hard to get everyone focused. Yes, this is a major risk. But we have so many risks at the moment, and some feel more proximate [to those in the business] than cyberrisks, such as regulatory risks."*
- **Personal technology.** The use of personal devices by employees connected to company systems – commonly referred to as bring your own device (BYOD) – is creating complex new challenges. Banks are increasingly allowing employees to use their own devices for cost and employee satisfaction reasons, but as a technology leader remarked before the meeting: *"[BYOD] has major implications. These devices are less secure, but they are now part of the firm's ecosystem, [yet] firms don't control them."* Even departed employees pose a threat. Passwords and access rights may be left open or, worse, criminals may approach former employees to seek their help.
- **The *"insider threat."*** The most sinister threat comes from criminal activities by employees themselves. As one director said, *"I am concerned about the insider threat."* Another participant agreed, noting, *"[Employee] espionage is real … so our aim is to protect our [intellectual property] before it is stolen. We are enhancing our ability to predict people's behaviors."* Another participant said his firm is investing heavily in analyzing trader behaviors on a real-time basis: *"We have 25 key performance indicators that identify potentially problematic actions of traders. For example, the number of office entries made at nighttime, the number of changes made to a single transaction, the amount of holiday taken. This allows us to identify the five to 10 cases of behaviors that need investigating."*

New customer interfaces are creating more vulnerabilities

Mobile and internet banking offer new ways for banks to engage with customers and provide them with greater convenience and service. Indeed, online banking is now the preferred mode of interaction,[5] with 50% or more of adults in the United States[6] and UK[7] performing transactions online. Smartphone adoption is the fastest of any technology in history,[8] and it is not difficult to see a day when, for many, these devices replace cash machines and wallets. However, mobile technology opens up a Pandora's box of cybersecurity issues. As a bank executive observed before the meeting, mobile devices *"create multiple access points"* for infiltrating banks' systems, thereby increasing an institution's vulnerability.

One meeting participant said, *"People will get into your system, and they can compromise you via your customer."* As such, one regulator said, *"Firms should focus more on their customers. Accessing your system via a customer is a reality."* One participant said banks should ask, *"Are our customers aware of the threat? How can they help protect themselves and your institution?"* An executive remarked, *"We are trying to look at it from the customer perspective as well. Is the customer protected through using [our services]?"* Few participants at the meeting could confidently say their organizations have fully addressed this vulnerability, with one saying, *"We have a great deal to teach our customers on how they can protect themselves."*

Use of third-party vendors causes an outsized increase in risks

Banks have always been major users of third-party information and technology vendors, but this practice has become even more pronounced as banks seek to lower their costs in the face of new regulatory requirements and stagnant growth. Consequently, as one BGLN participant said before the meeting, *"Vendor and outsourcing relationships create a real risk."* Several meeting participants agreed, with one saying, *"Firms need to focus on the weakest link in the systems – for example, contractors."* Another said, *"Your supply chain is a major vulnerability."*

Supervisors have raised the concern of the sector's ability to manage this risk, with one saying before the meeting, *"The movement of services or data to the cloud or third parties is a big concern. Firms don't have control of that data."* A bank executive said, *"Third parties are coming to the fore in terms of supply-chain risk. Do we understand security or even what information they possess? … Do we understand the fourth and fifth parties and further downstream? If they can't get to us directly, this is where they will go."*

Responding systemically

The financial system is intricately interconnected and complex, with data constantly moving in and out of other banks' systems thousands of times a second, amplifying the system's vulnerability and that of individual banks in the system. Not surprisingly, as threats have grown in number and potency, governments and

[5] Ernst & Young, *The Customer Takes Control: Global Consumer Banking Survey 2012* (EYGM Limited, 2012).

[6] Susannah Fox, "51% of U.S. Adults Bank Online," *Pew Internet*, August 7, 2013.

[7] Office for National Statistics, *Internet Access – Households and Individuals, 2013* (London: Office for National Statistics, August 8, 2013).

[8] Stephanie Mlot, "Smartphone Adoption Rate Fastest in Tech History," *PCmag.com*, August 27, 2012.

regulators across the world have taken concerted action to protect critical infrastructure. Individual governments have stepped up their investments in cybersecurity for the financial system and have established information-sharing units so that the official sector and banks can share information quickly and effectively. The French and UK governments have been highly visible in these efforts, as has the United States. While governments and regulators should be applauded for increased attention and investment in protection, there are areas where enhanced systemic approaches could build a more resilient financial system.

Assessing the system's vulnerability

War-gaming exercises are becoming more commonplace, using simulated cyberattacks as a means to see how financial institutions and the system cope under duress. In the UK, Waking Shark 2 was recently completed, resulting in the Bank of England's Financial Policy Committee calling on regulators to develop action plans in the event of a major cyberattack. Similarly, the Banque de France recently assessed the country's readiness to deal with a cyberattack, including its ability to coordinate participants' business continuity plans, enable coordinated communication with external stakeholders, and check that links to government representatives, network operators, and critical-service providers were effective.[9]

Regulators at the BGLN meeting commented positively on these types of exercises. *"Industry scenarios are very helpful. They show everyone how the system connects together and how others might react,"* said one. Another noted, *"The scenarios help the players practice their reactions and take lessons from what they learn so they can adapt their approach."* While best practices and information are shared, challenges for defense are also made evident. Before the meeting, one regulator said, *"These exercises show institutions act alone … and that doesn't make for a complete system response."* Meeting participants also highlighted the need for improved communication, with one saying, *"In every scenario, the most acute problem is communication between the government authorities and the sector, and across the sector."*

Protecting the key system nodes

The challenge in protecting the financial system at large is that it is almost impossibly complex. As one regulator said before the meeting, *"We have started to map the sector from a systems perspective to identify system vulnerabilities, but the task is vast. What we do know already is the system is phenomenally sophisticated and no single person understands it."* The key is focusing on the critical parts of the system. As one regulator at the meeting said, *"We are looking at the system-wide vulnerability and key nodes within the system."* Central banks are particularly concerned about clearing and payments systems, a concern validated by a July report by the World Federation of Exchanges finding that more than half of the 46 exchanges it surveyed had fought off a cyberattack in the past year.[10] Yet, as one regulator admitted, *"The regulatory community is starting to assess the cyberpreparedness of the main nodes in the system, but there's a lot more work to do."*

[9] Secretariat of the Robustesse Group Coordination Unit, *Report by the Paris Robustesse Group: Market-wide Exercise on 12 and 22 November 2012* (Paris: Banque de France, 2013).

[10] Phillip Stafford, "Half of Exchanges Fight Off Cyber Attacks," *Financial Times*, July 16, 2013.

Part of the problem is that the regulator's role is unclear. One regulator said, *"We don't currently have a specific focus on cyberrisks, other than in the recovery planning and general IT assessment. The question is, should we?"* Moreover, as another regulator said, *"The challenge for regulators is that we are used to static risks, ones we can write rules for through a proper consultation process. [But] that's too slow for cyberrisks; we need to be much more agile. The legislative and rulemaking process imposes a risk for our approach in this area."*

Improving information sharing and coordination

Information sharing represents a major area of system weakness, even as meeting participants emphasized its importance. One participant noted, *"Intelligence is crucial. We constantly analyze our adversary's attacks and fuse that together within other internal and external pieces of intelligence."* The participant continued, *"Collaboration on actionable intelligence is important. It helps you understand the threat and be more prepared. There is great benefit in sharing intelligence across the sector and with other [critical national infrastructure] sectors."* In that participant's experience, *"The most effective collaboration is peer to peer within the private sector."* Yet a director asked, *"What is the scale of the risk? My sense is it is so large that we should be doing more together as an industry, and not just information sharing."*

Connectivity with the authorities is also essential, as one participant remarked: *"It is important that the [banking] industry build stronger bridges with government."* Yet, as another participant noted, *"We do not have optimal coordination amongst the government agencies and regulators yet."* The weakness most cited by industry executives is the limited information flow from governments to banks. Government agencies often have significant human and technical counterintelligence data; however, as one regulator put it, *"The challenge with information sharing from the government is, often, the sources are sensitive. Plus, the authorities tend to have a closed mindset about information sharing."* Notwithstanding that concern, a director urged action: *"We need to ignore the boundaries between our organizations and collaborate more."*

Strengthening the board's role in cybersecurity

The impact of a cybersecurity breach is exacerbated by the limited experience that most boards have in this area, as well as by a lack of principles for a board's involvement. BGLN discussions have highlighted several areas where improvements are needed:

- **Defining governance roles and responsibilities.** Boards and management teams still struggle with the question of how much board or committee time should be dedicated to cyberrisks, and they are looking for emerging frameworks to improve their approach to this threat. The draft National Institute of Standards and Technology framework in the United States is a start; however, recent frameworks raise an underlying question: what are the appropriate roles and responsibilities of directors versus executives?
- **Incorporating cyberrisks into risk appetite frameworks.** Few banks have effectively built cyberrisk into their enterprise risk appetite framework. According to a recent report by EY, 62% of organizations surveyed have not aligned their information security strategy to their risk appetite or tolerance, suggesting that "when setting budgets or determining resource requirements, too few

organizations consider the cyber risks they are prepared to accept or must defend against at all costs."[11] One regulator said, *"Banks have not gone far enough in building [cyberrisk] in their risk appetite frameworks. It should be a distinct risk."* Those that have tried admit it is difficult.

- **Developing an effective set of performance metrics.** To properly govern, many directors point to the need for appropriate metrics against which to assess the changing scope and nature of the threat and the bank's success in repelling it. One director commented, *"What we need are some comprehensible metrics so we know how well we are doing. How vulnerable are we? What are the metrics?"* There are no industry standards, as there are in fraud, but pragmatic approaches can help. Another director said, *"There are some metrics you can use. You can measure the number of attacks; the number we stopped; when and how we caught them; whether we are catching them earlier over time."*
- **Developing a coordinated control approach.** Most banks have yet to determine the right approach to managing cyberrisks across IT, risk management, internal audit, and compliance internally. The challenge is compounded as these risks extend to customers, employees, and third-party vendors and as they draw in other key functions, such as human resources and legal departments.

⋆ ⋆ ⋆

The financial service sector is the most targeted industry in the world of cybercrime, appealing to attackers in many ways: financial crimes are rewarding; personal data is incredibly valuable; and for the politically motivated, attacks that further degrade the industry's image capture the public and media attention. Bringing down a national financial system would have serious implications for an economy at large. This appeal means that the most dangerous attackers are well-funded and experts at what they do. The scale, frequency, success rate, and economic impact of attacks looks set to increase.

To successfully fight these adversaries, every actor in the private and public sector has to do more to ensure their institution plays its role appropriately and fully, and that they work together across constituencies, borders, and sectors. While progress has been made since the BGLN started discussing the topic, much remains to be done. As one director put it, *"I don't know of any aspect of risk that is so big, yet so difficult to understand whether we are doing enough to address it."* Boards and directors have a critical role to play in protecting institutions from cyberrisks and, with concerted action, they can do much to create a more resilient banking and financial system.

[11] EY, *Under Cyber Attack: EY's Global Information Security Survey 2013* (EYGM Limited, October 2013), 7.

Bank Governance Leadership Network
ViewPoints

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, 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 multi-stakeholder 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.

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of any individual bank, its directors or executives, regulators or supervisors, 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.

Appendix: Meeting participants

- Mr Marc Andries, ACPR
- Lord Norman Blackwell, Lloyds Banking Group
- Sir Sandy Crombie, RBS
- Mr Renato Fassbind, HSBC
- Mr Gavin Frampton, Lloyds Banking Group
- Mr Simon Fraser, Barclays
- Mr Ralf Hafner, Goldman Sachs
- Sir Callum McCarthy, ICBC
- Mr John Milne, Bank of England
- Mr Lyndon Nelson, PRA
- Mr Bertrand Peyret, ACPR
- Mr James Quinault, Cabinet Office
- Ms Nathalie Rachou, Société Générale
- Mr Michael Roberts, Cabinet Office
- Mr Anton van Rossum, Credit Suisse
- Mr Giri Sivanesan, Lockheed Martin

EY

- Mr Ian Baggs, Global Banking & Capital Markets, Deputy Leader, Financial Services
- Mr Serdar Cabuk, Director and UK Cyber Security Lead, EMEIA Financial Services Advisory
- Mr Robert Cubbage, Partner and Banking & Capital Markets Leader, EMEIA Financial Services
- Mr Steve Holt, Partner, Financial Services Advisory

Tapestry Networks

- Mr Dennis Andrade, Principal
- Mr Jonathan Day, Senior Advisor
- Mr Mark Watson, Partner
- Mr Charles Woolcott, Associate