# Data governance: securing the future of financial services

Financial Services Leadership Summit
January 2018

tapestry NETWORKS

EY
Building a better working world

# Financial Services Leadership Summit

FSLS

VIEWPOINTS

# Data governance: securing the future of financial services

> *Data is the new oil, but we do not yet know how to value data properly … If the good twin is digital transformation, then the evil twin is cyber risk. We need to figure out how to monetize information, but these two need to be addressed in tandem.*
>
> —Summit participant

Data is becoming the world's most valuable asset, and financial institutions gather, process, and store massive quantities of it; they have been described as "information technology companies with balance sheets." Yet banks, insurers, and asset managers are in the early stages of taking full advantage of data. As technology and technological transformation expand institutions' ability to profit from data, it ushers in new vulnerabilities. Protecting data remains among the most pressing issues facing financial institutions. As one director observed, *"Security is the foundation of the business. Whether it is holding your money in the best vault or providing promised aid during difficult times, financial institutions are premised on trust and security."* New regulations provide greater access to third parties and increase compliance risk around violating customer privacy. Directors are working hard to keep up with rapid developments in the field.

Governance of data is undoubtedly a board level issue, with significant implications for strategy, business model, IT architecture, and capital investment, as well as assurance, reporting, and management structures. On October 11–12 2017, leaders and regulators of major institutions in banking, insurance, and asset management met in New York for the Financial Services Leadership Summit, an event that brings together the Bank Governance Leadership Network (BGLN) with the Insurance Governance Leadership Network (IGLN). This *ViewPoints* synthesizes the discussions in preparation for, during, and following the summit. It is organized in the following sections:

- **Financial institutions need a strategic approach to data governance** ***(pages 3–14).*** Exploiting institutions' vast data collections is increasingly important to their competitiveness. New regulations are raising the stakes for data management, particularly with regards to privacy and security. Data governance is an increasingly strategic issue for boards.


- **Emerging technology will shape the value and use of information assets** ***(pages 15–23)*****.** Technology is expanding the information that financial institutions can access, but also making more information available to others outside the sector. Technologies like artificial intelligence, distributed ledgers, and process automation could have a profound impact on workforces, business models, and competition in financial services.
- **Cyber risk continues to grow as risk management and governance try to catch up** ***(pages 24–39)***. Cyber risk is not new, but it continues to grow and the nature of the risk changes quickly. The consequences of a major breach could carry massive direct costs, and potentially even worse indirect costs, including reputational damage. Boards are under pressure to be sure that cyber risk is being effectively managed in their institutions. Risk managers and directors are making progress toward better cyber governance, but it remains a challenging objective.

# Financial institutions need a strategic approach to data governance

> *"Collecting, safeguarding, and analyzing data is a core competency for banks. How we do that in the future is a key question."*
>
> – Participant

Data is an increasingly valuable asset to be managed and protected. Over the course of the summit, data was referred to as *"the new oil"* and *"the new currency."* One participant likened the rush to mine and create data to the California Gold Rush of the 1840s and 1850s. The centrality of information to financial institutions requires boards to treat the governance of the data they acquire, create, use, and monetize as a primary strategic issue. Indeed, as one participant stated, *"Collecting, safeguarding, and analyzing data is a core competency for banks. How we do that in the future is a key question."*

Even as boards are beginning to make data governance a priority, new regulations are raising the stakes of getting data governance wrong. One participant observed, *"We started with cybersecurity and the role for the board because the risk was so great. As we move forward, I think the role for the board gets bigger. It is about what data we have and how we use it, not just how we protect it."* A participant said the question for institutions is, *"How do I free data, think with data, and make use of it in the context of new regulations?"* Getting that right means understanding the frameworks for data usage, data security, systems and technologies for storing, analyzing, and securing data, and management and governance structures, as well as questions about ethical and acceptable use that go beyond compliance with regulations. A participant observed, *"Financial services has been data driven since the fractional reserve banking system. This isn't new. It is very much what they do, but they are not worrying about it or really thinking about it in a more strategic way yet.*

> *"As we move forward, I think the role for the board gets bigger. It is about what data we have and how we use it, not just how we protect it."*
>
> – Participant

## New regulations have heightened boards' focus on data usage, privacy, and security

A host of new cyber and privacy requirements have gotten the attention of boards and have opened discussions about data governance to include data usage, privacy considerations, and information security. Taken together, these laws and regulations make companies and their boards more accountable for breaches and compliance failures related to data. One director noted, *"Having regulators set a clear direction forces the board to start discussing data protection. What is the implication for our customers and for us?"*

## General Data Protection Regulation

The most notable of the new regulatory requirements, Europe's General Data Protection Regulation (GDPR),[1] highlights the need for better management of data privacy and usage. GDPR harmonizes regulation across the EU, but it also introduces significant new requirements, many of which are intended to empower individuals to better control personal data. In terms of regulation of digital activity, the GDPR represents a sea change. Its broad scope and application ensure that it will affect any company in possession of data related to European citizens or companies, including those headquartered and operating outside of Europe. In the context of existing privacy requirements, it takes the past work of privacy commissions and regulators and makes mandatory what some organizations previously considered voluntary.

### What is GDPR?

The GDPR, which will come into force in May 2018, applies to any company that processes the personal data of an EU subject, regardless of the firm's location. The regulation requires that contracts governing consent to use data be clear and easy to understand. It grants, or enshrines in law, new rights, including the right to know whether and how a firm is using an individual's data, rights to data access and portability, and the "right to be forgotten," meaning the right to have individual data erased and no longer disseminated. The law imposes a 72-hour mandatory breach-notification requirement in cases where a breach is likely to "result in a risk for the rights and freedoms of individuals."[2] Penalties for violations are stiff, as much as 4% of the firm's annual global revenue or €20 million, whichever is higher.[3]

Several important principles underpin the GDPR and similar legislation that is cropping up around the world:

- **Lawfulness.** Personal data shall only be processed when there is a lawful basis (e.g., consent, contract).
- **Fairness.** Data subjects should have enough information about processing to exercise their rights.
- **Transparency.** Information given to subjects must be easy to understand and concise.

## What is GDPR? *contd.*

- **Purpose limitation.** Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed.
- **Data minimization.** Processing of data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy.** Personal data shall be accurate and kept up to date.
- **Storage limitation.** Personal data should not be kept in a form that permits identification for longer than is necessary.
- **Security.** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage.
- **Accountability.** A data controller shall be responsible for demonstrating compliance.

*"We have millions of customers and vendors around the world. How do you ensure you are storing data and obtaining consent appropriately? It is a mammoth task."*

– Director

Participants raised several issues regarding the legislation that are of particular concern to boards:

- **Scope and cost.** *"We have millions of customers and vendors around the world. How do you ensure you are storing data and obtaining consent appropriately? It is a mammoth task,"* said one director. The large scope of the regulation will make compliance costly and requires additional investments in systems, processes, and personnel. Participants noted that the same challenges that plagued efforts to digitize their enterprises, namely issues related to fragmented and legacy systems, will hinder compliance with new regulations.
- **Readiness.** Furthermore, readiness surveys suggest most firms are underprepared. For example, a recent HM Government report suggested that a mere 6% of UK companies reported being completely ready to meet their compliance requirements.[4] By some accounts, the financial sector may be ahead of other sectors as a result of massive system modernization efforts; however, most directors concede a lot of work remains to be done. One director asked, *"Despite efforts to improve legacy systems, I wonder how many firms know where all this data is and can update their processes?"* Given these challenges, some participants

*"Despite efforts to improve legacy systems, I wonder how many firms know where all this data is and can update their processes?"*

– Director

questioned feasibility. *"No one knows how to do it. It may be that it can't be done. So what happens when it goes live?"* asked one director.

- **Compliance risk.** Participants observed that there is limited guidance or historical precedent as to how the regulations will be applied, yet the scale of potential fines—in the case of GDPR, up to 4% of annual global turnover—represents a major compliance risk. One insurance director said, *"For us, 4% is over $2 billion. We don't take a risk that size in a hurricane, and that is our business. I don't think we've put enough into our data management process."*

*"The portability of GDPR is important ... The ideas behind it are advancing even if some companies are not."*

– Participant

- **Global reach.** Several participants raised concerns about whether European standards should be applied globally in order to ensure compliance with potentially more stringent data requirements that could be adopted in other jurisdictions. Indeed, one expert noted that other countries are already moving forward with their own rules.[5] Even in countries like the United States, which have taken different approaches to data regulation historically, one participant predicted, *"The portability of GDPR is important. It will be implemented broadly and it is hard to see how that doesn't seep into the US. The ideas behind it are advancing even if some companies are not."*
- **Conflicting or ambiguous regulations.** Participants, including regulators, made two important points regarding regulatory views on data governance. First, these views differ significantly around the world, as do legal structures. The European GDPR limits data usage and promotes individual rights. In contrast, one participant suggested that the United States *"does not have a coherent view on data and privacy"* and, to date, has broadly favored data use in service of innovation over individual rights. Second, regulators are still defining their roles and responsibilities vis-à-vis data. Regulators also noted the importance of collaboration across jurisdictions and among different types of regulators, particularly as existing banking and insurance regulations may not align neatly with privacy requirements. *"Data breach requirements in the GDPR are pushing privacy regulators to work with other regulators. As companies like Amazon and Alibaba expand, this concept of regulatory cooperation is absolutely essential."*

## Regulations providing access to third parties

Two regulations that provide access to third parties raise important questions about data ownership and accountability. One, Payment Services Directive 2 (PSD2), aims to enhance consumer protection, promote innovation, and improve the security of payment services within the EU. Among the goals of

PSD2 is to encourage competition, in part by requiring that financial institutions grant third parties access to some primary account-holder information.

To address similar goals, the UK Competition and Markets Authority is implementing a program known as Open Banking, which enables customers to share data securely with other banks and third parties via applications program interfaces (APIs). UK banks will be required to allow consumers to share their own banking data with other banks and third parties, as well as manage multiple providers through a single app. Final implementation of Open Banking will align with PSD2 in January 2018.

*"Five years ago, the idea that the industry would allow access to third parties would not have been taken seriously. But now it is the clear direction of travel."*

– Director

As with GDPR, Open Banking and PSD2 raise important board-level questions about strategy and risk. One director said, *"Five years ago, the idea that the industry would allow access to third parties would not have been taken seriously. But now it is the clear direction of travel—so how do we get it to work? What is the setup and common language needed so it can function for good customer outcomes?"* Others agreed with one who said, *"APIs and third parties may be great for customers, but there is a heightened rate of fraud and unauthorized transactions. Right now, if a transaction is authorized by the customer, the default assumption is the banks will cover it. But the idea that banks have an open checkbook is absolutely terrifying if it is the customer making the mistake. Can the old-world rules apply in the digital world?"*

The implementation of these additional directives requires financial institutions to consider not just how they use and store data but also the ways in which third parties may access and use that data, as well as any resultant risks or liabilities.

## Cybersecurity regulations

Several new regulations specifically addressing cyber risk elevate the board's role in information security. As with GDPR, some in the industry have decried these requirements as overly prescriptive, inflexible, costly, and difficult to comply with. Others worry that they create the additional risk of regulatory arbitrage. Still, others welcome the additional attention these regulations bring to important issues.[6] One chief risk officer suggested that new requirements might force greater attention to and maturation of cybersecurity functions: *"The New York [Department of Financial Services] regulation is probably a wake-up call. There's doing cybersecurity oversight well, and then there's being able to prove it. Most companies are doing pretty well, but can they prove it? Have corners been cut? A lot of things need to be sharpened up, so in that sense it's probably good."*

### Examples of new cybersecurity regulations in the US

- **New York State Cybersecurity Requirements for Financial Services Companies.** One analyst called New York's new cybersecurity regulations for entities licensed in the state "the most stringent rules in existence" for non-military organizations.[7] The regulations, effective August 2017, contain several mandates, including that entities maintain a cybersecurity policy approved by the board or a senior officer based on the entity's risk assessment. Covered entities must appoint a chief information security officer (CISO) or equivalent, perform periodic penetration and vulnerability testing, and establish limits to access and data retention. They must also have a written incidence response plan and notify the Department of Financial Services within 72 hours in case of a cyber event.[8]
- **National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law.** In October 2017, the NAIC adopted a model law that is largely consistent with the New York cybersecurity regulations noted above.[9]
- **Enhanced Cyber Risk Management Standards.** In late 2016, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Federal Reserve released an advance notice of proposed rulemaking regarding enhanced cybersecurity standards for large and interconnected entities under their supervision. The standards would apply to large financial institutions—those with greater than $50 billion in assets—and their significant third-party service providers. The rules would impose more stringent standards and would require boards to approve management's cyber risk strategies and ensure management stays within a cyber risk tolerance framework.[10] Even stricter standards would apply to "sector-critical systems" that consistently support the clearing or settling of at least 5% of transactions in certain markets, including a requirement that firms be able to restore those systems' operations within two hours of a cyber incident.[11]

## Data governance requires a strategic mindset

*"We need a data stewardship approach that looks at what is appropriate, not just what's allowed."*

– Expert

As data governance rises on the board's agenda, participants acknowledged that what has historically been a compliance approach to data security and privacy issues will no longer be sufficient. While most firms are racing to meet the upcoming GDPR deadlines, participants widely agreed with one expert who advised, *"Senior leaders need to take a more strategic view of data. This includes the risk and regulatory concerns, but it extends well beyond those as well. In many cases, reticence risk is greater than compliance risk. Firms don't use data out of an excessive concern about compliance risk. We need a data stewardship approach that looks at what is appropriate, not just what's allowed."* In fact, according to this participant, Summit participants outlined the next steps in advancing data governance.

### Understanding and valuing data assets

Underpinning all questions of data and strategy is an assessment of what data an institution stores, uses, and creates, as well as the value of that data. Yet senior leaders report that most institutions cannot fully answer these questions. Security and privacy considerations are forcing financial institutions to improve their mapping of and accounting for information assets. While wary of adding yet another area where boards are expected to go deep, most summit participants agreed that boards should have a better understanding of the data their institutions hold and prioritize investment in how they can analyze and secure that data. One director said, *"Getting the data from the basement to the world's leading edge of data analytics is at the top of the board's agenda."*

*"Getting the data from the basement to the world's leading edge of data analytics is at the top of the board's agenda."*

– Director

One expert suggested, *"In some ways, banks are better off than some because at least they know where their data is and have strong contracts with vendors."* However, even where boards are confident that their firms have a good picture of the data they possess, they question how institutions can better assess the value of that data. *"Does anyone really know what the data is worth?"* asked one director. One expert further suggested,

> *When we talked to companies about cyber insurance, we found that they can't value their informational assets. There is no harmonized approach to valuing information. Data is the new oil, but data has no way to be valued properly. We need a better way to think about the enterprise value of data. In the future, I think disclosing the enterprise value of data will be a regulatory requirement related to the risk profile of informational assets. Just like we stress tested financial assets after the crisis, informational assets need to be stress tested in a similar way.*


However, valuation methodologies are far from perfect. One director noted, *"I have a problem with applying a dollar amount because it doesn't capture the negative value. It doesn't take account for what can go wrong, regulatory risks, etcetera."* Another agreed, suggesting, *"Part of the work is being able to quantify downside, even if you can't quantify upside. Then you get some sort of probability."* Despite these challenges, participants agreed that working to improve the nature of informational asset valuation could contribute to better-informed board discussions and decision-making.

## Tech companies face a shift in public sentiment and additional scrutiny

As regulatory pressure has mounted, so too has public and political scrutiny of tech companies' practices with respect to data privacy and security and how their platforms are being used. Recent breaches, combined with a growing number of real and alleged misdeeds by several large technology and data companies—including tax evasion, manipulating users, monopolistic behavior and market abuse, cooperation with legally questionable government surveillance, fostering abusive work cultures, and facilitating crimes such as election tampering and human trafficking[12]—have raised high levels of concern. One director said, *"A few years ago these firms could do no wrong. Now what you mostly hear about is the problems. There is a more critical eye on the businesses themselves, not to mention some of the culture issues."*

The culture that provides tech companies with some innovation advantages over established financial services firms might be challenged by additional public and regulatory scrutiny. One participant cautioned that technology firms are growing out of touch with shifting political sentiment: *"The East Coast and the West Coast of the US speak different languages. They are almost like two nations with different goals. The West Coast and the tech companies see themselves as benefitting society. They do not see the changing regulatory energy in Washington; there is a hardening of opinion. They don't get it and something is going to break."*

**Tech companies face a shift in public sentiment and additional scrutiny *contd.***

IGLN and BGLN participants have long suggested that technology firms, whether large or small, will face greater regulation as they increasingly perform traditional financial services functions, and the current climate points, in particular, to greater regulation and scrutiny over how they aggregate and analyze data and operate dominant platforms. If, as an industry commentator noted, "banks are the very definition of data companies, with data so rich that the likes of Facebook or Amazon would kill for it,"[13] then the current and likely future experience of some of these tech firms may be a cautionary tale for financial services firms as they consider how to advance their use of data and develop their own platforms.

## Determining the risks and benefits in how data is housed

*"Not even Google knows how to run analytics well across multiple places. The data has to be in the same place."*

– Executive

Financial institutions house vast amounts of data—as a director noted, *"Fintechs or others may lease data or access it, but I don't see how banks or insurers get out of the business of holding onto customer data"*—and they are increasingly able to analyze and use the data in ways that can be valuable for marketing, product customization, and other purposes. But the liability and security issues related to holding that data is raising questions about the relative tradeoffs. If institutions continue to warehouse and use large quantities of data, an important question for leaders becomes, Where should data be housed and what limitations will companies face in their ability to move data across jurisdictions?

Analytics and security professionals agree that centralizing data into fewer locations creates significant advantages, but it is not without risk. One noted, *"Not even Google knows how to run analytics well across multiple places. The data has to be in the same place."* With respect to security, a CISO said, *"Data is easier to protect in one place. Security tends to like a homogenous environment."* Despite the myriad advantages, another CISO reported, *"It makes me nervous if it is all in one place. It can be easier to steal … The consequences of an insider attack go up if the insider can access more data."* Indeed, a key security flaw in the recent Equifax breach was the colocation and connection of many data pools. Several participants suggested that in the future, decentralized blockchain applications, which would not be subject to single points of failure, could offer better solutions.

*"Real savings will occur from standards that reach across borders."*

– Regulator

Local regulatory environments will also play a role in where and how firms store and process data. They face two important considerations. One is the degree to which banking and data regulation conflict. *"Many institutions are struggling with data localization laws that conflict directly with banking laws. There is greater data nationalism so the regulators and policymakers can have access, but this conflicts with policies to port data globally,"* one expert explained. The second, and broader, consideration is that divergence in local rules will create new risks and opportunities for global institutions. One executive acknowledged that centralizing data increased *"subpoena risk,"* noting that *"there is a case going to the US Supreme Court that looks at whether governments can access data stored elsewhere."* Some participants also suggested the possibility of regulatory arbitrage related to data standards; according to one expert, *"There are jurisdictions that are relatively open, like the UK, which will be attractive, but for privacy, more stringent jurisdictions will also be attractive."*

*"The regulatory structure, under GDPR for example, is too limited. A better alternative is a full stakeholder assessment, which understands what is beneficial to all parties."*

– Participant

However firms decide to centralize or decentralize data, one security expert suggested, *"It's not practical to have all data in one place with high walls, so the controls and competencies need to be with data and travel with the data."* A regulator acknowledged, *"Real savings will occur from standards that reach across borders. It's sort of irrelevant where the data is. In some ways, we have transcended this—data and business don't respect political borders, which is why real solutions will be multinational. It's like the horse is already out of the barn and we are trying to regulate barn construction."*

## Balancing multiple stakeholder considerations

To date, financial institutions have tended to focus on the value they can derive from data usage, rather than the benefits and costs to a broader universe of stakeholders. A participant asserted, *"The regulatory structure, under GDPR for example, is too limited. A better alternative is a full stakeholder assessment, which understands what is beneficial to all parties. This broader attitude won't come from a chief privacy officer or chief compliance officer. It really needs to be CEO and board led."*

While most participants agreed that if firms focus on the interests of customers, they will ultimately serve the interests of their institutions, new regulations such as the GDPR require that organizations evaluate which uses of data constitute a *"legitimate interest"* of the firm. That requires the organization to balance its interest against those of the customer and other stakeholders. The GDPR also permits the processing of data "for a task carried out in the public interest."[14] In that regard, a participant said, *"Bringing*

*all of that data together is the most powerful anticrime tool we have, but it is not that simple."*

Regulation is prescribing more in-depth consideration of external stakeholders, including customers, vendors, and the public. At the same time, some participants question whether social norms around data use are shifting such that some individuals may be more or less willing to provide data in exchange for service. One noted, *"Forty-four percent of millennials don't trust financial institutions with their information because of breaches, yet they freely share personal information on social media."* The trade-offs and balancing necessary in the current environment generate challenging questions for financial institution leaders and policy makers if they are to protect their reputations and avoid running afoul of not just regulations, but changing public expectations.

## Considering how governance and management structures need to evolve

Many firms are rethinking how data governance is structured, how roles are defined, and the kinds of talent needed in senior leaders. Roles like chief data officer and chief privacy officer are being reconsidered as these issues move from largely compliance or marketing roles to needing to address more strategic questions for financial institutions. As the complexity of the considerations involved increases, a participant asked, *"Have we structured our team to do this type of thinking and balancing? You need a different approach to staffing. It is not just a compliance function."*

One participant asked, *"What does a data protection officer even mean? How is the role defined? These are important questions."* Another noted the challenge in defining the role and therefore the required skills for a future chief data officer: *"These issues involve operational IT and business strategy questions all rolled up in one. That is a challenging role for a chief data officer."* Some firms have placed chief data officers in the C-suite, reporting to the CEO and responsible for all data, including its usage and protection. Others are exploring different models such as reporting to the chief risk officer, chief information officer, or chief legal officer. Finally, some are redefining the chief information officer's responsibilities to focus less on executing transformation projects and more on data and technology stewardship.

While firms appear to be experimenting with the construction of data functions, most participants agreed with one director who said that the skills required today are different from what was required in the past:

*"These issues involve operational IT and business strategy questions all rolled up in one. That is a challenging role for a chief data officer."*

– Participant


*[The data governance function] might have been some middle or junior people in the marketing or IT departments spread across the organization in the past. Now, it becomes a requirement to have someone who is thinking about regulatory control issues around data architecture to deliver data on a regulatory basis, and also to create data analytic capabilities. The challenge is finding somebody who combines a whole set of different skills that haven't been brought together in that way. There are not many people with the seniority and breadth of skills to really bring that together.*

***

A commentator noted, "Banks are the very definition of data companies, with data so rich that the likes of Facebook or Amazon would kill for it … Yet interestingly, JPMorgan, the world's most valuable bank, with a history (read 'data') of over 218 years, when compared to Facebook (2004) and Amazon (1994), is valued at less than half of the $500Bn both these internet companies achieved just last month."[15] As bank leaders focus on transforming their institutions through technology, and consider new business models and ways to leverage their assets, these questions about the relative value and use of data will be increasingly central to strategic discussions.

# Emerging technology will shape the value and use of information assets

Governments and other institutions have been collecting data since ancient times, and technology has always changed the way data is gathered, stored, analyzed, and shared. But recent years have seen profound developments in information-related technologies, including artificial intelligence, blockchain, large-scale data analytics, and data-sharing facilitated by APIs. These new technologies not only affect day-to-day operations, but also have the potential to transform and disrupt business models in ways that are difficult to predict. Over the course of the summit, participants explored several areas in which advancing technologies are profoundly affecting the information and security of financial institutions.

## Technology has expanded both the scale and scope of information assets

*"The smart phone and the concepts of unstructured data and advanced analytics changed the world."*

– Participant

As people have generated more and more information about themselves through social media and as the means of gathering all kinds of information expand—whether via mobile phones, online transactions, CCTV cameras, or sensors generating data about the moment-to-moment operation of refrigerators or jet engines—the sheer volume of data has exploded in recent years. By one estimate, the amount of data generated worldwide grew tenfold between 2010 and 2016, and analysts predict that growth will accelerate over the next decade.[16] Much of this growth is in "unstructured" data, such as images, behavioral patterns, and voice recordings, but there has also been an explosion of more traditional "structured" data, such as credit histories, demographic data, and financial records. As one participant said, *"The smart phone and the concepts of unstructured data and advanced analytics changed the world."*

The availability of new types of data raises questions about what organizations can and should do with that information. Examples raised during the summit include:

- **Facial recognition.** One participant said, *"People put selfies on the internet all the time. Do insurers have right to look at those and use facial recognition in underwriting? How much information are people putting out that they think doesn't have any value?"*

- **Voice patterns.** One summit participant noted, *"There are start-ups doing natural-language processing that can measure the tone of voice on quarterly investor calls to find patterns that give clues about the next quarter's results."*
- **Behavioral patterns.** Some analysts are using the amount of time an individual pauses over a blank on an online form before answering a question as a behavioral indicator that could help assess credit or insurance risk.
- **Biometric data.** One participant noted that firms are *"experimenting with building consumer wearables that measure three or four biometrics that tell you a lot—heart rate, sweat, galvanic response. If a wearable is watching those signals that indicate an impulse purchase, it delays you. There are systems that alert people that their bodies are telling them that they don't want to do something."*

*"The level of data is exploding … But the number of people who know what to do with it is not very many."*

— Director

These new types of data could have a significant impact on financial services organizations, but only if the organization can derive meaningful insights from the oceans of data available. As a participant from the insurance sector said, *"The level of data is exploding—it's growing at two to three times a year, and with the increase in computing power, the possibilities are endless. But the number of people who know what to do with it—whether insurers or regulators—is not very many."* Another participant said, *"The only way to extract value from data is to do something with it, by using it in some area of the business."*

## Emerging technologies have significant implications for the sector

Summit participants discussed three technologies—artificial intelligence, blockchain, and API interfaces—and their implications for financial services.

### Artificial intelligence and machine learning

Big data has given new life to artificial intelligence (AI), which encompasses a cluster of technologies that enable computers to achieve, or at least approximate, humanlike interactions with the external environment. Thanks to their ability to analyze enormous data collections, AI systems can surpass human beings in finding patterns in data, often identifying highly counterintuitive ones that no human could.

Many of the major advancements in AI in recent years are in the subfield of machine learning, the process whereby software, rather than being programmed with instructions for specific tasks, adapts and learns by testing

its actions when exposed to vast quantities of data. Indeed, it is that huge store of data, along with massive increases in computing power and rapidly declining data storage costs, that have driven advances in machine learning.[17] In essence, these systems train themselves without human intervention and improve their ability to perform analysis and make decisions. By 2017, AI algorithms had achieved or surpassed parity with humans in their ability to recognize human language.[18] In a very recent breakthrough, a machine-learning system programmed only with the rules of chess—no strategies or recipes for winning or example games—achieved "superhuman" levels of play simply by playing against a version of itself for 24 hours.[19]

*"Anything that involves identifying patterns is better done by AI than by humans."*

— Participant

In the financial services sector, AI and machine learning have much to offer. As one participant noted, *"Banks have had lots of data forever. Banking is based on data."* The same could be said of insurance companies and other financial services organizations. Machine learning makes it possible to garner insights from that information as well as to capitalize on new forms of information. Banks and insurance companies can use AI systems to decide whether to offer credit or how to price an insurance policy, based on analyses that are not possible for human beings to perform. One participant described a Chinese insurer that had deployed a mobile app to sign up new customers. The app used facial recognition software powered by AI not only to verify a person's identity, but also to tell if a potential customer was lying on their application. If the system detected a lie, it would require the applicant to come into the office to apply in person. A recent study from the Financial Stability Board (FSB) noted that machine learning is being used "to uncover non-linear relationships among different attributes and entities, and to detect potentially complicated behavior patterns of money laundering and the financing of terrorism not directly observable through suspicious transactions filing from individual entities."[20]

Summit participants had significant concerns about the implications of deploying AI, however:

- **The future of work.** By making possible the automation of tasks such as basic claims processing, underwriting, and credit scoring, AI has great potential to increase efficiency and reduce costs, but also profound implications for the future of work and workforce issues. One participant observed, *"I don't believe that skilled professionals are exempt. Anything that involves identifying patterns is better done by AI than by humans."* Another participant pointed to research showing that algorithms were better at reading scans than human radiologists. Similarly, a recent study found that a significant amount of the work done by lawyers, especially

tasks such as document review, could be done faster and more accurately by machines, reducing lawyers' hours by as much as 13%.[21] The systematic displacement of—according to some sources—up to 50% of existing tasks raises questions not only for government policymakers but also for large companies and their boards.[22]

- **Security.** AI is vulnerable to hacking, including the form known as adversarial machine learning, in which hackers use altered data to manipulate and retrain algorithms.[23] A participant described how adversarial machine learning works: "*You can poison the algorithm by poisoning the training data set.*" Another participant noted, *"I recently learned about the possibility of teaching algorithms to do bad things. In other words, in the same ways you teach them to catch fraud, you can teach them to miss fraud or bypass security."* To date, cybersecurity has largely focused on addressing hardware and software vulnerabilities to prevent or recover from loss of data or damage to systems. In the future, firms will have to protect themselves from data manipulation and loss of data integrity as well.

*"We need to build ethics into artificial intelligence. Ethics should be built in like the business objectives."*

— Executive

- **Ethics and algorithmic decision making.** Even putting aside the issue of deliberate manipulation of data and algorithms, entrusting computers with decision-making authority raises questions. One privacy expert warned, *"With machine learning, there is also the issue of algorithmic discrimination. How should we think about technologies and what they produce that is not already captured by legal systems?"* An insurance industry leader told a group of peers in 2017 that he would "be happy to wager with anybody here that any firm represented in this room will have a scandal in the next three years to do with an unethical algorithm. I'm sure it's going to happen."[24] One summit participant said, *"We need to build ethics into artificial intelligence. Ethics should be built in like the business objectives."*
- **Regulation.** Regulators are starting to address the issues associated with reliance on AI. For example, in addition to prohibiting discrimination by automated decision-making processes, the GDPR's "right to explanation" entitles EU citizens to an explanation if they are adversely affected by decisions made about them by an algorithm.[25] This may be difficult to enforce, however: because the algorithms train themselves, it is difficult to determine why they make certain decisions. One participant asked, *"When processes are difficult to understand, how is discrimination hidden?"* Sometimes even programmers don't know why algorithms make the decisions they make, much less regulators and industry leaders. Observers

find it unsettling to contemplate machines that are beyond their creators' understanding or control.[26]

- **Accountability.** Machine learning also complicates accountability, and financial regulators have expressed concerns that it could be difficult to hold parties accountable for decisions made by algorithms. The FSB recently stated, "If AI and machine learning based decisions cause losses to financial intermediaries across the financial system, there may be a lack of clarity around responsibility … It may not be possible to understand how undesired events occurred and when steps may need to be taken to prevent a recurrence."[27]

*"An infrastructure is being built around blockchain now. It's going to happen, and you're already seeing it be deployed in some places."*

— Participant

## Blockchain

Blockchain is one of the most discussed technologies of recent years, but all the publicity has not resulted in widespread understanding. One participant confessed, *"I am ignorant on blockchain—I don't get it; I don't understand it. We are experimenting at this point."* Summit participants generally agreed, however, that blockchain technology is moving from hype to implementation as the number of practical applications and blockchain test cases—in areas including settlement and clearing and maritime insurance—has increased significantly. *"An infrastructure is being built around blockchain now. It's going to happen, and you're already seeing it deployed in some places,"* said one participant. Many implementations remain at experimental or proof-of-concept stage, but others are already deployed, and new implementations have emerged steadily over the course of 2017.

### What is blockchain?

Blockchain refers to a form of distributed-ledger technology. A blockchain is a secure distributed database that allows for the verification and validation of information without relying on a central authority like a bank. Each new transaction depends on data from preceding transactions, verified by mathematical tests that, in theory, make the ledger indisputable and immutable. Blockchain depends on encryption technology, and only those with access to the proper encryption keys can add information to the ledger or retrieve encrypted data.

**What is blockchain? *contd.***

All parties have access to the ledger at the same time, which means that all parties have the same information. Some blockchains are open or public, meaning anyone has access to them, and individuals can add data to the ledger anonymously. Others, including most implementations by financial services organizations, are private or "permissioned," meaning only certain parties have access to the ledger, and the identity of those who add data is known.

Participants noted many potential benefits of blockchain, including increased efficiency and security and lower cost and friction, but they were equally keen to address challenges raised by broader blockchain implementation.

- **Access to accurate shared data**. Blockchain's distributed-ledger technology gives multiple parties secure access to shared data in real time. One banking executive described its promise thus: "Every bank, exchange and clearing house, we all have our own sets of the same data, which get out of sync and have to be updated and reconciled. The distributed ledger is the first technology that could implement a shared golden copy of that data."[28]

  Similarly, blockchain offers parties to an insurance contract access to more accurate and up-to-date information about the value of assets and their risk exposure, which can be updated in real time, based on changing circumstance. In 2017, EY partnered with insurers XL Catlin and MS Amlin, blockchain company Guardtime, and shipping giant Maersk to build a platform for maritime insurance based on blockchain. The platform "facilitates the secure capture and sharing of data among chosen participants in real time with an immutable audit trail," giving the platform the potential to eliminate the inefficient paper trail characteristic of today's maritime insurance industry.[29]

- **Automating transactions.** Blockchain's distributed ledger can automate agreements and transactions and eliminate the need for human interaction in the process through "smart contracts" that execute automatically once certain conditions are met. A relatively simple example is found in flight insurance, such as a new product called Fizzy, launched in 2017 by AXA. A customer requests flight insurance from a smart contract residing on the blockchain, which establishes a premium based on historic data about the particular flight gathered from an air traffic database. If the price is agreed,

the transaction is recorded on the blockchain and a smart contract goes into force. The contract monitors the flight database for status of the flight, and as soon as a delay is detected, a payment to the policyholder is automatically triggered.[30]

In banking, 22 of the world's largest banks and fintech start-up R3 (itself a consortium of some of the world's biggest banks, launched in 2014) announced in late 2017 an international payments system that would permit real currencies—not just cryptocurrencies like bitcoin—to be transacted on a blockchain. According to R3 and its partners, the elimination of manual processing and authentication through intermediaries will make payments faster and more efficient, to the point of enabling almost instantaneous international payments.[31]

- **Security.** One summit participant said, *"It is very early days on this, but security is really one of the things driving blockchain."* Referring to the recent Equifax data breach, another participant said, *"The critical flaw in credit reporting agencies is putting all that information in one place. Blockchain is distributed and decentralized, so no single loss would be catastrophic."* But like many new technologies, blockchain raises security risks even as it addresses existing ones. The most well-known implementation of blockchain technology, bitcoin, has been hacked on numerous occasions, including a hack in November 2017 in which hackers stole nearly $70 million worth of bitcoin.[32] However, one participant observed, *"Blockchains have been hacked, but they are maturing and getting more secure."*
- **Reliability.** A participant cautioned, *"Blockchain relies on encryption, and the math behind encryption is really solid, but the implementation is not solid … With blockchain you are surrendering governance, so you need perfect technology—how likely is that?"*
- **Fraud and integrity.** Another director raised the question of *"the integrity of the data. Will parties put in less-than-authentic data? How can you trust the data?"* Other participants pointed out that the same potential for fraud existed with older paper-based systems and that the speed of automated transactions could make fraud easier to detect, while admitting that blockchain would not eliminate *"the need for due diligence."*

## Application programming interfaces and "open access" to financial systems

Increasingly, APIs are facilitating deeper collaboration between major institutions and third parties, enabling both incumbents and challenger firms to offer new and customized products and services. APIs are "hooks" built into systems or software that allow other applications to access data or functionality present in the system. In banking, APIs are typically built on top of a provider's internal applications, including legacy and third-party systems and data. APIs may be open, providing data to a variety of external groups, or closed, providing data only to select contracted parties or to the institution itself. Financial institutions can use APIs for services such as reporting or to meet customer demand for services such as product or price comparisons. The growth of platform businesses is fueled in large part by APIs that can link data between organizations.

In the European Union and the United Kingdom, banks will be legally required to provide third-party access to current accounts via APIs effective January 2018 under PSD2. Some aspects of the United Kingdom's Open Banking initiative, which aims to make data more available, are already in effect.[33] While granting more third parties access to data and systems, PSD2 also includes "strict security requirements for electronic payments and the protection of consumers' financial data."[34] In the United States, providers are increasingly volunteering to open up their systems to outside groups to develop complementary applications.[35]

Open banking and data sharing through APIs raise both security concerns and regulatory issues. Offering outsiders greater access to proprietary data and systems creates many more interfaces that financial institutions and their partners must secure. Unsurprisingly, this can prove difficult. In 2015, for instance, a breach of a US Internal Revenue Service API enabled hackers to steal sensitive tax information from about 100,000 US taxpayers.[36] Not only do APIs and greater reliance on third parties create security challenges, they raise thorny liability concerns as well. As one director put it, *"If a customer says I want X company to be my interface and they sign something passing the data to them, and the company then doesn't have proper protections and something happens, who's liable? In fact, the answer right now is likely the bank."* Another insisted on the need for *"a clear regulatory framework around these third-party providers that we're going have to give customer data to. What obligations do they have?"*

## The new technologies may cause significant sectoral disruption

The discussions of blockchain, AI, and APIs surfaced questions about the disruptive potential of new technologies. *"The question is who is going to be the first to participate in the blockchain transformation. If it is fintech firms, how is that going to impact existing institutions?"* asked one participant. Participants said that open banking with APIs presents a fundamental challenge to the industry. *"Unless we get to the point where we can use the data we have stored smartly and innovatively, we risk being taken out of the process if third-parties are better equipped to interface with customers. So actually getting the data from the basement to the world-leading edge of data analytics is at the top of the board's agenda,"* said one bank director.

*"Unless we get to the point where we can use the data we have stored smartly and innovatively, we risk being taken out of the process if third-parties are better equipped to interface with customers.*

— Director

Over the course of the summit, participants discussed other challenges raised by emerging technology as well:

- **Disintermediation.** One director noted, *"There are clear winners and losers in this. It is changing the structure and business model of the industry."* Another participant noted that in the insurance sector, *"brokers will worry, because intermediaries are the first to get it … Brokers need to be providing a valuable service if they want to maintain relevance. Where the broker is a drag, they shouldn't exist; where they provide a necessary service, they should flourish."*
- **Adverse selection and the challenge to risk pooling**. Several emerging technologies have the potential to help insurers better evaluate and price risk, but have the downside of undermining the insurance business model. One director observed, *"When it comes to the pool for writing business, that's the way it started, helping each other if someone had a big loss. I can do risk and asset management for one person, but this leads to the idea that good risks will stay out and bad risks will be impossible to cover. That goes against the whole insurance model of helping each other."*
- **Removing friction from the system.** Participants noted that emerging technologies have the potential to lessen the friction created by information asymmetries and other inefficiencies in the system. One director called that information asymmetry, *"the cornerstone on which banking and insurance are built"* and said that *"the flow of information is changing the way business models are working."* Another participant put it bluntly, saying, *"Taking friction out will decimate the insurance business model."*

# Cyber risk continues to grow as risk management and governance try to catch up

Virtually every summit participant said cyber risk is among the top three risks for their firms. More than any other aspect of data governance, cyber risk and information security are driving board activity around data and information. During the last five years, companies and their boards have invested a tremendous amount of time, energy, and financial resources in improving cyber risk management. In 2016, some of the largest financial institutions spent as much as $500 million on cybersecurity efforts, in some cases doubling expenditures from prior years.[37] Despite this investment, one director spoke for many when he admitted, *"After all of this, I do not know that we are safer."* No one yet thinks that cyber risk is effectively managed and governed. In fact, when asked who believed boards were managing cyber risk effectively, not one summit participant raised their hand. Evidence suggests that directors are right to remain vigilant. The financial services sector has been the most targeted sector for cyber attacks,[38] and the cost of attacks continues to climb. In 2017, some of the most damaging attacks succeeded in paralyzing large global companies and governments resulting in individual company losses of several hundred million dollars. [39] As the nature of the threats continues evolving, so too do the potential vulnerabilities as financial institutions, their suppliers, and their customers implement new technologies and increase the surface area for attackers.

*"After all of this, I do not know that we are safer."*

– Director

Summit participants outline three main causes for the uniquely challenging nature of cyber risk:

- **The nature of the threat is dynamic and growing.** With increasingly sophisticated cyber villains including nation-states and criminal organizations, often attacking with tools that were once the sole property of national espionage agencies, financial institutions need constant vigilance across the entire organization.

- **Governance of cyber risk remains a work in progress.** Boards are still trying to define their role in oversight of cyber risk. Stakeholders, including regulators, are calling for improved cyber oversight—and boards want to provide it: they would like to be sure their firms are doing everything possible to protect customers' money and information. To understand the risk and their role better, boards are calling on experts and in some cases creating specialized subcommittees. Yet, getting cyber risk management and governance right is particularly challenging. When even minor breaches can have unforeseen consequences, and when major breaches can have massively damaging and even systemic impacts, how do firms set a risk tolerance for cyber? And how do they measure and size the risk when the reputational and other impacts could be greater than the impact of a breach itself?

## The nature of cyber risk is dynamic and growing

Cybersecurity first emerged in network discussions around 2011. At that time, many directors who lacked technical expertise noted that they felt completely out of their depth, and that they struggled to understand what the information they were receiving about attempted, prevented, and successful cyber attacks said about their firms' defenses. Cyber experts could provide rudimentary frameworks, such as simple breakdowns of attacker types—vandals, "hacktivists," and saboteurs, spies, thieves, etc. These helped boards at least characterize the problem, but not to do much about it. Risk managers, at the time, spoke of frustrations in their efforts to size the risks facing their institutions, to understand the likelihood and potential impact of a significant breach, and to determine what tolerance, if any, their institutions should have for cyber risk.

In the intervening years, financial institutions have put a tremendous amount of time, attention, and money into cybersecurity. Boards, risk managers, and other executives are more knowledgeable and are asking better questions. The more they know, however, the more they become aware of the extent of the challenges facing their institutions. Despite huge investments, and despite intensive learning about cybersecurity, few directors are confident that they have mastered oversight and governance of this risk. Most leaders agreed with one participant who said, *"People are dramatically more informed, but it's changing so quickly that this is not a subject someone is ever going to master."*

Non-executive directors may not need to become technical experts, but several participants insisted that boards understand who their principal adversaries are. Knowing whether an attacker is a nation-state, a criminal

gang, or a 'hacktivist'—a cyber villain intent not on theft or random damage, but on promoting a political or social cause—and knowing at least something of the attacker's motives will shed light on the attack method and on assets the attacker may be pursuing. It can help inform where to focus security efforts and investment in capabilities. A participant said, *"What risks are we talking about? We tend to lump them together, but there are distinct threats. External adversaries in cyberspace, fraud, insider threats, physical security, business continuity, accidentally emailing firm information out."*

*"What risks are we talking about? We tend to lump them together, but there are distinct threats."*

– Participant

A CISO further described what boards should know about their attackers:

> *What do I expect you as a board to understand? Number one, who are your adversaries? Are nation-state actors going after you? They have more sophistication, time, and resources. If you worry about theft—it's the old story of I don't have to outrun the bear I have to outrun the person next to me. If they are after money, you only have to be better than your peers. But, if they are after something particular, you have to outrun the bear. You should ask management, 'What are top three-to-five criminal gangs after us, and what are their techniques?' I don't care about the answer—just that management has an answer and that they've thought about it. Finally, information about hacktivists and potential insider weaknesses in the firm. You want that kind of information into what you are facing.*

*"I don't care about the answer—just that management has an answer and that they've thought about it."*

– CISO

## Advanced methods are spreading

The first six months of 2017 did little to allay director concerns about cybersecurity, and many experts suggest that the world is entering a more destructive phase. The headline-grabbing attacks originated in new locations and used new methods. They tended to be viral, rather than focused, creating greater potential for collateral damage. Some used state-sponsored technology that is among the most sophisticated available. In several cases the intention was to destabilize entire political systems rather than simply to steal secrets or to harm specific entities. *Appendices A and B provide more detail on recent attacks and evolving and worrisome features of the current environment.*

## Advanced methods are spreading *contd.*

- **State-sponsored exploits.** Experts' greatest concerns are with nation-state or state-sponsored actors. They have the resources and technology and operate with virtual impunity. It is difficult for one state to react to cyberattacks sponsored by another state without escalation and unpredictable consequences. As a result, one expert cautioned, ***"The cavalry is not coming."*** Firms must be responsible for their own security and should not expect governments to protect them from other nation-states. Government organizations have been engaged in cyber warfare for many years, but recent exploits have been well documented and more directly attributable than past attacks. Motives include economic and military damage, political influence (e.g. electoral interference), and theft of government, military, and commercial intellectual property. Governments must weigh trade considerations and decide whether putting pressure on a country, for example through financial sanctions, could actually make future attacks harder to detect.
- **Proliferation of advanced cyber weapons.** In August 2016, a group known as the "Shadow Brokers" claimed to have stolen technology from the US National Security Agency. They subsequently used a digital weapon in two of the most notable attacks of 2017 to date – WannaCry and NotPetya. Experts continue to track not only the dissemination of state-level technology but also the expansion of profitable cyber attack-for-hire services and even services to advise would-be cyber villains. One forum that was taken down recently was owned by two teenagers and known for its helpful customer service and inexpensive subscription model, with packages ranging from $19.99 to $199.99 per month.[40]

**Advanced methods are spreading *contd.***

- **The spread of ransomware and the advent of destruction-of-service (DeOS) attacks.** By now, firms are familiar with the threat of ransomware attacks, which encrypt data and files on infected computers and then demand a payment, often in untraceable cryptocurrencies such as bitcoins, for the digital key needed to unlock the files. If organizations refuse to pay, the keys are typically destroyed, rendering the files permanently useless. One research report suggests that some firms are now holding bitcoins in reserve in the event of such an attack.[41] Ransomware is now regularly deployed by actors, including criminal enterprises, terrorist groups seeking additional resources, and nation-states. Ominously, several recent attacks that appeared at first to be ransomware proved to be aimed at permanently disabling the target institution—so-called DeOS attacks. Instead of demanding ransom, these attacks destroyed original data, backups, and safety nets, rendering recovery almost impossible. To date the motivations for DeOS attacks appear largely political; destruction is intended to cripple adversarial institutions and governments. If these attacks are not well controlled, they have the potential to inflict tremendous collateral damage.
- **Internet-of-things (IoT) botnets and distributed denial of service (DDoS).** DDoS is a familiar form of cyber attack, but recent attacks have made use of tools able to commandeer new types of devices, including IoT devices and mobile phones, exploiting vulnerability in these less secure devices or creating seemingly harmless mobile applications, making detection very difficult. [42]

## Governance of cyber risk remains a work in progress

Directors are looking to improve their ability to assess security and resiliency efforts and to do a better job at measuring progress. One bank director expressed the tension felt by many: *"Cyber is top of mind for everybody. But it is tough to tackle. How do you come at it from the board's perspective and understand what best practices are? No one has done a really good job of outlining the board's role, what accountabilities it has, what is really best practice for oversight."* As a subject matter expert asserted, *"No board, or very few, have really cracked the code of governance in this space."*

## Regulators are putting additional pressure on boards

*"If we as regulators try to prescribe the way to tackle these things we will fail, … We should be focusing on outcomes"*

– Regulator

As noted in the first section of this *ViewPoints*, regulators have been pressing for greater board attention, in some cases via formal rulings, like those from the New York Department of Financial Services, or the rules jointly proposed by the Federal Reserve, OCC, and FDIC in the US. Some supervisors are calling for greater attention to cyber risk management at the board via supervisory letters, including in the UK. Some participants welcome the attention and the benefit of having to demonstrate what firms are doing to protect themselves. Others worry that regulatory attention may create more of a distraction, leading to *"long checklists"* that add little value. The standards demonstrate a new focus for regulators: a participant noted, *"Previously, cyber regulation was all about prevention. This is about governance models."* A director said, *"Everyone is investing a lot, communicating with security agencies, participating in industry initiatives. As a director, what more can I really do than continue to press management to be sure we are doing everything we reasonably can?"*

One summit participant observed, *"As soon as something pops up as part of the regulatory regime, the half-life of the related control goes down dramatically. Attackers become aware of the regulatory requirement, so you have to do something more and look for unique and unexpected capabilities."* A regulator acknowledged, *"If we as regulators try to prescribe the way to tackle these things we will fail, we don't have the expertise. What we should be focusing on outcomes … If we focus on a compliance approach, we will all fail."*

## Boards are still working on defining effective oversight

*"This is not a risk where you set a tolerance—there are too many unknowns, there is no data out there, we are guessing."*

– CRO

Recent years have brought an increasing focus on operational risks in financial institutions. Cyber risk is among the most challenging to quantify, monitor, and oversee. As a result, financial firms are adapting approaches and boards are refining the structures and information they need to be effective. Participants discussed the following areas of focus to improve governance of cyber risk:

- **Establishing a cyber risk tolerance.** As with conduct or compliance risk, the notion of an appetite, or even a tolerance, for cyber risk can seem challenging and counterintuitive. A CRO cautioned, *"This is not a risk where you set a tolerance—there are too many unknowns, there is no data out there, we are guessing. In the cyber world, it's all a guess, so you can't say you have a tolerance. The appetite is that we don't want to have our share price plummet because we are deemed to have been derelict in responsibilities."* Because cyber risk is part of doing business, however, one expert asserted, *"The most important decision for a board is what is the risk*

*"If you want to reduce risk in half are you willing to double your investment? How do you know where to draw line between mitigation and acceptance?"*

– Participant

*tolerance or acceptance that you are willing to take … This allows you to make better decisions. If you want to reduce risk in half are you willing to double your investment? At some point, it is not worth doubling the expense to halve the risk. So, how do you know where to draw line between mitigation and acceptance?"*

A CISO outlined how boards might go about establishing a cyber risk appetite: *"There are two ways you can approach risk appetite. One is to roll up cyber risks to create a strategic metric. The second is to create granular tactical metrics. There are benefits to that approach, because they are fully quantitative. I've never seen a strategic metric without a heavy dose of subjectivity, and with that much subjectivity it loses value. I would rather have granular, tactical metrics and appetites bound to those metrics. It doesn't give you a complete picture, but if you get a little bit more clarity, it can be enough to drive change."*

- **Prioritizing security efforts.** Because cyber breaches are inevitable, and there are limits to the prevention investment that firms can make, many firms are shifting from zero tolerance to the notion of acceptable losses, which requires a clear hierarchy of information assets. Industry leaders increasingly recognize the need to prioritize which risks must be prevented, acknowledging that some need to be accepted, mitigated, or transferred through insurance.[43] One CRO described this as moving down from the crown jewels to the areas where, *"while you don't want to get attacked, it is more acceptable from a tolerance perspective to have vulnerabilities."* The CRO continued with an analogy: *"Suppose there is a fence around your house. Can they get through the fence? The locked front door? The safe in the basement? Getting through the fence may happen every day, but they should never get into the safe."*

*"In 2014, boards were taking on oversight of the risk and they wrote a blank check. Now they wonder when they get to close the wallet"*

– Executive

- **Understanding the long-term investment needed.** A director asked, *"How do you determine whether to spend the next $100 or $200 million? What difference does it make? Or is it a management decision where they can try to define, 'if I spend x, it would dramatically improve our posture?'"* An executive observed, *"If you go back five years, a lot of large financial institutions 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."* Another expert said, *"In 2014, boards were taking on oversight of the risk and they wrote a blank check. Now they wonder when they get to close the wallet, but there are two things to remember: one, we are*

*dealing with 20 years of underinvestment, and two, the bad guys are evolving as fast as we are, so you have to run faster just to stand still."* The result, another participant said, is that, *"financial institutions need to spend as much as they can manage financially,"* and boards need to accept that there will be some waste in that investment, but some trial and error is needed.

- **Focusing on response and resiliency.** One expert said that boards, after reading about a breach occurring elsewhere, often ask, *"Are we protected?"* when they should be asking, *"How do we assess the risk if that were to happen to us and what are our capabilities to deal with that risk? The question is not, are we protected, but what is the risk and what are our competencies to deal with it?"* A critical part of security frameworks and regulatory rules is an emphasis on resilience and recovery. One participant pointed out, *"Security and resiliency are two different things … There's prevention, like protecting the crown jewels, and then there's if you have a system outage, making sure you have redundancy, etc. That's really important—how fast can your systems come back up?"* Many boards now have contingency plans, setting out the steps their firms need to take in the event of a breach.

> *"The question is not, are we protected, but what is the risk and what are our competencies to deal with it?"*
>
> – Participant

A participant pointed out, *"With [the breach at] Equifax, the real damage was in how they responded."* One expert suggested that boards need to clarify their response goals before an attack takes place: *"What is your objective in incident response? Is it to do right by the customer? Catch the bad guys? Reduce the likelihood of disclosure? This is an important board-level conversation."* There are important tradeoffs for boards to consider. Another participant said, *"The longer you wait to inform stakeholders about a breach, the more you may be able to find out about the attack, but boards need to monitor and understand the tradeoff between gaining a more complete picture and responding quickly."* Following a significant attack, the board has a valuable role to play in helping to determine what information should be released to the public and when, and to be sure the interests of the customer are prioritized. A participant observed, *"The calculus on what you say or not is complicated, but the evidence suggests that doing right by customer leads to the better outcome in the long run."* A director noted, *"In the situations where the customer was poorly informed by the company about what had happened, the boards had little involvement and were themselves poorly informed."*

## Refining the ability to measure and monitor cyber preparedness

Conversations with directors and executives from across financial services reveal a widespread desire for better tools—frameworks, checklists, dashboards, or lists of questions—to help boards provide effective oversight of cyber risk. A director described the fundamental challenge they are trying to address: *"What is the scorecard so that the board can see whether we are getting ahead of the bad guys or behind?"* Commonly used tools include: The Framework for Improving Critical Infrastructure Cybersecurity of the National Institute of Standards and Technology (the NIST Framework) and the 27000 family of standards from the International Organization for Standardization and the International Electrotechnical Commission. However, these standards are highly detailed, technical, and aimed at management and cybersecurity professionals rather than board directors.

*"We are choosing tactical metrics that we think have strategic implications because we don't have good strategic metrics."*

– CISO

Despite a number of frameworks targeting boards in recent years, directors still describe a lack of concrete guidance on how to satisfactorily discharge their duties and what constitutes good practice in the context of complex financial institutions. A recent EY study concluded that board members "find that their prime [cybersecurity] challenge is obtaining relevant, objective and reliable information, presented in business-centric terms. This affects board members' ability to understand the risks facing their organizations and evaluate management's response to these risks."[44] One CISO acknowledged, *"There are no widely used strategic metrics, only fairly tactical ones. This is part of the work that needs to be done. We are choosing tactical metrics that we think have strategic implications because we don't have good strategic metrics."*

Several ideas emerged regarding the kind of metrics and information boards need:

- **Attempts to quantify, without missing the forest for the trees.** A CISO said, *"What I give my board is some subjective math on vulnerabilities—the number and potential severity, how many security updates have we not finished, and I assign a weight that is subjective and I can tweak. It is not a risk score, but a vulnerability score compared to how valuable the asset is."* Another expert suggested that boards push management to use simple ratings: *"You can ask them to assign the risk a score of 1 to 10, then map that to capabilities measured from 1 to 5. That allows you to look at how they pair up and assess what we need to invest in order to move from 3 to 4."* These risk indicators can be helpful, but a participant cautioned against boards and security teams becoming too focused on metrics: *"When board*

*members ask a question about a metric like that, that's where all the energy goes, so if you ask about those metrics, you are impacting the organization's focus. And there are other things that need to be done. Those metrics suggest actions that need to be taken. You risk over indexing the security team."*

*"I need users to be sensors rather than bricks in a wall. I just need one to report it."*

– CISO

- **A range of indicators that can inform board questions.** A director noted, *"Boards have to know what the right questions are and to make sure what they are being presented with is focused enough to address the right risks. This means having the right questions to probe one level below what you are being presented. What we need is something really specific. We are all getting reporting, but the question is, are we getting the right report?"* Participants listed some indicators of broader preparedness for boards. Among them: how quickly systems are being patched to ensure they are up to date; how many "pipes" or points of connection the company has to the internet; the frequency and effectiveness of internal training; the results of tests to see what percentage of users click on phishing emails and the percentage that report it. As a CISO said, *"I care less about the percentage that clicks than the group that reports. I need users to be sensors rather than bricks in a wall. I just need one to report it."* Other indicators include the results and frequency of independent penetration testing; and internal audit findings and the time it takes to address them.
- **Data that shows trends rather than snapshots.** One director said, *"For every new meeting, I don't really care to see a dashboard that shows what we've blocked, how many attacks we've gotten. That measure is not as important as the trend line or if we are seeing more hacks."* Unfortunately, even trend data can be difficult to interpret. One executive reported that his company was pleased that his firm was improving on measures related to phishing attacks—until their internal testing team crafted a better email that tricked a far greater number of employees.
- **Measures of how the organization is engaging with outside groups.** Improved, faster information sharing is often identified as a key step to improving cybersecurity. Outside groups include industry consortia, security experts, and government agencies. *"I want to know who we are talking with and how often, and what is the result,"* said one director.
- **Goal-based metrics.** As firms set additional goals related cybersecurity and resilience, such as the acceptable amount of downtime from an attack, boards are keen to understand how close their organizations are coming to

meeting those goals and, more importantly, whether they are the right goals in the first place.

- **Improved ability to benchmark against industry peers**. Several directors acknowledged the importance of benchmarking to understand relative capabilities, though they acknowledged that this can be difficult to do. The nature of different businesses, the number of potential entry points, the nature of the assets being protected, and a range of other variables make comparisons difficult. But many directors are still looking for comparative data to get a better sense for how their defenses stand up to peers.
- **More systematic collection of lessons learned.** *"The postmortem is important. If we failed, why did we fail? If we managed the risk well, why did we manage it well?"* Several directors noted the importance of reporting on lessons learned from recent experiences either within the firm or from other firms' experiences. After and event, one participant said auditors can help assess whether the initial risk assessment was correct, and if not, why.

## Clarifying organizational structures and processes

*"Line two is strong on quantification of risks, which traditional cyber has been weak on."*

– Executive

Many leading financial institutions are still grappling with fundamental questions about cybersecurity as a function, how it is organized, and how best to structure effective board reporting structures. One executive underscored this challenge, asking, *"Where does cyber sit? Are there three lines of defense? What are the three lines? How are the lines of responsibility defined? What are the reporting lines? Who is involved in cyber oversight? Is it diffuse or consolidated governance? There are some big questions."* Most organizations now have aspects of cybersecurity embedded in different lines—the IT organization in the front line, the risk function in the second, and cybersecurity expertise in the audit function in the third line to be able to test effectiveness.

In brief, the first line of defense is in the business units, which are responsible for assessing and monitoring risks associated with their business activities and for ensuring that they implement procedures that are in keeping with the organization's cyber risk framework and risk tolerance. The second line rests with the enterprise risk management and compliance functions, which analyze cyber risk at the enterprise level and report on the implementation of the company's cyber risk management framework. The third is internal audit, which provides assurance that the cyber risk management framework complies with applicable regulations and is appropriate for the firm's size, complexity, systemic importance, and risk profile. The audit function also incorporates assessment of cyber risk management into the overall audit plan.[45]

One executive said, *"If you have a cyber expert in the second line, the most value comes from a focus on quantification and prioritization among risks. Line two is strong on quantification of risks, which traditional cyber has been weak on. Having done that for line two, you can drive more changes of behavior from the business side."* Having some cyber risk management outside the direct reporting line to the CIO offers some benefits: *"It is fine to have the CISO report to the CIO, but someone else who is accountable for information security should not report to the CIO. You need an alternative avenue for information to go up the chain. There are examples of CISOs reporting to the general counsel, the CFO, the CRO, or the COO. It partly depends on the culture of the organization."*

*"You can have this whole conversation without ever mentioning technology. It's a risk management discussion."*

– Participant

Spreading reporting and accountability can also allow for better delineation of responsibilities. An executive illustrated the challenge in defining the role of the cybersecurity function, saying, *"Let me tell you some risks under my purview or that we've discussed being under my purview: Fraud, business continuity, someone accidentally emailing firm information to the wrong recipient, etc."* While some participants argued that the CIO should ultimately be accountable for cybersecurity, since IT ultimately creates cyber risk, most financial institutions are integrating cyber into the three lines of defense model as well.

## Adapting board committee structures and accessing additional expertise

An ongoing debate in network discussions involves board composition and expertise, particularly related to technology. A cyber expert was blunt, *"My advice to the board: You're never going to understand this stuff, you need to get expertise on the board."* Some boards have brought on directors with technical, or in some cases, even highly specialized cybersecurity expertise, for example one bank added the former deputy director of the National Security Agency to their board. In contrast participants generally share the concern expressed by one who said, *"It is very dangerous to rely on one person, you think to yourself 'who am I to question them?' And they end up being the only person in the room with a viewpoint."* As one director put it, *"We are not experts in a lot of things, and we manage to figure it out. So, you just have to get educated."* Another participant said, *"Boards should not be despondent. You can have this whole conversation without ever mentioning technology. It's a risk management discussion."* Most boards are adding limited technical expertise, but relying more on third parties to share information on a regular basis.

Boards are engaging third party cybersecurity experts on a regular basis. Some are experimenting with bringing cybersecurity advisers into special committees or creating advisory committees to the board. In some cases, experts are now permanent members of board subcommittees dedicated to the topic or to related technology issues. A director asserted, *"You can't have a different board member to understand every technological development. It is more about having access to experts."* In some cases, different experts from different outside organizations are brought to provide directors with a broader view. In others, firms have agreements with specific cybersecurity firms or experts who regularly advise the board. One executive said, *"If you are on a board, how do you know if you are industry leading in this area? The best answer is a third-party assessment. The evaluation can tell you where the institution is and where it came from. Then you ask, what is the next frontier?"*

*"We will never solve it … We manage risks to an acceptable level. We are not there now, but the goal is not zero."*

– Executive

For some boards, the structure of cybersecurity oversight is still evolving. While the overall responsibility for managing cybersecurity falls on the entire board, boards organize themselves in a variety of ways to get the job done. Among participants, responsibility for in-depth review varies among the audit, risk, or technology committees, where they exist, or some combination of these committees. Some boards have established subcommittees of the board focused exclusively on cybersecurity or on related aspects of technology risk.

A recent study of US boards found that most boards assign primary oversight of cyber risk to the audit committee, while 11% assign responsibility to the risk committee.[46] Those who entrust the audit committee with the task often say that audit's familiarity with oversight of controls gives it the right tools and perspective to oversee cyber risk. *"In the audit committee, what we do is all about process and controls, so our mind-set and day-to-day work is such that cyber fits well—because it's always about process,"* said one director. One director reported that her board *"shares oversight between the audit committee and the risk committee. A lot of things cross over, and we pass information. It's pretty fluid. When the audit committee starts getting into risk issues, we park it and pick it up with the risk committee. On cyber, a lot of issues will be shared between risk and audit."* Increasingly, the range of issues involving technology is causing more boards to create technology committees, which will often meet with the risk committee for discussions on cybersecurity.

***

An executive reminded summit participants, *"We will never solve it, like crime, or spying. We manage risks to an acceptable level. We are not there now, but the goal is not zero."* The Summit discussions demonstrated that while cyber risk has been on board agendas for years, risk management and governance are still relatively immature and will continue to evolve. The focus over the course of the summit on a broader set of issues related to data governance, including privacy and the implications of emerging technologies also suggest the focus on information security in all its forms will continue to be a priority for boards. A director said, *"All signs point to more focus on cyber risk and more investment. When your business is digital, your risks are digital."*

## Appendix A: Notable recent cyber attacks

- **Equifax**. In September, Equifax, the credit reporting firm, announced that 143 million people in the US may have had personal financial data stolen in a cyber breach. According to one analysis, that "accounts for well more than half of all US residents who rely the most on bank loans and credit cards," who "are now at a significantly higher risk of fraud and will remain so for years to come."[47] This demonstrates that the risk is not just from direct breaches of financial institutions, but that financial institutions can be exposed to fraud and financial crime indirectly as the result of breaches elsewhere in the ecosystem, raising questions
- **Energy company infiltration.** A group of hackers, believed to be Russian and known as Dragonfly, Energetic Bear or Berserk Bear, are believed to have hacked into a number of energy companies, concentrated in Turkey and the US. According to one analyst, "They are waiting in case there is some kind of political event, then they have the cyber offensive means," to switch off the power and sabotage computer networks.[48]
- **WannaCry.** In May, this ransomware strain spread to more than 100 countries, affecting public entities, including hospitals, and resulting in an estimated $8 billion in cost.[49] US intelligence agencies concluded that WannaCry was the work of North Korean hackers. The attack exploited a Microsoft vulnerability that had a patch, though many organizations had not applied the patch at the time of the attack.
- **NotPetya/Nyetya.** A month later, another attack spread around the globe. This attack significantly damaged Ukrainian infrastructure, caused business interruptions in a number of sectors, and resulted in hundreds of millions of dollars of damage. While designed to look like the ransomware, NotPetya was a DeOS attack that wreaked havoc in public and private systems.[50] One chief information security officer noted, "It was new and a scary level of risk because it was nation-state technology and it was not controlled. In a situation like this, it is far easier to be subject to collateral damage, whereas before you had to be the target. In addition, in a remote-controlled attack, you have two opportunities to get the attackers: when they enter and when they phone home. Now they may not call home, so you've lost that opportunity." Ukraine has suggested Russia is behind the attack, given the targeting of Ukrainian assets and the timing on the eve of Constitution Day, which celebrates the country's split from the Soviet Union.[51]
- **WireX**. This network, comprising tens of thousands of Android mobile devices across more than 100 countries, was used to launch a number of cyber attacks.[52] It relied on approximately 300 different free mobile apps available via Google's Play store that mimicked innocuous programs.
- **SWIFT**. In 2016, criminals with suspected links to North Korea compromised the SWIFT financial institution messaging servers, resulting in the theft of US $81 million from the central bank of Bangladesh[53]

## Appendix B: Recent reports and frameworks aimed at boards

- Governing Cyber Risk in Financial Services (EY, 2017).
- *Advancing Cyber Resilience: Principles and Tools for Boards* (World Economic Forum, 2017).
- *NACD Director's Handbook for Cyber-Risk Oversight* (National Association of Corporate Directors and the Internet Security Alliance, 2017).
- *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers* (Palo Alto Networks and the New York Stock Exchange, 2015).

## Appendix C: Summit discussion participants

In 2017, Tapestry and EY hosted nine BGLN and IGLN meetings, including the second Financial Services Leadership Summit. In preparation for the summit, Tapestry and EY had more than 65 conversations with directors, executives, regulators, supervisors, policymakers, and other thought leaders. Insights from these discussions helped to shape the summit agenda and inform the enclosed *ViewPoints* documents.

The following individuals participated in discussions for the 2017 Financial Services Leadership Summit:

### Directors

- Homaira Akbari, Non-Executive Director, Santander
- Joan Amble, Non-Executive Director, Zurich
- Mike Ashley, Audit Committee Chair, Barclays
- Norman Blackwell, Chair of the Board and Nomination & Governance Committee Chair, Lloyds Banking Group
- Jan Carendi, Senior Advisor, SOMPO
- Kathleen Corbet, Lead Director, MassMutual
- Nick Donofrio, Non-Executive Director, Liberty Mutual
- Dina Dublon, Risk Committee Chair, Deutsche Bank
- John Fitzpatrick, Risk and Capital Committee Chair, AIG
- Tim Flynn, Non-Executive Director, JPMorgan Chase
- Sheila Hooda, Non-Executive Director, Mutual of Omaha
- Olivia Kirtley, Risk Management Committee Chair, US Bancorp
- Eileen Mercier, Audit Committee Chair, Intact Financial
- Scott Moeller, Risk Committee Chair, JPMorgan Securities
- Nathalie Rachou, Risk Committee Chair, Société Générale
- Dorothy Robinson, Risk and Compliance Committee Chair, TIAA
- Alexandra Schaapveld, Audit and Internal Control Committee Chair, Société Générale
- Bob Scully, Non-Executive Director, Chubb & UBS
- Ted Shasta, Non-Executive Director, Chubb
- Kory Sorenson, Audit Committee Chair, SCOR
- Eric Spiegel, Audit Committee Chair, Liberty Mutual
- Doug Steenland, Chair of the Board, AIG
- Kate Stevenson, Corporate Governance Committee Chair, CIBC
- Katie Taylor, Chair of the Board, RBC
- Joan Lamm-Tennant, Non-Executive Director, Hamilton Insurance

## Executives

- Anthony Belfiore, Senior Vice President and Global Chief Security Officer, Aon
- Colin Bell, Group Head, Financial Crime Risk, HSBC
- Douglas Caldwell, Chief Risk Officer, Transamerica
- Anne Fealey, Global Chief Privacy Officer, Prudential Financial
- David Fried, Advisor, QBE
- Mark Hughes, Group Chief Risk Officer, RBC
- Axel P. Lehmann, Group Chief Operating Officer, UBS AG
- Stuart Lewis, Group Chief Risk Officer, Deutsche Bank
- Linda Mantia, Senior Executive Vice President and Chief Operating Officer, Manulife
- Andy Ozment, Chief Information Security Officer, Goldman Sachs
- Nick Silitch, Senior Vice President and Chief Risk Officer, Prudential Financial
- Al Tarasiuk, Group Chief Security Officer and Group Chief Information Security Officer, Deutsche Bank
- Cathy Wallace, Chief Risk Officer, State Farm

## Regulators

- Gary Barnett, Deputy Director, Division of Trading and Markets, US Securities and Exchange Commission
- Megan Butler, Director of Supervision, Investment, Wholesale, and Specialists Division, UK Financial Conduct Authority
- Beth Dugan, Deputy Comptroller, Operational Risk, US Office of the Comptroller of the Currency
- Art Lindo, Senior Associate Director, Division of Supervision and Regulation, US Federal Reserve System

## Other Participants

- Martin Abrams, Executive Director, The Information Accountability Foundation
- Dante Disparte, CEO, Risk Cooperative; Chair of Business Council, American Security Project
- Marissa Kimball, Palantir Technologies
- Jon Ramsey, Chief Technology Officer, SecureWorks
- Mike Rogers, Former Chair, House Permanent Select Committee on Intelligence, and Director, Ironnet Cybersecurity
- Steve Weber, Professor, School of Information, Department of Political Science, UC Berkeley, and Faculty Director, Berkeley Center for Long Term Cybersecurity
- Marcel Wendt, Founder and Chief Technology Officer, Digidentity

## EY

- Peter Bellamy, Executive Director
- Tom Campanile, Partner, Financial Services
- Shaun Crawford, Global Insurance Leader
- John Doherty, Partner, Information Technology Advisory Services
- Paul Haus, Americas Banking & Capital Markets Assurance Leader
- Gary Hwa, Global FSO Markets Executive Chair & Asia-Pacific FSO Regional Managing Partner
- Adam Lange, Senior Manager, Advisory Services Practice
- Mike Lee, Global Leader, Wealth & Asset Management
- Marcel van Loo, EMEIA FSO Regional Managing Partner
- Ed Majkowski, Partner, FSO
- Mark Manglicmot, Senior Manager, Cyber Threat Management, Risk Advisory Practice
- Ian Meadows, Senior Manager
- James Phillippe, Executive Director and Principal, Advisory Services Practice and Global Cyber Threat Management Competency Leader
- Brett Rogers, Manager, Advisory Services Practice
- Isabelle Santenac, EMEIA FSO Assurance Managing Partner
- John Vale, Principal, Insurance Advisory Practice

## Tapestry Networks

- Dennis Andrade, Partner
- Eric Baldwin, Senior Associate
- Leah Daly, Principal
- Jonathan Day, Vice Chair
- Brennan Kerrigan, Associate

## About this document

### About *ViewPoints*

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.*

### About the Financial Services Leadership Summit (FSLS)

*The FSLS is an annual meeting addressing key issues facing leading financial institutions. It brings together non-executive directors, members of senior management, policymakers, supervisors and other key stakeholders committed to outstanding governance and supervision in support of building strong, enduring and trustworthy financial institutions. The FSLS 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 FSLS discussions 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 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.*

## Endnotes

[1] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L119).

[2] "GDPR Key Changes," GDPR Portal, accessed December 14, 2017.

[3] "GDPR Key Changes," EU GDPR Portal. For more information on the GDPR, see EY, *GDPR: Demanding New Privacy Rights and Obligations Perspectives for Non-EU Financial Services Firms* (London: EYGM Limited, 2017).

[4] HM Government, *FTSE 350 Cyber Governance Health Check Report 2017* (London: Department for Digital, Culture, Media, and Sport, July 21, 2017).

[5] See, for example, Duncan Tucker, "Latin America's Complex Data Protection Laws Not Cause for US Firms to Reshore," *Nearshore Americas*, April 21, 2015; Melanie Bates, "Droit À L'Oubli: Canadian Perspective on the Global 'Right to Be Forgotten' Debate," *Future of Privacy Forum* (blog), April 25, 2017; Julie Seaman, "Latin American Data Export Governance," *Information Accountability Foundation* (blog), August 2, 2017; Martin Abrams, "Europe Sets the Standard—Other Regions Follow," *Information Accountability Foundation* (blog), July 19, 2017.

[6] See Lalita Clozel, "Regulators Doing 'More Harm Than Good' on Cybersecurity: The Clearing House," *American Banker,* June 2, 2017, and Shaun Waterman, "Accountants Join Pushback on Feds' Cyber Rules for Banks," *Cyberscoop,* January 24, 2017.

[7] Keith Button, "New Financial Services Cyber Laws Lay Responsibility on Boards," *Agenda,* August 7, 2017.

[8] Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23, § 500 (2017).

[9] NAIC, "NAIC Passes Insurance Data Security Model Law," news release, October 24, 2017 and Gloria Gonzalez, "NAIC Cyber Security Model Law Hews to New York State's Standard," *Business Insurance*, September 4, 2017.

[10] Enhanced Cyber Risk Management Standards, 82 Fed. Reg. 8172 (proposed October 19, 2016) (to be codified at 12 C.F.R. 30 and 364) and EY, Enhanced Cyber Risk Management Standards for Financial Institutions, Financial Services Regulatory Alert (London: EYGM Limited, 2017).

[11] EY, Enhanced Cyber Risk Management Standards for Financial Institutions, 4.

[12] For more information on critiques of large technology, data, and platform companies, see, for example, Tony Romm, "Tech Companies Fear Repercussions from a New Bill in the U.S. Congress to Combat Human Trafficking" *Recode,* August 1, 2017; Times Editorial Board, "Facebook's Lab Rats, A.K.A Users," *Los Angeles Times*, June 30, 2014; Jennifer Rankin, "EU to Find Ways to Make Google, Facebook and Amazon Pay More Tax," *Guardian,* September 21, 2017.

[13] Navin Suri, "A Bank Is a Data Company," *LinkedIn* (blog), August 28, 2017.

[14] "Legitimate Interest," GDPREU.org, accessed December 17, 2017.

[16] David Reinsel, John Gantz, and John Rydning, *Data Age 2025: The Evolution of Data to Life-Critical* (Framingham, MA: IDC, 2017), 7.

[17] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications* (Basel: Financial Stability Board, 2017), 8.

[18] Dave Gershgorn, "The Data That Transformed AI Research—and Possibly the World," *Quartz,* July 26, 2017; Emil Protalinski, "Google's Speech Recognition Technology Now Has a 4.9% Word Error Rate," *VentureBeat,* May 17, 2017; Matt Weinberger, "Microsoft's Voice-Recognition Tech Is Now Better Than Even Teams of Humans at Transcribing Conversations," *Business Insider*, August 21, 2017; Alison DeNisco Rayome, "Why IBM's Speech Recognition Breakthrough Matters for AI and IoT," *TechRepublic,* March 13, 2017.

[19] David Silver et al., Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm (Cornell, NY: Cornell University Library, 2017).

[20] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications,* 23.

[21] Steve Lohr, "A.I. Is Doing Legal Work. But It Won't Replace Lawyers, Yet," *New York Times*, March 19, 2017.

[22] James Manyika, Michael Chui, Mehdi Miremadi, Jacques Bughin, Katy George, Paul Willmott, and Martin Dewhurst, A Future that Works: Automation, Employment, and Productivity (McKinsey & Company, 2017), vii.

[23] For more information on algorithmic hacking, see Kira Radinsky, "Your Algorithms Are Not Safe from Hackers," *Harvard Business Review,* January 5, 2016.

[24] "Discriminatory Algorithms 'A Scandal Waiting to Happen,'" *InsuranceERM*, November 15, 2017.

[25] Bryce Goodman and Seth Flaxman, "EU Regulations on Algorithmic Decision-Making and a 'Right to Explanation,'" (paper, 2016 ICML Workshop on Human Interpretability in Machine Learning, New York, NY, June 28, 2016).

[26] Will Knight, "The Dark Secret at the Heart of AI," *MIT Technology Review*, April 11, 2017.

[27] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications,* 26.

[28] Martin Arnold and Jane Wild, "Suits Join the Hoodies with Blockchain Push," *Financial Times*, August 24, 2016.

[29] EY, *Better-Working Insurance: Moving Blockchain from Concept to Reality* (London: Ernst & Young LLP, 2017), 4.

[30] Maria Terekhova, "AXA Turns to Smart Contracts for Flight-Delay Insurance," *Business Insider*, September 15, 2017. See also "How Smart Contracts Work," *IEEE Spectrum*, October 2017, 34–35.

[31] Roger Aitken, "R3's 'Blockchain-Inspired' Payments Solution Poised to Interact with Central Bank Digital Currencies," *Forbes*, October 31, 2017.

[32] Allana Akhtar, "The $70 Million Bitcoin Hack Was the 4th Largest Breach in Cryptocurrency History," *Money*, December 8, 2017.

[33] For more on the United Kingdom's Open Banking initiative, see "Open Banking Standards for UK Banking."

[34] For a summary of the Payments Services Directive 2, see "Revised Rules for Payment Services in the EU."

[35] For more information, see Tapestry Networks, Revolutionary Change Is Transforming the Financial Services Landscape, ViewPoints (Waltham, MA: Tapestry Networks, 2016), 6, 10.

[36] Jeff Goldman, "100,000 IRS Taxpayer Accounts Compromised," eSecurity Planet, May 28, 2015.

[37] Morgan, "J.P. Morgan, Bank of America, Citibank and Wells Fargo Spending $1.5 Billion to Battle Cyber Crime."

[38] Steve Morgan, "J.P. Morgan, Bank of America, Citibank and Wells Fargo Spending $1.5 Billion to Battle Cyber Crime," *Forbes,* December 13, 2015.

[39] Christian Wienberg, "Maersk Says June Cyberattack Will Cost It up to $300 Million," *Bloomberg*, August 16, 2017.

[40] Brian Krebs, "Israeli Online Attack Service 'vDOS' Earned $600,000 in Two Years," Krebs on Security (blog), September 8, 2016.

[41] Tom Simonite, "Companies Are Stockpiling Bitcoin to Pay Off Cybercriminals," MIT Technology Review, June 7, 2016.

[42] Brian Krebs, "Tech Firms Team Up to Take Down 'WireX' Android DDoS Botnet," Krebs on Security (blog), August 28, 2017.

[43] Clinton, *Cyber-Risk Oversight,* 4.

[44] EY Center for Board Matters, *The Evolving Role of the Board in Cybersecurity Risk Oversight* (London: EYGM Limited, 2017), 3.

[45] For an analysis of the application of 3LoD to cybersecurity, see EY, *Cyber Risk Management Across the Lines of Defense* (London: EYGM, 2017).

[46] Larry Clinton, Cyber-Risk Oversight, NACD Director's Handbook Series (Washington, DC: National Association of Corporate Directors, 2017), 10.

[47] Dan Goodin, "Why the Equifax breach is very possibly the worst leak of personal info ever," *ArsTechnica*, September 8, 2017.

[48] Hannah Kuchler, "Hackers infiltrate systems of energy companies," *Financial Times*, September 6, 2017.

[49] Suzanne Barlyn, "Major Cyber Attack Could Cost Global Economy $53 Billion: Lloyd's." *Insurance Journal,* July 17, 2017.

[50] Andy Greenberg, "Petya Ransomware Epidemic May Be Spillover from Cyberwar," *Wired,* June 28, 2017.

[51] Ibid.

[52] Brian Krebs, "Tech Firms Team Up to Take Down 'WireX' Android DDoS Botnet."

[53] Aruna Viswanatha and Nicole Hong, "U.S. Preparing Cases Linking North Korea to Theft at N.Y. Fed," *Wall Street Journal,* March 22, 2017.