Bank Governance Leadership Network
ViewPoints

27 July 2015

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

Top and emerging risks: improving identification and oversight of key risks facing large banks

> *There are things we could envision happening that could call into question the very existence of the organization, and they are not quantifiable, nor can the bank put a timescale on them … They make normal business risks seem inconsequential.* – Bank director

Bank boards continue to face increasing accountability for ensuring banks are effectively overseeing risks. Yet, despite improvements in risk identification, reporting, and interaction between banks and their supervisors, participants in the Bank Governance Leadership Network (BGLN) question whether they are truly engaging in the right ways on the key risks that could bring down an individual bank or have a broader systemic impact.

Over several months, culminating with meetings on 9th June in New York and 17th June in London, BGLN participants shared perspectives on the top and emerging risks facing large banks and the financial system and how boards and supervisors can improve oversight. The exchange of perspectives yielded new insights and produced actionable next steps for individual and collective responses.

This *ViewPoints* synthesizes the perspectives and ideas raised in the meetings, as well as in nearly 30 conversations beforehand with directors, executives, supervisors, and banking professionals.[1] A list of individuals who participated in discussions on top and emerging risks is represented in Appendix 1. This document is divided into five sections. The first describes the challenges and opportunities in how boards can improve oversight of top and emerging risks. The remaining four focus on top risks prioritized for discussion by participants. A full list of risks identified by participants is included in Appendix 2.

- **Improving identification and discussion of key risks** *(pages 3-4).* Boards and risk committees spend a lot of time reviewing risk reports and discussing how their institutions are managing key risks. Yet, participants see opportunities to shift the focus of their efforts to be sure they are spending more time openly and informally discussing with management the key risks that are emerging and could impact the viability of their institutions.
- **Emerging sources of systemic risk** *(pages 5-8).* Much effort has been expended globally to decrease systemic risk in banking through new regulatory requirements. But these actions may be creating new risks by limiting the role banks can play in providing market liquidity, and in pushing systemic risk into the world of shadow banking, to which banks still have significant exposure, but which remains opaque and largely unregulated. In addition, participants question whether central clearing parties might be systemically important themselves.

- **The risk from misconduct could be an existential one** *(pages 9-10)*. Banks and regulators have been focused on addressing conduct issues, notably by launching culture reform initiatives and improving accountability and controls. But, participants see persistent risk of legal and financial damage, but also reputational and political risk that could threaten banks' ability to operate in some markets.
- **Increasing strategic risk and potential for disruption** *(pages 11-13)*. Banks are all identifying ways to build more agile, profitable institutions in the face of mounting pressure to improve returns with increasing competitive pressure from multiple directions, including financial technology companies, that threatens margins in core businesses. As the threat grows more quickly than many expected, the urgency to respond is increasing.
- **The unique and growing cyber threat** *(pages 14-16)*. Participants expressed growing frustration with the challenges of managing cyberrisk. As awareness and knowledge about the threat has improved, the nature of the risk continues to evolve, and while the damage from attacks to date has been relatively limited, participants see the potential for long-term threats to emerge in different and more damaging ways. Discussions included necessary actions individual firms can take, and the continued need for improved collaboration among banks, regulators, and governments to protect the system.

Improving identification and discussion of key risks

Since the beginning of the BGLN, conversations on risk identification have been closely aligned with broader themes around risk governance and culture. While participants said they have made significant improvements to their risk identification and escalation processes, they still feel that senior management and boards can improve the dialogue on the real risks their institutions face.

"There are very few human or technical resources available to look at extremely unlikely events."

–Director

Why is identifying and discussing top and emerging risks so challenging?

Participants described the following obstacles to improving board engagement on key risks:

- **The time and resources for discussing emerging risks are limited.** Time and resources are largely focused on reviewing near-term, core banking risks, compliance, and regulatory reporting activities. A director noted, *"There are very few human or technical resources available to look at extremely unlikely events."* Part of the challenge is that managers and boards often allocate time to current, near-term risks that are easy to capture at the expense of more distant and less manageable ones.
- **There is a tendency to avoid the really hard questions.** A chief risk officer (CRO) said two things are very difficult for executives and directors: *"One, asking the genuinely confounding and difficult questions about our strategy, and two, considering what we should really be stress testing. It is human nature to say, 'That will never happen here,' or to forget how painful it was the last time, or to blame someone else. That is why banks go through cycles."* A director elaborated, *"There is a danger that we have all been educated in not being the outlier and to do the same as everyone. It is a herd risk where we accept something is the status quo."*
- **The truly systemic risks are difficult to identify and mitigate in advance.** One participant argued, *"It is a struggle to figure out the process for identifying these top risks and the systemic risk beyond your books. The overall contagion effect is really hard to put your arms around."* Another director concurred, stating, *"It is one of the great challenges to know what is correlated."*

"We know what good looks like: focusing on a smaller number of topics and facilitating a discussion with good, challenging questions without obvious answers."

–Executive

Practical solutions to improving oversight of top and emerging risks

An executive asserted, *"We know what good looks like: focusing on a smaller number of topics and facilitating a discussion with good, challenging questions without obvious answers."* For most, the key to success is allowing the board to *"provide insight and foresight."* A director stated, *"We need a forum for that."* Specific recommendations included the following:

- **Streamline reporting and make risk information usable.** Directors said that *"voluminous"* risk reports are part of the problem. A CRO said, *"Directors often tell me they don't need the whole list of horrors. They say, 'Just tell me, what do I need to know? What are the two to three things that really impact our bank?'"* Another said, *"What we do in board*

meetings is too formal, with a thousand pages in every meeting. We are trying to get it down and highlight the actual issues."

- **Move from formal tick-the-box sessions to real discussions.** Most participants agreed that they continue to spend too much time in formal settings, running through a checklist of risk-related issues. One director noted, *"We need more opportunities for informal discussion where we can speak candidly without worrying that we will send a whole team scrambling for a deep dive."*

- **Focus on a limited number of issues on which board members can provide value.** Directors and executives continue to work toward a balance between being thorough and what most believe is the more effective approach to risk oversight: focusing on a limited number of issues that represent the greatest potential threats and those most amenable to board members' judgment. One CRO said, *"The key is ignoring the press and understanding your own top risks. The top risks that sell newspapers may be different than the risks that could kill your bank."*

> *"The top risks that sell newspapers may be different than the risks that could kill your bank."*
>
> –CRO

- **Ensure boards have access to expertise and exposure to internal and external perspectives.** Boards have sought to broaden their expertise through who they recruit, but they cannot bring on an expert for each technical, operational, and strategic risk the institution faces. There are other options. For example, one director's board now brings in outside experts as full members of special board committees. Others hold board meetings in places near emerging trends – for example, one bank held their recent board meeting in Silicon Valley. Others suggested boards should reach out to more employees deeper in their organization to get more insight into the organization's day-to-day workings.

- **Participate in more informal engagement with supervisors.** Directors and executives said there is still only limited informal discussion between bank boards and supervisors on emerging risks. One director was more critical of the content of the meetings than of their frequency: *"The regulators are starting to engage quite regularly with the board, but are asking more about how things are going rather than giving us information."* Participants agreed that more constructive dialogue requires additional trust.

Emerging sources of systemic risk

Individually, the banks are safer. Collectively, the system might not be.
– Participant

Since the financial crisis, governments, supervisors, and individual banks have been deploying significant resources to monitor systemic risks to the financial system. The financial crisis revealed that neither regulators nor institutions had a clear picture of risks building up in the financial system. In response, central banks have been given a more prominent role in macroprudential supervision and are using their new power to ensure individual firms are less susceptible to systemic risks. BGLN participants are concerned, however, about the movement of risk outside the regulated banking sector as a result. In addition, they see the potential for a liquidity crisis because of the restrictions on banks and the changing roles of market participants, as well as the potential creation of new systemically important financial institutions (SIFIs) in the form of central clearinghouses. The BGLN discussion on these topics resulted in concrete recommendations for actions to prepare for and address these risks.

Fears of a liquidity crisis triggered by rising interest rates

Several investment firm leaders, including the Blackstone Group's Stephen Schwarzman and Larry Fink from BlackRock, have cautioned that a lack of liquidity could cause or exacerbate a financial crisis.[2] Participants expressed concern that when the Federal Reserve ends its quantitative easing program and raises interest rates, a sell-off of assets might be triggered, prompting a chain reaction with unexpected correlations and impacts. One director remarked, *"I'm concerned about second-order unforeseen risks of the unwinding of low interest rates. We will see things that we don't expect in different asset classes."* A supervisor observed, *"I don't think it would take a great deal to break down liquidity, because it can't continue functioning as it should in a crisis, and the probability of a crisis is now higher."*

> *"We will see things that we don't expect in different asset classes."*
>
> –Director

Rising rates may prompt a sell-off with few buyers

A director expressed concerns about retail customer behavior as interest rates rise: *"On the bond side, for example in the ETF [exchange-traded fund] market, do retail customers understand yield maturity? When they see returns go negative for the first time, will they just sell? If so, where does the liquidity come from? Not the SIFIs."* And retail investors are not the only ones that might sell. One participant worried, *"When asset prices change, shadow bankers and investors, in theory, are professional, and these changes in prices will be passed on and stay contained, but I don't think this will happen. The herd instinct will be magnified by the algorithms used by many players. It will amplify the speed and momentum, and they will feed off of each other."*

New regulations tie SIFIs' hands

Participants felt that new leverage and proprietary trading prohibitions have curtailed big banks' ability to act as shock absorbers by buying distressed assets. Many banks have removed themselves from key equity and debt markets, significantly reducing

liquidity in the trading markets, especially for debt,[3] and non-bank players are stepping in to fill the void. A CRO summarized the problem: *"The industry has been firmly trained that size matters. Capital requirements, the leverage ratio, etc., have been driving every bank to shrink their balance sheets. Every firm is trying to keep inventory to the bare minimum. If you go back before the crisis, banks had large balance sheets with an ability to absorb corrections … Volatility now is quite significant."* One participant went even further, claiming, *"We created a procyclical system without buffers on the other side to buy assets. If ETFs, insurers, all say, 'Now is a good time to sell,' large institutions will be sitting there with their hands tied."*

> *"We created a procyclical system without buffers on the other side to buy assets."*
>
> –Participant

Correlations may not be well understood

A director said banks need to be looking beyond what they believe to be their direct and secondary exposures to consider how exposed they could be to potentially correlated risks. Participants expressed concerns about two related issues:

- **Models understate the correlations.** Several participants raised concerns about model risk more broadly. In the event of a liquidity crisis, those concerns could be realized. A director said, *"I am a mathematical modeler by training and I don't believe them."* Another warned, *"Volatility will be higher and the correlations will be higher than the models think."* A related concern is that the value of collateral is overstated and the counterparties may be less robust than expected. As a result, a participant said, *"I worry about the liquidity of so-called liquid assets. I am skeptical about the value of collateral on the trading books in investment banks."*
- **Accounting could exacerbate contagion.** Fair-value accounting has the potential to exacerbate contagion. Participants fear that the vulnerabilities of pension funds, insurers, and others to liquidity issues could be *"magnified into the banks by mark-to-market accounting."* A director predicted, *"[Vulnerability] will move quickly into bank balance sheets, then into capital."*

Though some commentators suggest the risk from liquidity issues is overstated, BGLN participants cautioned against understating a risk that could cause a crisis. An executive asserted, *"I think this is more urgent than regulators think. We are sitting in a big asset price bubble. At some point, it will unwind. It is going to happen."*

Participants urged greater collective preparation

Participants had several recommendations for concrete steps the industry and regulators can take to prepare for the worst:

- **Stakeholders should support constructive dialogue.** Regulators acknowledged the merit of banks' liquidity concerns, but said the refrain from banks often sounds like they are making the case for reversing new regulatory limitations. Industry participants recognized that they need to frame it differently. One director argued, *"We need a positive, more constructive*

dialogue with the regulators. We need to identify positive ways to introduce liquidity as opposed to unpicking regulations."

- **Supervisors ought to lead banks in scenario analysis**. In London, participants suggested that regulators adjust stress testing to include different scenarios. All participants favored candid discussion of how different constituencies can prepare and how they should react in the event of a crisis. Participants suggested collaborative scenario planning involving banks and regulators could help participants think through how a liquidity event could play out for their firms and the system.
- **Market participants should identify *"circuit breakers"* in the network that can stem the spread of problems.** Participants suggested that regulators introduce circuit breakers in extreme market conditions. They recommended that market participants and regulators work together to identify these circuit breakers, what the transmission mechanisms are and how they work.

Central banks may be forced to step in regardless

If a new crisis arises, will central banks intervene to inject liquidity? One regulator was of the opinion that *"central banks won't be lenders of last resort, but lenders of first resort"* because they will have to act to provide market liquidity. Part of the challenge is political pressure opposing government intervention and legal constraints on what the Fed or other central banks are permitted to do. One regulator stated, *"I don't see any other mechanism other than the Fed growing their balance sheet [further]. The problem is Dodd-Frank restrained what the Fed can do. We would need an act of Congress."*

Additional sources of systemic risk: shadow banking and central clearinghouses

Other sources of systemic risk have arisen and remain less regulated and understood. The risks from concentration in central clearinghouses and a shift of assets to shadow banking, which remains opaque and lightly regulated, are of concern to bankers and regulators alike:

- **The growth of risk in shadow banking.** At a recent BGLN meeting, a participant claimed that 40% of all global financial activity is now in shadow banking. Some participants suggested this is what policymakers wanted: the risk is out of the banking system and out of the SIFIs. But banks are still exposed: a participant noted that the greatest growth in lending from banks is to non-bank financial companies. Despite increasing attention from regulators and central banks, most regulators, with limited mandates, a lack of resources, and lack of political support, have been unable to do much to increase oversight or to curb or control the growth of shadow banking activities. One regulator acknowledged, *"We have a pretty murky view, yet there are significant risk concentrations because many of these institutions are highly leveraged."* Another regulator outlined the complexities: *"It is harder for regulators or central banks to intervene now. We do stay in contact with shadow bank players, but we don't have powers over them … We could cut off the credit providers, use bank regulation to achieve a market outcome, but I would prefer the banks do that themselves."*

- **Central clearinghouses: the new too-big-to-fail?** After 2008, regulators turned to clearinghouses both to shed light on the $700 trillion swaps market and to ensure losses at one bank did not imperil a wide swath of companies. Critics argue that relying on central clearinghouses shifts the risk to a dangerously small handful of entities. They claim that the collapse of even one clearinghouse could lead to uncapped losses for the banks. One participant complained that banks are required to do business with CCPs and *"have huge concentration risk"* as a result, yet have *"little say on how [CCPs] are run."* One director said, *"The problem with central clearers is they can't be solved with capital because the dollar amounts on intra-day basis are so big."* Another participant said, *"A CCP can't technically fail, but it's who is on the other side that could fail and bring all of us to the table. A lot of volume came out of bank balance sheets and on to CCPs. That is a huge risk that is not transparent to us … If there are big failures, the lights will go out."*

The risk from misconduct could be an existential one

> *It is impossible that in a large bank, someone won't be doing the wrong thing. The fear we have at this point is that we are subject to the pile-on effect and populism will feed those with political interests to take more drastic actions.* – Bank director

Recently, the BGLN has discussed conduct supervision and the need to address culture in the face of growing costs for conduct-related fines and provisions.[4] In the wake of the string of banking scandals, media and regulatory attention on cultural challenges, and increasingly aggressive commentary by senior regulators, some participants expressed a sense of fatigue at the prospect of addressing culture and conduct yet again.

But today's levels of conduct risk – with attendant fines, litigation, and reputation damage – threaten firms' very existence and have even been highlighted as a potential source of systemic risk. At the very least, misconduct could jeopardize banks' ability to operate in certain markets or businesses, with potential systemic consequences. A June report from the European Systemic Risk Board stated, "Misconduct at banks … may damage confidence in the financial system … Financial and other penalties applied in misconduct cases … may themselves entail systemic risks that … can create uncertainty about the business model, solvency and profitability of banks." The report continued, "The consequences of misconduct could be a withdrawal from financial markets and activities by a bank, either forced or on a voluntary basis, such that the functioning of a particular market is impaired, leading to a direct loss of financial services for the end user."[5]

"I would argue there is not a single firm in financial services that can say with confidence that they know the amount of conduct risk they are running."

–CRO

Long-term solutions for a short-term risk

One CRO remarked, *"I would argue there is not a single firm in financial services that can say with confidence that they know the amount of conduct risk they are running or what their tolerance is for it."* Despite all the attention given to conduct and culture, much is out of the organization's control. Another director said, *"With thousands of people in your organization, there will always be someone doing something that they shouldn't."* Policymakers, regulators, and bank leaders have embraced the idea that culture change is the way to improve conduct. BGLN discussions earlier in 2015 focused on how banks can take a holistic approach to addressing culture, a process that will take years.[6] A regulator suggested that banks will need to demonstrate that meaningful steps are being taken.

In the near term, improving oversight and accountability may only highlight isolated bad conduct, making progress difficult to measure and continuing to feed the narrative that banks and bankers are bad and need to be punished or, in the extreme, that large, universal banks inherently produce bad behavior and need to be broken up.

Continued legal uncertainty

The costs of past misconduct have accumulated, and the totals are massive: the total litigation costs for the biggest global banks since 2010 have broken the $300 billion barrier.[7] A new Bank of England assessment concluded that the amount British banks paid in fines in 2015 was equivalent to the amount raised from private

investors to bolster capital ratios during that same period.[8] What's more, there may yet be future litigation costs, even from issues thought to be settled. One participant noted specifically that the UK Supreme Court decision in Plevin v Paragon regarding payment protection insurance *"could open up more claims even among those deemed to be sold fairly in the previous process. The court ruled that high commission charges in and of themselves can render a product as mis-sold."* A director asserted, *"Some of these are very complex cases where there is no law or regulation we have contravened, but that is not limiting regulators and legal authorities from applying new standards to past practices. It could involve massive costs for reviews, lawsuits, and immeasurable make-good payments."*

"We have the tools to go after individuals, and I think we should."

–Regulator

Anti-bank populism and political backlash

Despite some signals that the enthusiasm for fining banks large sums may be waning in some key jurisdictions,[9] participants remain concerned about rising populist anti-bank sentiment. Referring to a recent multibillion dollar US Justice Department settlement on exchange-rate rigging, US Senator Elizabeth Warren wrote in an email, "This is not accountability for Wall Street. It's business as usual, and it stinks … The big banks have been caught red-handed conspiring to manipulate financial markets … but not a single trader is being held individually accountable, and regulators are stumbling over themselves to exempt the banks from the legally required consequences of their criminal behavior."[10] This kind of rhetoric has led participants to contemplate the following possibilities:

- **Increasing individual liability.** A regulator observed, *"No individuals really paid the price for 2008 because the legal standard has to show they committed fraud, not just negligence or incompetence,"* but another asserted, *"We have the tools to go after individuals, and I think we should."*
- **Increasing institutional liability.** While supportive of increasing individual accountability for bad actors, participants are concerned that institutions could be indicted, with potentially grave consequences. One participant argued that some US state attorneys general are moving in that direction and said the possibility that deferred prosecution agreements will become indictments in the future is *"a real risk that is being ignored."* While there was some debate about the extent of the threat, several participants agreed with one who asserted, *"It could kill a SIFI if it escalates too much."*
- **Political pressure to restructure large banks.** A participant asked, *"Is regulatory risk [or] political risk going to tip?"* A regulator suggested, *"We need to celebrate successes, so people are aware, but also acknowledge the bad behavior, demonstrate what is being done to address it, and make sure your people know what they shouldn't do. You are still playing catch-up, and I don't know if you have time before someone says, 'Let's see if we can break up a big bank.'"*

"It could kill a SIFI if it escalates too much."

–Participant

Increasing strategic risk and the potential for disruption

"Banking is one of the least agile industries. We have expensive, old IT systems, expensive structures, and it needs to change, almost totally, in five years." – Director

Over the last seven years, banks have made significant strategic changes. In addition to the regulatory and market changes driving strategic moves, a rapidly evolving competitive landscape is increasingly adding to concerns about the sustainability of bank business models. Last year, Francisco Gonzalez, chairman and CEO of BBVA, predicted that the next 20 years will see the world go from 20,000 "analogue" banks to no more than several dozen "digital" institutions.[11] Others warn that banks are in danger of "just becoming the plumbing" if they don't work out their role in the evolving financial ecosystem.[12]

Despite past discussions on the potential for disruption, the urgency with which participants view the potential risk has heightened. A participant suggested that banks have been too focused on the short term to properly consider long-term business model risks. A director noted, *"The risk meeting agenda is focused on current risks borne by the bank. Things like strategic risks are not being discussed because they won't blow up in your face, but they may cause your business to go away."*

Increasing urgency regarding potential disruption

As a range of new competitors threaten margins or disintermediation from customers, banks are determining the appropriate response. Recent BGLN discussions have focused on the increasing threat of digitally savvy competitors.[13] *"Every second start-up in Silicon Valley is in financial services,"* noted one participant. Other new competitors include non-bank hedge funds, large private equity firms, and asset managers. Large banks' responses are hamstrung by large organizations, cultures developed over many years, processes and systems not designed for the changing market, and limits imposed by regulators and supervisors. Taken cumulatively, these new sources of competition could present real threats to margins in banks' core businesses. Participants described two primary concerns:

"This issue crosses all lines, including relationships to customers, profitability, regulation, and the soundness of these businesses."

–Director

- **Disruption is about much more than payments.** One director commented, *"This issue crosses all lines, including relationships to customers, profitability, regulation, and the soundness of these businesses. A whole bunch of people are out there who think about eating the lunch of the established banks."* One director stated, *"All kinds of people are saying digitization poses an enormous threat in the payment space, but it could be way beyond that."* In one scenario, large, cumbersome banks with high operating costs struggle to compete with innovative, lower-cost, more customer-friendly enterprises. In another, banks are disintermediated from their customers by new intermediaries and customer-facing companies. In a third, digital competition threatens high-margin businesses and currently profitable business practices, such as cross-selling.
- **The threat is emerging faster than many expected.** For years, BGLN participants acknowledged these distant realities, but now the threat feels

closer. *"The threat from emerging competitors is materializing quicker than many of us thought. We used to be quite dismissive,"* admitted one director. *"This is not a problem that is 10 years out; it is coming now,"* said another.

- **Banks are not agile enough to respond quickly.** Several directors lamented the inertia and inflexibility in their systems: *"We struggle to cope with new regulations and old IT systems … and are therefore mainly reactive to new entrants,"* said one. Participants agreed agility concerns extend beyond traditional anxieties about legacy systems. *"It is not just IT systems,"* said one, *"We spend a billion and a half on IT, we have a staff brought up in a particular way, a culture groomed by management, and established systems, which are all in the way. We are hopelessly inadequate when competitors come in and take share."*

> *"In a relatively short period of time, we could be looking back and saying, 'How did that happen?'"*
>
> –Director

One participant predicted, *"There will be big failures. Large amounts of revenue in banking are payment related and will be disintermediated. Research shows that 30%–35% of earnings are at stake on the fee-based side."* Another said, *"The excess in profit is easy for Silicon Valley to extract. The fee-based model is disappearing."* A director warned, *"In a relatively short period of time, we could be looking back and saying, 'How did that happen?'"*

Despite these challenges, it is not all bad news

All banks are under pressure to improve returns. A participant observed that at many banks, *"the cost base is not shrinking as fast as the balance sheet."* If banks are to adapt, they need to understand their business models, where and how they are generating returns, and what they can do to improve the efficiency of their capital allocations and operations. One regulator criticized bank leadership: *"Looking at transfer pricing, structural reform, [and] recovery and resolution planning revealed that when you pick something out, bank leaders don't know how profitable it is or how it is capitalized."* Another observed, *"Most institutions lack real knowledge of the costs or profitability of individual products."*

In spite of these concerns, participants emphasized it is not all doom and gloom. In London, one director argued, *"There is a huge plus in the names of these institutions. It is hard to build that trust. There is quite a lot of inertia on our side."* Another pointed out, *"All of these potential entrants would die to have the information we do."* One director said, *"We should use the scale benefits that banks have. We don't need to be as agile. We just need to be more paranoid and act more quickly."*

> *"Most institutions lack real knowledge of the costs or profitability of individual products."*
>
> –Regulator

Participants highlighted the following strategies to confront digital disruption heads on:

- **Disrupt better than the competition.** One director said, *"Our competitors target the most profitable parts of the value chain. They go for the inefficiencies in the economics, but we know these things better than they do. We should choose what we want to play with and have strategic flexibility."* Others suggested watching market shifts to see where the greatest threats are emerging, then responding accordingly: *"Look at an area*

like payments. We can see Apple is targeting it and competing with limited risk, while extracting a rent. In peer-to-peer, competitors are attacking the intermediary subsidy that banks take. We can see where the big moves are and where they are coming from." With this insider view, bank staff should think like the innovators. A BGLN participant commented, *"Boards should be encouraging management to test, innovate, partner, and explore. We need our people working with customers on these things to understand what they want."*

"Rather than being good at a lot of things, we need to be great at a few."

–Director

- **Refocus core business strategies**. Banks may need to drastically alter practices that have become commonplace. *"Banks have to get out of businesses that are suboptimal,"* said one participant. *"You used to be able to subsidize the non-profitable portions of your business, but not anymore."* One director suggested an even more fundamental change is necessary: *"Rather than being good at a lot of things, we need to be great at a few. It is about focus versus complexity. Focus gets you a huge benefit, and some businesses still benefit from scale, but it is about scale in a product segment or geography."*

The unique and growing cyber threat

Any problem we have with hackers is nothing compared to the system being hacked. Banks should have a handle on day-to-day cyberrisks, but the bigger ones require the government taking a role. – Director

Since 2012, the BGLN devoted a series of discussions to cybersecurity.[14] It is clearly a risk that has emerged, and most institutions have accepted the notion that attacks are unavoidable. Even governments are unable to defend against breaches, as events such as the hacking of the White House computer system in April and the US Office of Personnel Management in June have shown. *"Cyber is not a risk, it is a certainty,"* stated one executive. A director characterized current knowledge of the threat as *"the tip of the iceberg,"* and said the threat is revealed as *"bigger and bigger the more we dig."*

Cyber threats could emerge in more damaging ways than attacks to date

While banks have been aware of the threat for several years, a director noted, *"The things people were worried about four years ago are not the same things they are worried about today."* As more activity moves to digital platforms, the risk only increases. Furthermore, highly publicized breaches like the theft and subsequent publication of information have shown the reputational damage that even "minor" attacks can cause.

Despite numerous public breaches, there has not been *"a billion dollar loss or any period of time with the whole system being brought down."* Should we take comfort in that? A participant suggested that attackers may be patient and that the breaches to date could primarily represent reconnaissance for future attacks or uses of data with potentially more harmful results. A regulator said, *"There have been very serious breaches. How long [the hackers] have been in there is unknown; the data lost is unknown."* Trying to imagine the thought processes of an attacker, one participant said, *"If I was thinking about the long game, I would build a customer information file and use analytics to predict behavior or steal money. The long-term reconnaissance is the same as [many data aggregators] seeking to collect data to monetize the customer."*

> "How long [the hackers] have been in there is unknown; the data lost is unknown."
>
> –Regulator

Increasing supervisory focus

Supervisors are increasingly focusing on ensuring all banks are appropriately prepared. In the United Kingdom, the Prudential Regulation Authority and Financial Conduct Authority have for the first time sent letters to banks with specific questions about their preparedness for cyberattacks. Others are enhancing their capabilities: one regulator took their best internal cyber expert and moved him into supervision. Another participant suggested that regulators establish standards to ensure weak links don't threaten the system: *"Anybody with a license to operate should have these standards. If you want access to critical infrastructure, then you need to have these standards."* Regulators, for their part, questioned whether they can keep up with the changes in the nature of the threats, but acknowledged their role in pressing for improvements and holding banks accountable.

Challenges for risk management and oversight

In past BGLN discussions, risk executives and directors admitted they were struggling with oversight of cyberrisk, with which few had direct experience. In the most recent discussions in London and New York, participants were asked if boards are any better prepared today. One director asked, *"What would a well-prepared board even look like?"* Some participants questioned the ultimate goal. One said, *"You need an objective on cyber. I haven't heard anyone articulate the objective."* Therefore, participants discussed important steps for improving governance of cyberrisk:

> *"[You need to] determine the level of investment required to achieve the level of protection that you are comfortable with."*
>
> –Participant

- **Defining a cyberrisk appetite or tolerance.** One director commented, *"It is a big challenge to develop a risk appetite for cyber. What are the metrics to do this? Most of the information is historical. How do you prioritize and articulate your risk appetite?"* As firms develop and improve systems and move to increasingly digital platforms, participants emphasized that a balance must be struck between customer ease of use and security. This reality makes defining a cyberrisk appetite or tolerance all the more important. One participant said, *"You need a risk appetite for the level of protection, and [you need to] determine the level of investment required to achieve the level of protection that you are comfortable with."* The objective must be to understand where the trade-offs are being made and how they are being managed.
- **Getting the basics right.** A participant asserted that in some respects, *"financial services is as good as it gets"* regarding cybersecurity. But others argued that banks are not even covering the basics. One regulator commented on recently completed reviews of firm-level efforts, observing, *"It showed that banks do not know their IT assets and capabilities. It is at the elementary level where they are finding deficiencies. For example, on things like [software] patch management, they are well behind. These are foundational issues that don't need IT experts to grapple with. It is the opposite of comforting. Basic infrastructure that should be in place is absolutely missing."*
- **Prioritizing investment.** Having increased their spending on cybersecurity, many organizations struggle with deciding if those increases are sufficient and where and how the money can be most effectively invested. One participant said, *"You are investing enough until there is a breach, and then it is not enough."* One bank board reportedly doubled its spending following a major hack. Benchmarking is also difficult, as one participant suggested, *"You shouldn't care what your competitors are spending, the question is how do you spend the right amount in the right ways for my organization?"*

  > *"The crown jewel is the information that shows how all of your data is organized, the map."*
  >
  > –Director

  Deciding where to spend money requires an understanding of what information is most valuable and potentially vulnerable. "Protecting the crown jewels," is an objective, and one director argued, *"The crown jewel is the information that shows how all of your data is organized, the map."*
- **Defining success.** Some suggested that directors simply need to ensure that management is doing everything possible, recognizing that breaches will

occur. One director said, *"What worries me is the people with more resources who may decide to make me a target. They have a lot more resources than I can possibly aggregate. All I can do is try to make it harder [for them]."* A director stated, *"I have no tolerance for not doing everything possible to protect ourselves, with the caveat that we can offer an acceptable customer and employee proposition."*

Protecting the system through public-private collaboration

While firms acknowledge more needs to be done on at the level of the individual institution, participants agreed that better cooperation among banks and an improved two-way flow of information between banks and regulators is vital. Participants highlighted the following possibilities for collaboration:

- **Pooling of resources.** Participants cited institutions such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) as the standard for collaboration, though some directors and executives complained that information sharing is still not happening quickly enough. The reality is that regulators' and security services' limited resources may be limiting their ability to keep up and share information with the private sector in real time, and there are a limited number of experts and heated competition for them. Some participants suggested banks and the public sector could pool resources to fund cybersecurity efforts where interests are aligned. One director argued, *"Because of the focus on financial services for things like anti–money laundering, it means we are now on the front lines of the war on terror in cyber. Cyberrisk is morphing with geopolitical risk."* One participant commented, *"The knowledge exists between Silicon Valley and professional services to win this, but we don't yet feel like we are in a war."*

"Cyberrisk is morphing with geopolitical risk."
–Director

- **Entering the security-privacy debate.** One participant said the significant cultural divide between Silicon Valley and the East Coast in the United States hinders potential cooperation on cybersecurity. Essentially, there is philosophical split, highlighted by the current encryption debate, with Silicon Valley championing privacy and governmental agencies saying that defense needs should supersede privacy needs.[15] There was a general agreement that the financial sector needs to use its resources to engage with public opinion and restore balance to the debate.

About the Bank Governance Leadership Network (BGLN)

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

About Tapestry Networks

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

About EY

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

Appendix 1: Discussion participants

Over the last several months, Tapestry and EY hosted two BGLN meetings on top and emerging risks in banking and had over 30 conversations with directors, executives, regulators, supervisors, and other thought leaders. Insights from these discussions informed this *ViewPoints* and quotes from these discussions appear throughout.

The following individuals participated in BGLN discussions on top and emerging risks:

Bank directors and executives

- Kathy Casey, Non-Executive Director, Audit Committee Member, Financial System Vulnerabilities Committee Member, HSBC
- Juan Colombás, Chief Risk Officer, Lloyds
- Sir Sandy Crombie, Non-Executive Director, Performance and Remuneration Committee Chair, Audit Committee Member, Nomination Committee Member, RBS Capital Resolution Board Oversight Committee Member, RBS
- Alan Dickinson, Non-Executive Director, Risk Committee Chair, Audit Committee Member, Lloyds
- Laura Dottori-Attanasio, Chief Risk Officer, CIBC
- Dina Dublon, Non-Executive Director, Risk Committee Chair, Deutsche Bank
- Byron Grote, Non-Executive Director, Audit Committee Member, Brand, Values and Conduct Committee Member, Standard Chartered
- Mike Hawker, Governance and Compliance Committee Chair, Audit Committee Member, Nominating Committee Member, Risk Committee Member, Macquarie
- Bob Herz, Non-Executive Director, Audit Committee Chair, Nominating and Governance Committee Member, Morgan Stanley
- Mark Hughes, Chief Risk Officer, RBC
- Phil Lofts, Chief Risk Officer, UBS
- Mike Loughlin, Chief Risk Officer, Wells Fargo
- Alan MacGibbon, Non-Executive Director, Audit Committee Member, TD Bank
- Heidi Miller, Risk Committee Member, Conduct and Values Committee Member, HSBC
- Sir Callum McCarthy, Non-Executive Director, Strategy Committee Vice Chair, Risk Management Committee, Nomination Committee, ICBC
- Tom O'Neill, Audit and Conduct Review Committee Member, Corporate Governance Committee Member, Executive and Risk Committee Member, Human Resources Committee Member, Scotiabank
- Nathalie Rachou, Non-Executive Director, Risk Committee Chair, Audit, Internal Control and Risk Committee Member, Société Générale
- David Roberts, Chair, Risk Committee Chair, Audit Committee Member, Nomination Committee Member, IT Strategy and Resilience Committee Member, Nationwide
- David Sidwell, Non-Executive Director, Risk Committee Chair, Governance and Nominating Committee Member, UBS
- Alan Smith, Global Head, Risk Strategy, HSBC
- David Stephen, Chief Risk Officer, RBS
- Kate Stevenson, Non-Executive Director, Audit Committee Member, Corporate Governance Committee Member, CIBC

Bank directors and executives *contd*

- Katie Taylor, Chair, RBC
- Richard Thornburgh, Risk Committee Chair, Audit Committee Chair, Chairman's and Governance Committee Member, Credit Suisse
- Alexander Wolfgring, Internal Controls & Risks Committee Chair, Remuneration Committee Member, UniCredit
- Tony Wyand, Internal Controls and Risks Committee Member, Remuneration Committee Member, UniCredit

Regulators, supervisors, industry groups

- Ron Cathcart, Senior Vice President, Enterprise Risk, Financial Institution Supervision, Federal Reserve Bank of New York
- Lyndon Nelson, Executive Director, UK Deposit-Takers Supervision, Bank of England
- Marty Pfinsgraff, Senior Deputy Comptroller for Large Bank Supervision, Office of the Comptroller of the Currency
- Todd Vermilyea, Senior Associate Director, Division of Banking Supervision and Regulation, Federal Reserve System
- Steve Weber, Center for Long-Term Cybersecurity, UC Berkeley

EY

- Ian Baggs, Global Banking & Capital Markets, Deputy Leader, Financial Services
- Steve Holt, Head of Cybersecurity for Financial Services
- Ted Price, Advisor, Risk Governance
- Isabelle Santenac, EMEIA FSO Assurance Managing Partner
- Bill Schlich, Global Banking and Capital Markets Leader, Financial Services

Tapestry Networks

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

Appendix 2: Complete list of top and emerging risks identified

Type of risk	Concern/potential impact
Market risks	
Changing interest rates	Changing interest rates could cause serious disruption in financial markets. Participants expressed concerns around the end of quantitative easing in the United States and the looming interest rate hike. Specifically, they questioned whether the authorities have the ability to control the rate of the adjustment and cited the risk of a possible liquidity event.
Commodity prices	Significant fluctuations in commodity prices could cause second-and third-order impacts on sovereign bonds, derivative corporate lending, and stress on housing markets in places dependent on oil revenue.
Deteriorating lending standards	Deteriorating lending standards creates increased credit risk as the industry enters a new stage in the credit cycle. Some participants noted a significant deterioration in lending standards across asset classes. Specific concerns centered on the mortgage and auto lending markets, along with punishing levels of US student debt.
European instability	Continued uncertainty over European instability poses major challenges for companies. Anxiety is increasing with the ongoing ambiguity over Greece's economic situation. Meanwhile, the triumph of the Conservative Party in the recent UK election means a UK exit from the European Union (EU) will be put to a referendum, creating new insecurity about the EU's future.
Geopolitical concerns	A range of geopolitical risks may create additional volatility in financial markets. Participants noted the increasing isolation of Russia and the crisis in the Ukraine, the rise of the Islamic State and war in Syria and Yemen, and political instability in South America as examples of risks they are monitoring.
Slowdown in China	A slowdown in China may generate significant headwinds for the global economy.
Operational risks	
Herd risk	Risk management practices may be threatened by potential herd risk, which leads to the acceptance of the current status quo and the lack of necessary action to avert certain risks. A handful of directors mentioned the danger of everyone being trained not to be the outlier leading all organizations and individuals to do the same as others.
Information systems	Lack of confidence in insights coming from information systems could hinder effective risk management. Some directors questioned how to know whether the correct information is coming forward, especially with the biases within institutions.
IT legacy systems	Many firms' existing technology systems are not well suited to respond to the realities and needs of the 21st century impacting their ability to compete. Modernizing and upgrading these systems will require massive investments of time and resources.

Type of risk	Concern/potential impact
Operational risks *contd*	
Model risk	Financial models may be inaccurate, especially in this new financial environment, which may cause firms to fail to capture and identify potential correlations. This includes concerns that regulators' guidelines and requirements start to dominate internal risk management processes.
Offshoring and outsourcing	Increased organizational changes regarding offshoring and outsourcing could increase challenges around maintaining control of processes in these locations.
Reputation	Reputational damage could jeopardize a banks' ability to operate in certain markets or businesses. For many financial firms, reputation risks are directly tied to broader perception issues for the entire industry. For example, the fines and lawsuits the financial sector has racked up create the appearance that the sector has not learned its lesson from the crisis. Many suggested reputation risk is not a type of risk, but an aspect of any risk to which banks are particularly vulnerable in the current environment.
Regulatory risks	
Conduct	Today's level of conduct risk–with attendant fines, litigation, and reputation damage– threaten firms' very existence. Participants continue to cite conduct risk as a primary concern for boards due to the growing level of fines and increasing political/legal uncertainty.
Populism	Rising popular sentiment, which takes a negative view of all corporations, and financial institutions in particular, may lead to new political and regulatory initiatives that impact banks' business models. The current wave is largely the result of the financial crisis.
Regulatory changes	Unrelenting regulatory change causes significant strategic and operational challenges for the sector. Participants continue to wonder where capital model requirements will finally land. They also expressed particular concerns around the standardization of capital models, bail-in provisions, and recovery and resolution planning. Some suggested what is needed is a mature conversation between industry, regulators, and the public on the role of the financial sector within the global economy.
Strategic risks	
Agility risk	Firms may not be agile enough to adapt to environmental change. Banks are hamstrung by large organizations, cultures developed over many years, processes and systems not designed for the changing market, and regulatory or supervisory limitations on their ability to innovate. This risk is amplified by pending digital disruption.
Cyber	Cyber could emerge in more damaging ways than attacks to date. Directors continue to struggle with how to manage and oversee the threat.
Non-traditional competitors	Taken cumulatively, these new sources of competition (digitally savvy competitors, non-bank hedge funds, large private equity firms, asset managers, and peer-to-peer lending platforms) could present real threats to margins in banks' core businesses.

Type of risk	Concern/potential impact
Strategic risks *contd*	
Talent	Firms may struggle to attract and retain top talent impacting their effectiveness as organization. Many questioned why people would want to work at a bank today with all the pressure and challenges. Reduced profitability adds to the problem as it limits the compensation that can be offered. Some directors said finding risk and compliance talent is particularly difficult as many firms are participating in a poaching war.
Systemic risks	
Central clearinghouses	CCPs may present a new systemic counterparty risk. Since 2008, regulators have turned to clearinghouses both to shed light on the $700 trillion swaps market and to ensure losses at one bank do not imperil a wide swath of companies. Critics are now arguing that relying on central clearinghouses shifts risk to a handful of entities. A potential collapse of even one clearinghouse could lead to uncapped losses for banks.
Liquidity	Financial luminaries across the industry are citing liquidity concerns as a potential cause or trigger for the next financial crisis. Essentially, the new and untested regulatory environment could lead to unintended impacts, especially after an event like an interest rate hike.
Shadow banking	As bank regulation increases, more activity, and more risk, will flow to the shadow banking system creating new potential systemic risk. How policymakers will address this remains unclear, and regulators, often hamstrung by limited mandates, lack of resources, or lack of political support, have done little to curb or control shadow banking.

Endnotes

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

[2] See Stephen A. Schwarzmann, "How the Next Financial Crisis Will Happen," *Wall Street Journal,* June 9, 2015, and "Fed's Tarullo, BlackRock's Fink Cite Bond Market Liquidity Concerns," *Today,* June 5, 2015.

[3] Stephen A. Schwarzmann, "How the Next Financial Crisis Will Happen."

[4] Bank Governance Leadership Network, *Addressing Conduct and Cultural Issues in Banking*, ViewPoints (Waltham, MA: Tapestry Networks, 2015).

[5] European Systemic Risk Board, *Report on Misconduct Risk in the Banking Sector* (Frankfurt am Main: European Systemic Risk Board, 2015), 3.

[6] Bank Governance Leadership Network, *Addressing Conduct and Cultural Issues in Banking*.

[7] Ben McLannahan, "Banks Post-Crisis Legal Costs Hit $300bn," *Financial Times,* June 8, 2015.

[8] Jill Treanor, "Banks' £30bn in Compensation Claims and Fines 'Pose Risk to Stability,'" *Guardian,* July 1, 2015.

[9] George Parker, Caroline Binham, and Laura Noonan," George Osborne to Signal End to 'Banker Bashing,'" *Financial Times,* June 5, 2015.

[10] Steven Mufson and Jonelle Marte, "Five Big Banks Agree to Pay More Than $5 Billion to Settle Regulatory Charges," *Washington Post,* May 20, 2015.

[11] Francisco Gonzalez, "Banks Need to Take on Amazon and Google or Die," *Financial Times,* December 2, 2013.

[12] Natalie Mortimer, "Lloyds Bank Digital Transformation Chief – 'We Are in Danger of Just Becoming the Plumbing,'" *Drum,* June 17, 2015.

[13] See Bank Governance Leadership Network, *Leading the Digital Transformation of Banking*, ViewPoints (Waltham, MA: Tapestry Networks, 2014).

[14] See Bank Governance Leadership Network, *Addressing Cybersecurity as a Human Problem*, ViewPoints (Waltham, MA: Tapestry Networks, 2013).

[15] J.D. Tuccille, "Hands Off Americans' Private Information, Tech Industry Tells President," *Hit & Run* (blog), June 10, 2015.