KPMG

Global perspectives on cyber security in banking

A roundtable discussion on the state of cyber security management in the banking sector

KPMG recently brought together a number of our regional global cyber security practice leaders for a round-table discussion of the rapidly-shifting landscape among top banks in some of the most active jurisdictions.

This dialogue revealed much commonality in strategies and issues faced by banks across the continents. Most notably, the banks are among the most mature industries from a cyber security perspective, due to their historically-conservative approach to risk, their consistent, sizable investments in security and privacy safeguards, and their tradition of collaboration within the industry and with authorities. As such, they continue to demonstrate significant investment to address the rapidly evolving, entrepreneurial and determined cyber threat from trans-national, organized crime.

At the same time, banks in the US, Europe and Asia share a common challenge reacting to mounting global, regional and local regulations that can create cumbersome compliance obligations. A prominent example of the new rules: the EU's General Data Protection Regulation (GDPR), which according to many industry observers, will receive very low compliance in the financial services sectors or any industry by the 25 May 2018 deadline.

While these topics suggest a serious escalation of cyber risks posed to the banks, the discussion also spotlighted a promising shift in approaches to cyber risk management. Currently, a number of best-in-class banks are recognizing that cyber security is not purely a 'technology problem' but rather a business challenge that requires business ownership and strategy development, with clear, aligned support by the technology teams. This evolving mindset explained below, suggests a path forward for banks as the cyber security and regulatory arenas grow more complex.

The banks are among the most mature industry from a cyber security perspective, due to their historically-conservative approach to risk, their consistent, sizable investments in security and privacy safeguards, and their tradition of collaboration within the industry and with authorities.

Charlie Jacco
Financial Services Lead,
Cyber Security Services
KPMG in the US

What are the largest cyber information security trends in your region?

Perspective from the USA

Perry Menezes
Banking Lead, Cyber Security Services
KPMG in the US

USA (Perry Menezes): While trends vary by sector in the US, banking is one of the more 'mature' industries when it comes to cyber security. Within banking, there is a notable convergence between cyber, anti-money laundering (AML) and fraud issues, as financial institutions begin to tackle these issues in a more integrated and holistic manner. The banks certainly feel significant pressure to meet regulatory requirements from multiple agencies, and they are taking a closer look at their affiliates as they focus on third-party risk management and cyber issues.

Perspective from Europe

David Ferbrache
Chief Technology Officer, Cyber Security Services
KPMG in the UK

Europe (David Ferbrache): Regulatory risk is also a dominant force in Europe where the GDPR is driving an emphasis on customer consent, meta data management, and a gradual move towards data-centric cyber security architecture. The rise of digital banking demands new more agile, usable and integrated approaches to customer security. Meanwhile, the emergence of open banking and the second PSD2 Payment Services Directive has the potential to transform the finance ecosystem, sparking debate around security capabilities of new players and the consequences of data breaches in those firms.

Within banking institutions, there is a greater management focus on cyber security operations, and revamping Security Operations Centers (SOCs) to create more dynamic defenses and to better leverage cyber threat intelligence. We also note a push for business ownership of cyber, by linking it more directly to business risk, in part to justify the necessary levels of investment, but often to recognize that cyber security has ceased to be a pure technology issue.

Perspective from Asia

Henry Shek
Head of Cyber Security Services
KPMG in China

Asia (Henry Shek): In Asia, while the banks are taking note to the above issues in other jurisdictions, we presently see that the sector is paying close attention to limit exposure to financial frauds committed through technology, in particular potential breaches to corporate payment processing, often known as a CFO scam. Banks are increasing internal controls to detect such frauds, including integration of fraud detection solutions with payment processing systems.

We also observe a greater focus by banks on the cyber risks arising from third-party service providers and connections. Banks are taking actions to evaluate security controls of third-party providers, scrutinizing what data is being shared with outsiders, and even beginning to conduct cyber security simulations that involve testing third-party connections and personnel.

What are the biggest challenges in addressing these issues?

Perspective from the USA

USA (Perry Menezes): Forging a stronger connection between technology and the business is also a theme in the US, since we must help the Chief Information Security Officers (CISOs) recognize cyber as more than a technology issue. Unfortunately, they are often so immersed in 'keeping the lights on' that they aren't fully cognizant of the business side of these issues. While third-party risk is a sizable risk relating to their inter- and intra-affiliates, the banks face a major blind spot in terms of regulatory uncertainty.

Perspective from Europe

Europe (David Ferbrache): Among European clients, it is about finding the right way of having a dialogue with the business about why cyber security really matters and the need to see cyber security investment as integral in order to harness digital opportunities. While insider threat is a serious issue, as noted in Asia, European banks also struggle to manage the increasingly complex ecosystem of third-party service providers, and the dependencies they create. For regulators, they worry about the implications for the operational resilience of banks and the broader financial sector.

Perspective from Asia

Asia (Henry Shek): In Asia, our predominant challenges are sourcing the required skilled security personnel, including finding vendors with robust cyber security services. This is especially true when it comes to finding personnel with a broad set of cyber security skills. This requires individuals with fairly deep technical skills and also a good understanding of the impacts of cyber risks to businesses. Although technology adoption in Asia has increased tremendously in the past few years, the pools of skilled cyber security personnel have not grown along the same pace. As a result, there's increased competition for limited talent.

What best practices do you see among clients in the area of education, training and awareness-raising?

Perspective from the USA

USA (Perry Menezes): To date in the US, we aren't seeing a clear best practice leader. Most of the main players are focused on general training and awareness and very few are digging deeper into cyber education or training.

Perspective from Europe

Europe (David Ferbrache): A number of our clients are achieving good results by engaging the business in developing (and exercising) cyber scenarios to build an understanding of the nature of cyber incidents and their impact on the business. Tailored training focuses on raising awareness of specific threats rather than delivering standard, mandatory training, and even applying gamification to engage their audiences. We also see a positive trend in terms of simplifying security so it is easy to use. For example, flagging external or suspect emails to the user, and allowing 'one click' reporting of suspected phishing.

Perspective from Asia

Asia (Henry Shek): One way that Asian companies are trying to address the shortage of skilled cyber security personnel is through increased attention given to cyber security training and awareness. Apart from providing existing IT staff with cyber security instruction, we see companies recruiting fresh graduates and providing them with on-the-job cyber security training. We're also seeing an increase in cyber simulations with organization-wide focus. Such simulations are aimed at increasing cyber security awareness among senior management and business users, and assessing effectiveness of existing incidents detection and response mechanisms. Typically, these simulations have an element of triggering corporate communication plans and online-based learning activities.

What differences do you see in how medium-sized versus large global banks are addressing cyber security?

Perspective from the USA

USA (Perry Menezes): In general, the larger global banks enjoy both greater funding and better executive-level buy-in to the issue, often with a mindset that they want to proactively get ahead of the cyber issue.

Perspective from Europe

Europe (David Ferbrache): In Europe, the status of bank approaches varies greatly. For example, although large banks are well funded and have sophisticated defenses, they can be quite compliance-centric and may be impacted by their legacy platforms or a sizable shadow IT to manage. There are some small, challenger banks that do security really well because they don't have the legacy infrastructure or diversity of IT environments to deal with. Other small banks show considerable weakness — with under-resourced and skilled security teams with little depth of expertise or awareness at the senior level.

Perspective from Asia

Asia (Henry Shek): Interestingly, while mid-sized banks lack global SOCs, this can actually make them easier to manage centrally, so they can better develop and execute agile cyber strategies. In contrast, large global banks are often very dependent on their global SOC. This can create vulnerability at the local level if in-country teams do not fully understand what the global SOC covers, causing black holes in critical security coverage.

What direction do you see cyber regulation going?

Perspective from the USA

USA (Perry Menezes): While there is regulatory uncertainty directly related to the political environment in Washington, it's clear that all key regulatory authorities have set cyber as a priority. However, with seemingly haphazard enforcement at the moment, banks may be unclear on the urgency with which they should address these issues. For example, while bank examiners are issuing Matters Requiring Attention/Immediate Attention (MRAs/MRIAs), increasingly related to cyber issues, we have not yet seen strong enforcement by supervisors.

Perspective from Europe

Europe (David Ferbrache): We are certainly witnessing a dynamic regulatory environment in Europe with EU GDPR, PSD2 coming into force and increasing emphasis on independent penetration testing through the Bank of England's CBEST scheme or forthcoming European Central Bank initiatives. We also see the UK Prudential Regulation Authority (PRA) focusing more on cyber and operational resilience and the Financial Conduct Authority (FCA) engaging in ongoing discussions about cloud services and associated systemic risk. All of this poses challenges to banking institutions to keep abreast of regulatory direction, adapt their strategies accordingly and allocate the necessary resources to satisfy compliance demands, but without creating inflexible controls.

Perspective from Asia

Asia (Henry Shek): China's centrally-governed China Cyber Law is among the dominant regulatory forces in Asia and its current focus is on requiring data onshoring, or government approval for any data-offshoring. For some clients, it is a challenge to clearly identify where data are housed and they are reluctant to move systems back onshore to comply with the law. In Hong Kong, the banking sector will be impacted by the Cyber Fortification Initiative. However, since this program mirrors the Federal Financial Institutions Examination Council (FFCEC) in the US, most foreign banks are comfortable with its compliance requirements.

What strategies do you see that could help banks navigate these inter-connected issues?

Perspective from the USA

USA (Perry Menezes): One exciting development is some very recent activity by several US-based, global banks to dramatically change the way cyber risk is managed. Typically until now, banks have maintained three lines of defense. You could describe them simply as business/technology (housing the CISO); risk; and internal audit. In this structure, the CISO has largely policed the actions of the business and dictates what the business can and cannot do.

Now, we are beginning to see a 'lift and shift,' by which a dedicated cyber risk organization is created and reports into Operational Risk. By doing so, and scaling up this group, it can develop sophisticated data models to calculate and quantify cyber risk. This ultimately enables the business to 'own the issue' and make sound, strategic decisions about new products, services and channels, and weigh the strategic risks, as they would for other risk categories.

Perspective from Europe

Europe (David Ferbrache): The other potential benefit of this approach is that it can simplify the regulatory compliance concerns we discussed earlier. If the business is making cyber decisions based on in-depth assessments of all related risks, with regulatory risks folded within those decisions, it should be more straight-forward for banks to demonstrate and document their compliance to authorities — or present solid arguments for their own bank's cyber security measures — since they are clearly aligned with the bank's approved risk framework. In short, this approach advocates for the banks to stop treating cyber security as special and focus more on the changing nature of operational risk in a digital world.

While all this is in the early stages, largely in the US market, with the degree of global collaboration and intelligence sharing we see among banks and increasingly amongst regulators, it's a trend we are likely to spot in other geographies. It's a very positive development and it really reflects our view that cyber risk is not a technology problem but rather a business issue that must be addressed from a business perspective. That way, banks can draw upon the best new technology opportunities to enable their business, with solutions developed and execute in close partnership with the technology groups. Banks can achieve the best results and manage the vigorous cyber security challenges they will continue to confront.

Perspective from Asia

Asia (Henry Shek): Yes, this is game-changing approach since it places accountability for cyber risk with the business — the group that generates revenue and may feel that its plans are stunted by a technology group or CISO who can't keep up with the bank's growth ambitions. The CISO would remain highly involved in the conversation about technology threats, however that group would primarily refocus on doing what they do best — protecting the organization — based on the strategic risk framework and risk appetite defined by the business. Not only can this free the bank to pursue greater business growth, but this new structure provides meaningful data at the board level. Directors can avoid getting bogged down in technical discussions and instead focus decisions on tangible issues about risk levels, asset exposure, and the necessary investments required to manage those risks.

Contacts

David Ferbrache
Chief Technology Officer, Cyber Security Services
KPMG in the UK

Henry Shek
Head of Cyber Security Services
KPMG in China

Perry Menezes
Banking Lead, Cyber Security Services
KPMG in the US

Charlie Jacco
Financial Services Lead, Cyber Security Services
KPMG in the US

kpmg.com/socialmedia

Designed by Evalueserve.
Publication name: Global perspectives on cyber security in banking
Publication number: 135368-G
Publication date: May 2018