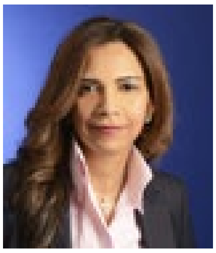
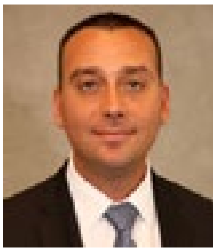
Cyber security moves towards a more resilient model to keep pace with a growing digital business

By **Bia Bedri**, KPMG in the UK
By **Charles Jacco**, KPMG in the US



Bia Bedri



Charles Jacco

Financial services firms are struggling to get on the forefront of cyber security in the face of increasingly frequent and sophisticated attacks. At the same time, they are also trying to protect an ever-increasing number of devices and data as the business goes digital, deal with shrinking security budgets due to cyber fatigue at the top of the house and respond to increased regulatory scrutiny aimed at minimizing risks that continue to strain the business and IT.

Complicating these major challenges for many firms is also the gap that often exists today between business leaders and their IT function in terms of a coherent, organization-wide strategy designed to anticipate, identify and respond to ever-evolving cyber security risks and needs.

"There is a rift or gap today between business leaders and their technology teams, and this is one of the biggest problems we are seeing in terms of addressing and responding strategically to critical cyber security issues," says Bia Bedri, a Partner specializing in Banking and Capital Markets Cyber Security for KPMG in the UK.

Technology security experts within organizations are tightly focused on cyber defense from a technology perspective but typically lack a 360-degree view of what may also be needed from the people and processes perspectives to heighten cyber security. Until recently, boards and executives have largely remained content to approve rising tech budgets without having a truly clear understanding of overall business risk and need from a security perspective. Now, they are demanding answers to fully understand where the funding has gone and questioning whether the spend has actually reduced the firm's overall cyber risk.

"Without guidance from the top and business engagement on priorities and risks, the IT function can be unclear about where the business overall needs to spend money to address evolving cyber risks that impact the entire organization," says Bia. "CEOs and boards in the past have simply devoted larger budgets to cyber security, but now they are increasingly asking, 'How is the money spent reducing my risk?' I think that's perhaps the biggest problem in cyber security today — that breakdown that fails to take the view that security is now a key business issue, not simply an IT issue."

Business leaders have traditionally seen security as a technology issue to which they continue dedicating budgets, staffing and resources, but with attacks growing more frequent and sophisticated by the day and as regulatory pressures place new focus on security solutions, executives and boards now need to be better engaged and understand their responsibility with regards to cyber security.

IT teams are looking at controls, technology and platforms without clarity or input from the business's leaders on what's key to the overall business in terms of precisely what they're protecting and why. Ultimately, you end up with a situation where no one can accurately respond to key questions like 'What's my current cyber security risk?' and 'How can I manage it all quickly and effectively?' If financial institutions hope to make real progress that uses their budgets, resources and time efficiently, they will require a more strategic approach.

Security needs to encompass people, processes and technology

Becoming a resilient, cyber-smart organization will require financial firms to ensure that their people, processes and technology are all strategically focused on cyber risk and appropriate solutions.

"That's really the end game here — adopting a more holistic view of cyber security risk that encompasses people, processes and technology," says Charles Jacco, Principal, US Cyber Security Services Financial Services Leader. "Some organizations will be better from a technology perspective, others may have a better view of cyber security risks in terms of processes, while others will have a really good culture around security awareness. But I don't know that anyone has mastered the need to be fully centered on all three areas — people, processes, technology — when it comes to cyber security. That's really where we see room for improvement today in

> “Security is now a key business issue, not simply an IT issue.”

A global financial organization demonstrates how to raise the bar on cyber security

Financial organizations are increasingly facing sophisticated external threats such as financial crime, ransomware, DDoS attacks and customer data theft. This, combined with internal threats that include rogue trading, fraud and misconduct, is forcing financial institutions around the world to dramatically sharpen their focus on the need for comprehensive new cyber security strategies.

Bia Bedri, a Cyber Security Partner at KPMG in the UK, says: "We were able to help one global organization, following a costly trading incident costing billions of dollars in losses and a significant hit to its brand in the marketplace, develop a strategy that involved rethinking its entire approach to information security."

In its efforts to precisely identify and understand the range of the threats and cyber risks it was facing, the bank undertook a significant challenge to address 'identity access management'. Given the complexity of the problem, the bank initially struggled to develop a strategic information security risk-management program that would include a response to questions raised by regulators.

With help from KPMG's cyber security specialists, working shoulder to shoulder with the organization, the bank ultimately developed a remediation plan that would transform its information security across the organization. KPMG helped the organization deliver the program by designing, implementing and embedding new controls that covered data and business systems operating in more than 30 countries in order to meet business and regulatory requirements.

The results were remarkable. The bank not only reduced risk significantly while optimizing many of its processes, it also enhanced its status in the marketplace by being viewed as an industry leader on cyber security.

most cases. Organizations need to move away from the traditional cyber defensive posture and focus on enabling the business to become a resilient organization."

Unfortunately, there is no time to lose on the need to adopt a strategic approach that goes beyond IT to engage the entire organization.

Cyber security, meanwhile, has become the leading risk concern among CEOs, with nearly three-quarters admitting that they do not feel fully prepared for a cyber event.

Three-quarters of CEOs also say they are concerned about keeping up with new technologies and many are voicing worries about customer loyalty amid the wave of change. KPMG's *Consumer Loss* Barometer, meanwhile, shows that business leaders have good reason to be worried about consumer loyalty as new business models emerge: a third of consumers surveyed say they would consider moving an account in the event of a hacking incident or security breach that affected them.

"Cyber security is a huge issue today, and the increasing focus of customers, governments and regulators is making the need for strategic approaches and immediate solutions even more intense," says Charlie. "Cyber security has to be a top priority for CEOs today. This is a problem that is not going away. If you don't have the culture, the people, the processes and the technology all aligned on everything that you do as a bank or insurer, in terms of understanding cyber risk and security, it doesn't matter what you automate. Organizations need to get the whole concept of a resilient organization in place. And that really needs to come from the top down."

IoT increases need to take a 360-degree organizational perspective

Raising new alarm bells on the need to heighten cyber security is the advance of the 'Internet of things' (IoT) and the impact of billions of new connections between everything from mobile phones, cars and transportation systems, to home appliances, wearable devices and much more.

Soon, for example, people's credit card data will be stored on many more devices, beyond simply a phone or tablet to include cars, appliances, wearables and so on, making it critical for confidential customer data to remain protected in a more open or accessible environment. The whole IoT concept means everything will be interconnected and security controls need to be in place as those technologies move forward. This is a very significant challenge for financial organizations and their need to protect critical customer data.

Some organizations understand the importance of the issue and how it's growing in complexity, but many are having difficulty unravelling it all in terms of knowing what to do next.

Solving the cyber security dilemma as the ecosystem expands is at least as challenging for insurers as they are typically 'less mature' than banks today in developing cyber security capabilities. The fact that they have more ground to

The Global CEO Outlook survey by KPMG reveals that, with disruptive technology and marketplace forces redefining business models and blurring traditional lines between competitors and industries,

72% of CEOs believe the next 3 years will be more critical for their industry than the last 50.

Nearly half of the close to 1,300 CEOs surveyed also said their organization will be significantly transformed in the coming 3 years.

> “Soon, for example, people's credit card data will be stored on many more devices beyond simply a phone or tablet to include cars, appliances, wearables and so on, making it critical for confidential customer data to remain protected in a more open or accessible environment.”

cover on cyber security has not escaped the scrutiny of regulators in places like the US and the UK, where they are increasingly turning their attention to this sector in addition to banks.

"In the UK, for example, regulators have started paying far closer attention to the insurance sector in the last 6 to 12 months. And many firms are discovering that they don't understand or have the capability to respond to the security issues that are arising," says Bia.

All things considered, today's financial organizations remain stuck in a 'reactive mode' when it comes to data attacks or security breaches, and they need to take a far more proactive approach aimed at anticipating and preparing for potential attacks before they occur.

When banks have a breach, they spend a lot of money trying to understand what the breach was, how it happened, what the customer impact was, what the business impact was. But they tend to cover the same path every time, regenerating the same process or reaction, as opposed to pursuing a response and assessment that positions them to be ready and prepared for future scenarios that are very likely to occur.

Looking at people, processes and technology

How then can financial institutions best begin pursuing a much more strategic approach to cyber security that goes beyond throwing money at technology, to instead create a 360-degree view encompassing people, processes and technology?

CROs and CIOs should be collaborating closely today to gain a clearer understanding of who owns what when it comes to cyber security policy, while recognizing that it's no longer simply 'an IT problem' but one in which the CRO and the board all need to be involved. Working together, they can start by identifying their top 10 cyber risks and exploring the complicated processes and technologies that need to be addressed, as well as what that is going to cost.

In some cases, financial firms are already pursuing strategic solutions quickly and efficiently via innovative partnerships with financial technology firms (Fintechs) that can advance or complement today's well-entrenched banking infrastructures to deliver faster and better services in the face of emerging marketplace competitors.

Ultimately, concern and awareness about cyber security need to be ingrained in every business and no longer treated as merely an IT problem. It is a business problem, and it is crucial that businesses understand that the issue must be addressed more from a cultural perspective. There is a fine line between simply 'reacting and adopting' technology and 'thinking ahead' strategically in order to create a secure business environment amid tremendous ongoing changes. ■

Contributors

Bia Bedri
Partner, Banking and Capital Markets Cyber Security
KPMG in the UK
T: +44 20 73115278
E: bedria.bedri@kpmg.co.uk

Bia is a Partner in the London office of KPMG LLP's Advisory Services practice and is the UK Cyber Security Financial Services Industry Lead across banking and capital markets. Bia is an experienced consultant with 20 years' industry knowledge, leading large-scale complex transformation and change programs to enable clients to effectively manage emerging cyber threats, risk and regulatory expectations, while delivering business objectives, innovation and growth.

Charles Jacco
Principal, Cyber Security Services Financial Services Industry Lead
KPMG in the US
T: +1 212 954 1949
E: cjacco@kpmg.com

Charlie is a Principal in the New York office of KPMG LLP's Advisory Services practice and is the US Cyber Security Services Financial Services Industry Lead across capital markets, banking, payments and insurance clients. Charlie has focused extensively in multiple disciplines of the information security field including security strategy and governance, security transformation, digital identity, enterprise identity, access management and cyber defense over the last 15 plus years.