PwC's Kyra Mattar on The Evolving Risks for Wealth Management Firms in the Digital Age

In her role as Partner and Financial Services Lead for Digital Trust at PwC in Singapore, Kyra Mattar has a bird's eye view of the role of digital and the inherent risks facing financial intermediaries and advisers of all types. She offered delegates at the Hubbis Compliance in Asian Wealth Management Forum 2020 her views on making sure that risks are avoided while opportunities are grasped, she explained why cyber hygiene is so important, and outlined strategies for technology and cyber risk management for increasingly digitally-enabled organisations. And she urged delegates to accelerate their data protection and security standards, especially in Singapore in anticipation of the regulator's cyber hygiene directives.

INTRODUCING HERSELF, MATTAR EXPLAINED THAT HER ROLE AT PWC COVERS DIGITAL RISK RELATING TO THE FINANCIAL SERVICES SECTOR. "We live in an age of disruption," she began, "and we are going through a digital revolution that is complementing our lives today, much as the post-industrial revolution, bringing cars, televisions, washing machines and so forth, actually significantly improved our lifestyles."

The sky is the limit

She pointed to the Cloud as a major new advance for the financial services industry, with cloud solutions growing at an incredible pace, citing Gartner's projection of 16.5% growth in 2020.

"Infrastructure as a service, platform as a service and also software as a service are all having a wide-ranging impact across the world of financial services," she observed. "We no longer need to think about maintaining all those systems and infrastructures. We live in a mobile-first, cloud-first world with computing power at our fingertips. All this is changing our engagement with customers in what is now a data economy."

KYRA MATTAR
PwC

Link to Article on website
Link to Event Homepage

Risks as well as rewards

But Mattar warned that with this digital revolution, there are clearly risks. Cyber-attacks on individuals and businesses come because data equates to money, or to customer insights and competitive advantages. "Cyber breaches," Mattar conceded, "are all too regular nowadays, with organisations getting attacked almost daily, although we do not necessarily hear about those attacks until they become public."

The ecosystem of connectivity with different partners means that the ecosystem of trust is much more expansive today. "There is so much more that you need to control and monitor, so whereas data on customers was hidden away in some back room before, now there is a vast amount of data out there, and increasingly often in the cloud."

Regulators will regulate

Mattar pointed to the regulators now increasingly becoming concerned and highly focused on these challenges. "They are striving to keep up with this pace of change, constantly issuing new requirements. The Monetary Authority of Singapore, for example, issued a notice on cyber hygiene that is now law." Moreover, she noted that the MAS is, appropriately, constantly reviewing and revising their guidelines, issuing, for example, a recent consultation paper on technology risk management.

Breaching the fortifications

Mattar then offered an example of a cyber-attack, citing the crippling May 2017 ransomware crisis, a massive online attack that seized control of computers at hospitals, shipping firms and telecom companies around the world. "It hit the Microsoft Windows operating systems," she noted, "even though Microsoft had actually released a patch to fix such a problem some two months earlier, but numerous organisations either did not know about it or did not implement those patches."

Another form of cyber-attack that Mattar highlighted is what is called 'denial of service' where the attackers block off access to systems, as was made public when the Hong Kong Exchange suffered such an attack on its website at the same time that there were connectivity issues on its derivative platform, halting trading.

"We do not always know why an attack is launched, but in the wealth management sphere," Mattar observed, "the motive is most likely customer and bank information on what is, of course, a high-value target." She pointed to the USD80 million 2016 Bangladesh Bank cyber heist when fraudulent instructions were issued by security hackers via the SWIFT network to illegally transfer money from the Federal Reserve Bank of New York account belonging to Bangladesh Bank, the central bank of Bangladesh.

"That was not a SWIFT problem," she explained, "it was an attack on Bangladesh Bank. We all think we have got fantastic controls around our payments and we usually do, but something can get in and take control, which is what happened in the Bangladeshi heist situation."

Mattar also highlighted other attacks, such as Equifax, when more than one hundred million customers' details were hacked, and the more recent Capital One breach thought to have been instigated by an ex-employee of Amazon Web Services, which provided the bank with cloud services. She explained that the breach appears to have occurred due to misconfiguration of the cloud service by the bank and not the fault of the cloud service provider.

Many motives, many ways

She warned that attacks can take place at any time and through many different ways. A phishing attack generally involves someone clicking on a link in an email that appears to be from a genuine source, but is not, and then dangerous software is installed onto the computers, waiting for data of value to steal, for example, usernames and passwords. "Just one loophole can open the door to such an attack," Mattar warned, "so we all need to be incredibly vigilant, and to report and then act on any suspicious activity."

She extrapolated that the human side of all this means that the individual employee's role in the processes and procedures of any financial, or other, organisation must be devised and structured to prevent such problems. All employees must be cyber aware and diligent so as not to become the weak link.

Mattar then mined into further detail on the MAS cyber hygiene notice of August 16 last year, which applies to all financial institutions in Singapore and which will become effective in August this year.

MAS's six steps to cyber hygiene

She briefly highlighted the six key measures the MAS has outlined for cyber hygiene. Number one is making sure that the system administrator accounts that can access systems are secure. Patches need to be implemented in a timely manner to prevent vulnerability. Security standards need to be understood, reviewed regularly and monitored for conformity.

The fourth directive concerned the network perimeter defence, which must be in place and restricted to authorised access. Malware protection must be up to date to ensure protection against viruses and to detect any malware. And, last but not least, is multi-factor authentication - for example the protocol of password as well as one-time pins sent to mobile phones or other devices - to verify account access or access to critical systems or data.

Mattar noted that the sixth MAS hygiene measure, multifactor authentication, is both challenging and costly for organisations, but is crucial to protecting data, customers and therefore, the business itself.

Take action

Mattar's final word was to appeal to the assembled wealth management audience to truly understand the issues and the actions they must take. And as all these areas will soon be law, as defined and monitored by the MAS in Singapore, there is great urgency required. ■