How Digital is Both Helping and Hindering Compliance, Cyber-Hygiene and Data

Technology is making compliance more complex and more challenging at the same time as providing digital tools to help resolve both age-old and newer compliance challenges. Private banks and wealth management firms must rise to the challenges of digital KYC/onboarding, AML monitoring, the expansion of digital platforms, the migration of data infrastructure to the Cloud, Artificial Intelligence, data security, and cyber-crime. Experts in a panel at the Hubbis Compliance in Asian Wealth Management Forum tackled these key pressing concerns.

These were the topics discussed:

- *Cybercrime - what new threats are there for you?*
- *Cyber Hygiene, Cloud and Ecosystem - What are the risks and how do you manage them?*
- *What are the challenges relating to electronic platforms like robo advisors or digital banks?*
- *Digital ID - good idea or bad idea?*
- *In the region every country has its own cyber security rules and it's difficult to make sense of what you can do or not do?*
- *Banks have the challenge of dealing with the non-uniformity - what can you do?*
- *Data confidentiality - do we assume there is none?*
- *How do you ensure appropriate products are made available on execution-only platforms?*
- *How does Technology affect the compliance profession and processes?*

PANEL SPEAKERS

- **Kyra Mattar,** Partner, PwC
- **Anu Phanse,** Operational Risk and Business Compliance, Swissquote
- **Andrew Chow,** Compliance, BNP Paribas
- **Daniel P. Levison,** Partner, Morrison & Foerster
- **Uthra Parameswaran,** Director - Compliance & Operations, Propine

Link to Event Homepage

THE KEY OBSERVATIONS

You cannot wash your hands of Cyber-hygiene

In a digital world and amidst a proliferation of data and the expansion of Cloud-based storage and infrastructure, in a world of digital payments and even digitised storage, the proliferation of cyber-crime translates to the vital need for cyber-preparedness.

Build the right ecosystem

Nobody has yet invented software or devised systems or processes to fully protect themselves or their firms against every kind of cyber risk out there and to come in the future. So it is vital to create and evolve the right ecosystem.

Compliance experts must be digitally savvy

In an increasingly digital world in which data is at ever-greater risk, compliance professionals must be in tune and up to speed on all facets of the digital solutions. They do not need to be coding, but they need to be aware of the implementation, uses and risks relating to technology.

Attacks are on the rise, defences must be battle-ready

Cyber-attacks such as spear phishing (targeting a specific individual) and ransomware (generally targeting institutions) are proliferating. Compliance experts must work with their top management and colleagues to ensure their firms are battle-ready at all times.

Digital solutions must be aligned to good governance

Recommendations from the Monetary Authority of Singapore are increasingly focusing on the need digital security and good practices, good conduct and governance amongst the financial community. Multi-factor authentication, maintaining up-to-date software security patches, malware protection and a host of other defences are all essential.

Be careful not to fall into the gap

There is a lot of technology available today, but compliance teams should be sceptical as to their efficacy and security, as by some estimates there is as much as a one-third shortfall between mission and achievement in many systems and software. But the regulators will not likely continue to accept that sort of gap, so compliance experts must beware of those risks.

Realise that cyber risks are always around the corner

The most resilient and prescient organisations have a fundamental mindset that the danger to their data, their systems, to their clients and their business is not 'if' but 'when', so constant vigilance is required.

ANU PHANSE
Swissquote

FIRST UP FOR THE PANEL WAS THE PROLIFERATION OF CYBER-CRIME AND THE VITAL NEED FOR CYBER-PREPAREDNESS at the private banks and broadly across anyone involved in dealing with wealthy clients in any jurisdiction. The biggest banks have global budgets to tackle these challenges, to acquire the latest systems and software, but smaller banks, boutique banks and the independents will be more challenged from a budgetary perspective.

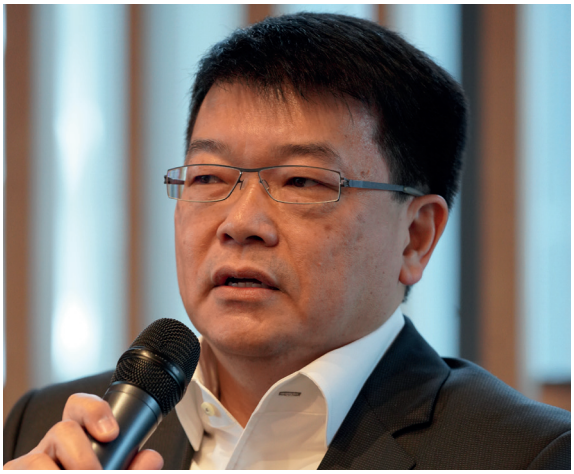
"It is about creating the right ecosystem," said a panellist, "as nobody can protect themselves against every kind of attack out there and to come in the future. You have to build a community of trust where everybody has the same standards, including your partners. But you are all in the business of banking or wealth management, not cyber-security."

Facial recognition in China has become so prevalent that most apps also require you to create facial recognition to use them today. Facial recognition cameras are present throughout China, as the country pushes itself as the cutting edge of new technologies. "But there is no data privacy in China so far," warned one expert, "so there are also immense risks internally. And if you outsource data and services to China, there are significant risks of data privacy and banking secrecy."

Every plus has a minus

A panellist pointed to the online banks which are transforming the way KYC is conducted. "With

KYRA MATTAR
PwC



ANDREW CHOW
BNP Paribas

everything done online and through the app it might be incredibly fast, but with every pro, there will be a con. As compliance professionals, if we are in a business model where we use a lot of online services, and digital IDs, we just need to be conscious of various scenarios that could happen and all the fraudulent cases that might happen. We must test through all those and make sure that these loopholes are not exploited."

Cyber-attacks such as spear phishing (targeting a specific individual) and ransomware (generally targeting institutions) are proliferating.

Up for ransom?

A guest highlighted the billions of dollars paid out in ransom to these attacks since 2017. "The incentives for people to just make the payments are real," he said. "Companies or individuals want to regain control of their systems and their data and are willing to take the chance they might pay, perhaps through insurers, and still not regain control. But the problem is every payment further emboldens these types of criminals."

Moreover, the cyber-criminals are armed with the same or similar tools as the banks and organisations use, such as AI, big data, data analytics to target either specific segments of the population or particular individuals, so the battle is extremely intense, especially as the more paid out in ransom fuels even more technology and even more dastardly threats.

Good governance required

A panellist pointed to some of the recommendations that have been forthcoming from the Monetary Authority of Singapore, which has increasingly been driving the message of digital security and good practices amongst the financial community. Multi-factor authentication, maintaining up-to-date software security patches, malware protection and a host of other defences are all essential.

DANIEL P. LEVISON
Morrison & Foerster

WOULD YOU TRUST THE SECURITY AND PROCESSES OF A VIRTUAL BANK? WOULD YOU PUT THE MAJORITY OF YOUR MONEY WITH A NEW PLATFORM?

Source: Compliance in Asian Wealth Management Forum 2020

"Shockingly," a recent survey I saw decided that 75% of us have what they call risky cyber behaviour," a guest reported. "We need to boost awareness, ensure regular training takes place, keep investing in the latest software and antivirus, all these are basic actions that anyone should do in the world of wealth management."

Compliance includes digital

Another expert explained that compliance professionals and teams need to see cybersecurity as a core element of their responsibilities. "You need to conduct a full risk assessment, you need to see where you must invest, what you can do to focus your efforts and resources, and if you have to go in front of the regulator, you have a very clear and principled reason for why you took certain decisions."

Another guest pointed to the use of simple protocols such as digital identity aligned with transaction limits as well as multi-factor payment authentication. "We need to keep it simple and just really think about the controls that we need to incorporate throughout," he advised.

Mind the gap

A panellist pointed out that there is a lot of technology available today, but the compliance teams should be sceptical as to their efficacy and security. He indicated there might be a 30% gap between the success and shortfall for certain systems and software, so the regulators will not likely continue to accept that sort of gap, especially in areas such as transaction monitoring for AML, where the banks are held to a very high standard in any well-regulated market.

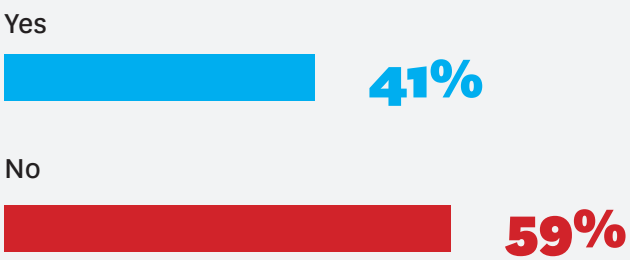
UTHRA PARAMESWARAN
Propine

With respect to machine learning and AI, he added, there is still a major challenge around the integrity of the data and the biases that are built into the data. "We really need to retain a healthy dose of scepticism and ask the difficult questions, test the data and think about it from all of these different angles," he advised.

Looking into the future, a guest observed that banks today are the custodians of wealth and money, and in the future organisations are becoming custodians of your identity and of your data.

A fellow panellist agreed, warning that we must be wary of actually trusting machines. "The issue now is data," he observed. "I think the scariest

HAVE YOU PERSONALLY HAD ANY CYBERSECURITY ISSUES IN THE LAST 12 MONTHS?



Source: Compliance in Asian Wealth Management Forum 2020

thing for me is the insurance companies where they actually look at DNA and they predict the possibility of you having a certain form of cancer and therefore refuse to actually insure you."

Turning the discussion specifically to compliance, a guest noted that there are numerous RegTech solutions, including in areas such as natural language processing, artificial intelligence, machine learning. "You need to assess and decide on which solutions you can really trust and rely on, you need to test the reliability and where they can actually augment or replace human effort and skills."

Continual vigilance

An expert advised that the most resilient organisations have a fundamental mindset that the danger is not 'if' but 'when'. "Constant vigilance is essential," he said, "so the best-prepared organisations are those that have simulated such crises and attacks, and that know exactly how to respond, so they are not simply caught asleep at the wheel."

Internal preparedness is also all about having the right systems and approach to personnel, training and the appropriate standards. Access to data internally must also be carefully thought out and structured to ensure that it cannot be hacked or stolen from within, thereby avoiding the potential insider threats that have plagued many organisations around the world.

"And you must be extremely cautious about access to data for personnel who have actually left banks or other firms," another expert warned. "There are plenty of incidents I am aware of when someone has left a bank, perhaps left the IT team, and a few weeks later, their IDs and access permissions still exist. These must be deleted immediately for correct cyber hygiene notice. It is now law in Singapore, so anyone with an admin account who can administer your IT systems must be removed if they leave. If you don't remove that type of access you are in breach of the law."

Classify and simplify

The final word went to a guest who said that simple things such as basic internal controls on data classification -what is confidential, what is restricted, which data is openly available - these are all basic steps all organisations should implement. "You also need to decide what data is classified on what auditors call the 'need to know' basis, so whether an employee really needs to know this data, needs to really have access to data," they advised. "And the third key element of cyber hygiene is multiple layers of authority, so it is not just one person with the ultimate authority to either approve payments or to make changes to the data, but everything follows a multi-eye principle. And tracking logins internally and access, that is another key area." ■