Produced in association with Conventus Law

Osborne Clarke

CYBERSECURITY ASIA

Facing the threats

INTRODUCTION

SINGAPORE

INDIA
coming soon...

ABOUT OSBORNE CLARKE AND CONTRIBUTORS

CYBERSECURITY ASIA – Facing the threats

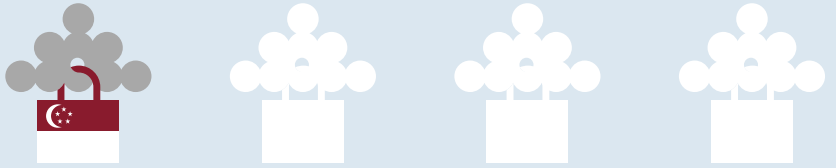
Introduction

Digital Transformation and rapid innovation are double-edged swords. In a costly game of "cat and mouse", as businesses adopt and adapt increasingly sophisticated technologies, so does the world of cybercrime. As interconnectivity (across multiple devices, networks and platforms, often not fully compatible) increases at both enterprise and consumer levels, so does the number of "chinks" in cybersecurity armour against cyberattacks, disruption and theft.

Cybercrime and data security are now frequently cited as the biggest risk issues troubling boards and regulators, for good reason. All organisations are vulnerable to cyber risk – and the risk is increasing as businesses accelerate digital transformation strategies in order to compete, using the likes of AI, IoT and robotic process automation. The costs (in both reputational and financial terms) of major incidents can be devastating. The World Economic Forum 2019 Global Risk report names cyberattacks and data breaches as the 4th and 5th most serious risks facing the world today – and there are numerous studies which identify companies in Asia Pacific regions as more exposed to cyber threats, with greater frequency, than elsewhere globally.

While the majority of incidents is still enabled by human error or "insiders", newer forms of cyber breaches are growing threats too – such as AI-generated Authentication, DDoS, form-jacking, malicious chips, data poisoning and "C2"(command-and-control) server-generated bot attacks (with the last of those being found particularly prevalent in China, South Korea, Japan, India and Hong Kong, according to CenturyLink).

The imminent proliferation of 5G in Asia regions is unlikely to do anything other than exacerbate this outlook, in the context of worrying latest statistics. Already, analysis show that AsiaPac businesses are the subject of one form or another of cyberattacks roughly every 39 seconds, whether they know this or not – and that over 25% have suffered a material security incident over the last 18 months (and 78% at least once ever), whereas 27% are not able to confirm their position, having not undertaken any detailed breach assessment (ZDNet, 2019). The loss to the region from cyberattacks in the last year is estimated at an eye-watering US$107.5 billion.



CYBERSECURITY ASIA – Facing the threats

Introduction

In this scenario, in collaboration with cyber attack response specialists Blackpanda and our Osborne Clarke colleagues in Singapore, India*, Hong Kong and Shanghai, we are producing a four-part series of reviews of the latest approaches to cybersecurity risks being taken by enterprises and institutions in each of those jurisdictions. As part of our research for each feature, we will be speaking with leading individuals in those regions for whom cybersecurity and data protection issues are vital. We hope that you find this series informative and useful.

The first in this series looks at Singapore. At OC Queen Street, given our intensive sector focus and the nature of our clients' businesses, advising on cybersecurity and related data protection issues (whether from preventive and remedial perspectives) is increasingly at the forefront of key issues for our clients, particularly those in the Financial Services & FinTech sector. This is a sector which handles some of the most sensitive information – with data ubiquity as more services go on-line and the move to "anytime, anywhere" mobile access forges ahead, there are present and growing challenges for this sector.

At Osborne Clarke we have a market leading international team of regulatory and litigation specialists which spans 11 jurisdictions* and three continents, advising on incident prevention and response. We have developed effective and innovation crisis management tools, such as a crisis App and a secure client platform for effective communication and document management, while maintaining regulatory compliance, confidentiality and legal privilege. We speak from experience, having acted on many of the biggest cyber crises to hit the news in recent years.

Ashley Hurst
Partner, International Sector Leader, Tech, Media and Comms, UK
T +44 20 7105 7302
ashley.hurst@osborneclarke.com

Charlie Wedin
Partner, co-head, International Cybersecurity group, UK
T + 44 20 7105 7856
charlie.wedin@osborneclarke.com

Adrian Bott
Foreign Legal Consultant, (Registered Foreign Lawyer), Hong Kong
T +852 2535 0126
adrian.bott@osborneclarke.com

*Expertise in India is provided by BTG Legal, Osborne Clarke's relationship firm

CYBERSECURITY ASIA – Facing the threats

Singapore boosts cybersecurity on back of FinTech boom

Singapore is embracing legislative and collaborative initiatives to bolster its cybersecurity amid an ongoing expansion of the city's digital economy. Singapore's ongoing liberalisation of the finance sector has led to an explosion in FinTech startups in the city, as digital rivals emerge to compete with traditional banks. The number of such startups has risen from around 50 in 2015 to more than 600 today.

Although the rapid digitalisation of the city state's economy is creating new growth opportunities, it is also throwing up an increasing number of cybersecurity challenges for both the government and financial sector to overcome.

The country's Cyber Security Agency (CSA) revealed in its third annual Cyber Landscape report in June that 90% of the fake – or spoofed – websites detected last year imitated banking and financial services, technology or file hosting companies. The CSA observed 16,100 phishing URLs with a Singapore link in 2018, up from 2,500 such sites in 2016.

The number of recorded business e-mail impersonation scams – where attackers use spoofed business e-mail accounts to trick companies into following bogus instructions – rose from 257 in 2016 to 378 in 2018.

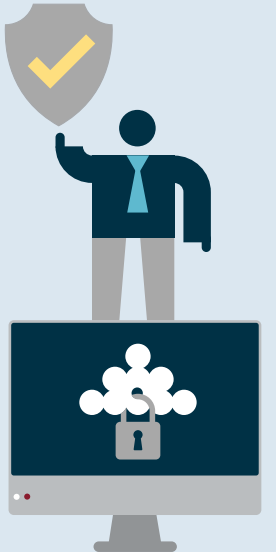
In response, Singaporean authorities have introduced initiatives to deepen cybersecurity co-operation with neighbouring countries, such as the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in October, as well as a number of legally binding requirements for local financial institutions.

Securing against cyberattacks

As part of Singapore's Smart Nation vision, the government aims to turn the city into an e-payments society. To this end, the Monetary Authority of Singapore (MAS), the central bank and financial regulator, created the Project Ubin and Payments Council initiatives to collaborate with industry leaders.

Singapore is also expected to announce in 2020 details of a single platform that will allow consumers to aggregate account information from various financial institutions and share the consolidated data between organisations.

Despite these initiatives, the city's FinTech sector continues to be exposed to cyber threats such as data theft, fraud and malware attacks. Such cyber threats led to the introduction of the Cybersecurity Act 2018, which created a regulatory framework for the monitoring and reporting of attacks.



Singapore boosts cybersecurity on back of FinTech boom

Moreover, MAS issued in August a set of legally binding rules that more than 1,600 licensed financial institutions must adopt to secure their systems against cyberattacks. Known as the Cyber Hygiene Notices, the requirements focus on critical system recovery, customer data protection and incident reporting.

Ezra Tay, general counsel for invoice financing platform Capital Match, interviewed in October 2019, noted that such legislation was important for the sector, as it created a baseline from which companies could evolve their cybersecurity strategies. "While it depends on the individual financial product, with differing products having varying levels of risk, legislation creates an important benchmark for the sector. The majority of Capital Match's business is not MAS-regulated, but we believe it is beneficial to standardise cybersecurity measures across our entire platform," Tay said.

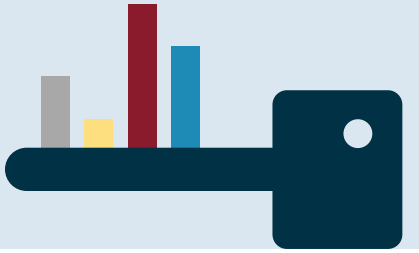
"Compliance does not equal safety. Meeting the legislation's requirements is the absolute bare minimum for the sector."

Kian Teck Soh, CTO for international payment provider QFPay, said that while the Cyber Hygiene Notices forced companies to become more cybersecurity conscious, achieving compliance should just be the start of the security process. "Compliance does not equal safety. Meeting the legislation's requirements is the absolute bare minimum for the sector," Soh said.

"When the Payment Services Act comes into force in 2020, you should see an industry-wide rise in cyber readiness standards."

Chia Ling Koh, managing director of the Singapore-based OC Queen Street, said the government understood this need for greater cybersecurity preparedness. He said: "Many of the MAS rules are formulated to strengthen the FinTech company's systems and processes against cyberattacks. When the Payment Services Act comes into force in 2020, you should see an industry-wide rise in cyber readiness standards."

"Legislation shouldn't be too prescriptive; it needs to be tech agnostic. Singapore is getting this right."



CYBERSECURITY ASIA – Facing the threats

Singapore boosts cybersecurity on back of FinTech boom

The rapid pace of technological change, however, has repeatedly left legislators across the globe struggling to draw up rulesets that can adapt. As such, Singapore's focus on collaboration and innovation in the cybersecurity space – rather than solely relying on legislation alone – is a step in the right direction.

Prabhakaran Janarthanan, the head of international bank UBS' data protection legal team, praised Singapore's adoption of a principle-based approach that addressed the broader cybersecurity framework. "Nobody wants to be attacked and governments are better served trying to work with companies. Legislation shouldn't be too prescriptive; it needs to be tech agnostic. Singapore is getting this right," he said.

Employee vulnerability

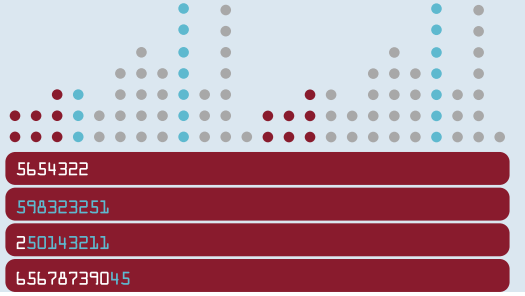
As with most cyber-conscious companies, the international bank has found those attacks focusing on its staff to be one of its biggest vulnerabilities.

"It's all about raising awareness and positively reinforcing the need for added vigilance."

"Targeted social engineering attacks against an individual can be very hard to defend against," Janarthanan said, adding: "We've invested significantly in defending against cyber assaults that target our IT infrastructure, but when it comes to attacks targeting an individual it boils down to how closely that person follows their training."

UBS has established training programmes focused on identifying phishing attacks and regularly conducts internal probes to simulate real-word attacks. The bank also trains employees to send any suspicious messages directly to the bank's cybersecurity team for analysis. Janarthanan said: "It's all about raising awareness and positively reinforcing the need for added vigilance."

In addition to socially engineered attacks, similar to other organisations, ransomware attacks are also another area of concern for the bank. The company has invested extensively to address these threats and is working closely with international law enforcement agencies as well as national regulatory bodies to build a comprehensive cyber defence.



Singapore boosts cybersecurity on back of FinTech boom

These concerns are echoed by QFPay's Soh, who said phishing represented the "biggest danger" to his company. He added that while most of the company's systems were cloud-based, protected by server-side security, there was always the risk that a successful phishing attack targeting employees could open up a backdoor.

"Educate, educate, educate; it's the only way. We are constantly assessing our staff through fake email exercises. It's not something we'll ever stop doing, because we need everyone to be aware of the risks such emails pose."

Asked how QFPay was addressing these concerns, Soh said: "Educate, educate, educate; it's the only way. We are constantly assessing our staff through fake email exercises. It's not something we'll ever stop doing, because we need everyone to be aware of the risks such emails pose."

Gene Yu, co-founder and CEO of Blackpanda, the cyber incident response company, said it was impossible to achieve 100% impenetrable cybersecurity, "no matter how much we invest in cybersecurity tools or services". He added: "Playing defence is very difficult. Bad actors only need to get it right once, while the defence must anticipate any and all methods of attack."

This is why, he said, companies are turning to cyber incident response firms. "In the same way a neighborhood requires access to emergency police, fire, or medical services regardless of individual homes' security and preparedness, individual firms deserve the same level of service on stand-by for cyber emergencies."

A multifaceted approach

Cyberattacks are an increasing part of the fabric of modern society and, while governments can introduce legislation to protect their citizens, much of the work needs to focus on generating greater awareness at an individual level.

"The reality is that individuals tend to be overly relaxed when it comes to security."

Capital Match's Tay noted that FinTech companies were naturally security conscious simply because "data is a modern-day currency". However, he added: "The reality is that individuals tend to be overly relaxed when it comes to security." Tay said the consequences of a major data breach were rarely felt at a personal level, which led to complacency and created vulnerabilities that criminals could exploit.

Singapore's collaborative approach, with other governments as well as industry, highlights the city state's understanding that a multifaceted approach is needed to counter cyber threats. Legislation should be just the starting point for the country's FinTech sector and, as interconnectivity expands, greater sector collaboration as well as more comprehensive staff training will be the order of the day.

About OC Queen Street

Queen Street

At OC Queen Street, given our intensive sector focus and the nature of our clients' businesses, advising on cybersecurity and related data protection issues (whether from preventive and remedial perspectives) is increasingly at the forefront of key issues for our clients, particularly those in the Financial Services & FinTech sector. In that context, in collaboration with cyberattack response specialists BlackPanda and our Osborne Clarke colleagues in India, Hong Kong and Shanghai, this four-part series reviews the latest approach to cybersecurity risks being taken in each of those jurisdictions.

OC Queen Street is a Singapore law firm and part of the Osborne Clarke international legal practice. As a firm with deep sector specialism across digital transformation, Financial Services & Payments, Technology, Media & Communications, and Digital Health, we focus primarily on business in the ASEAN region. In this, our clients include some of the world's leading technology innovators and technology-driven companies.

Our expertise encompasses M&A, Investment Funds, Cryptocurrency, Financial Services, Competition, Competition Economics, Regulatory, IP (Patent & Copyright) Litigation, Dispute Resolution, Investigations, Data Protection, IT, Telecoms, Media, Employment, Capital Markets, Banking & Finance, Payments and FinTech.

osborneclarke.com

"OC Queen Street is a modern firm with technology-savvy lawyers. Clients with disruptive business models are drawn to the firm's understanding of and dedication to innovative technologies such as AI and blockchain."
Chambers Fintech 2019

"…by far the market leader in the area of cutting edge issues presented by new technologies"
Legal 500 TMT 2019

Chia Ling Koh
Managing Director
OC Queen Street, Singapore
T +65 6350 4380
chialing.koh@osborneclarke.com

About Osborne Clarke

Osborne Clarke is an innovative international legal practice for business, with legal technology and digital transformation expertise to help challenger, fast growth and top tier businesses in Asia and beyond succeed, with presence and capabilities in 26* locations across Asia, Europe and the US.

We do not aim to be “everything to everyone”. We are completely focused on our seven chosen core market sectors, in which we deliver genuine, full-service sector expertise. In Technology, and at its intersection with Financial Services & Payments , we are widely regarded as market leaders. Every day we work with clients who are looking to do things differently and where technology and digital transformation provides a key competitive advantage.

Our sector-led approach means that we’re focused on the issues driving industry change and shaping business strategy. We are continually looking at the trends and innovation within our sectors, to remain at the cutting edge of developments within them. Rather than producing generic output, we overlay our advice with our sector knowledge and our understanding of your business. We focus on solving problems and delivering real, practical advice.

*Expertise in India is provided by BTG Legal, Osborne Clarke’s relationship firm

osborneclarke.com

CYBERSECURITY ASIA – Facing the threats

Our experts

For further information, please contact one of our experts in this field:

Chia Ling Koh
Managing Director
OC Queen Street, Singapore
T +65 6350 4380
chialing.koh@osborneclarke.com

Vikram Jeet Singh
Partner
BTG Legal, India
T +91 22 2482 0820
vikram@btg-legal.com

Guohua Zhang
Co-managing Partner
Zhang Yu & Partners (OC China)
T +86 21 6279 8808
guohua.zhang@oclegalchina.com

Prashant Mara
Partner
BTG Legal, India
T +91 22 2482 0820
prashant@btg-legal.com

Albert Yuen
Foreign Legal Consultant
Osborne Clarke, Hong Kong
T +852 6165 3165
albert.yeun@osborneclarke.com

Contributors

About Conventus Law

At Conventus Law, we approach our business with a different perspective. We strive to create environments which encourage collaboration, generate conversation, create imagination, develop positive experiences and encourage community building.

As an online legal media company, we want to challenge the market's perception of the role of the lawyer in a business context. We believe lawyers should be valued business advisors as well as trusted legal advisors.

Our narratives encourage businesses to look at law firms and legal departments in a different way. We hope it will lead to conversations about working with lawyers at a strategic business level.

By partnering with the best and most reputable international and domestic law firms across Asia, Conventus Law keeps the market informed about the latest business developments in Asia and gives businesses new ideas on how to navigate the business environment when investing in Asia.

As an online legal and business media publisher, we provide a full suite of media services for our partners.

conventuslaw.com

Stephen Lai
Managing Director, Conventus Law, Hong Kong
T +852 6621 1608
stephen.lai@conventuslaw.com

BLACKPANDA

Gene Yu
Co-founder and CEO, Blackpanda
info@blackpanda.com

CYBERSECURITY ASIA – Facing the threats

Acknowledgements

In producing this feature, we would like to thank all the leading individuals who so generously agreed to contribute their time and insights to it and particularly our chief researcher and editor, Andrew Kemp, and publisher Stephen Lai, both at our supporting partner in this project, Conventus Law. The interviews were conducted during October and November 2019.

Publication number Q_1911191739FWE