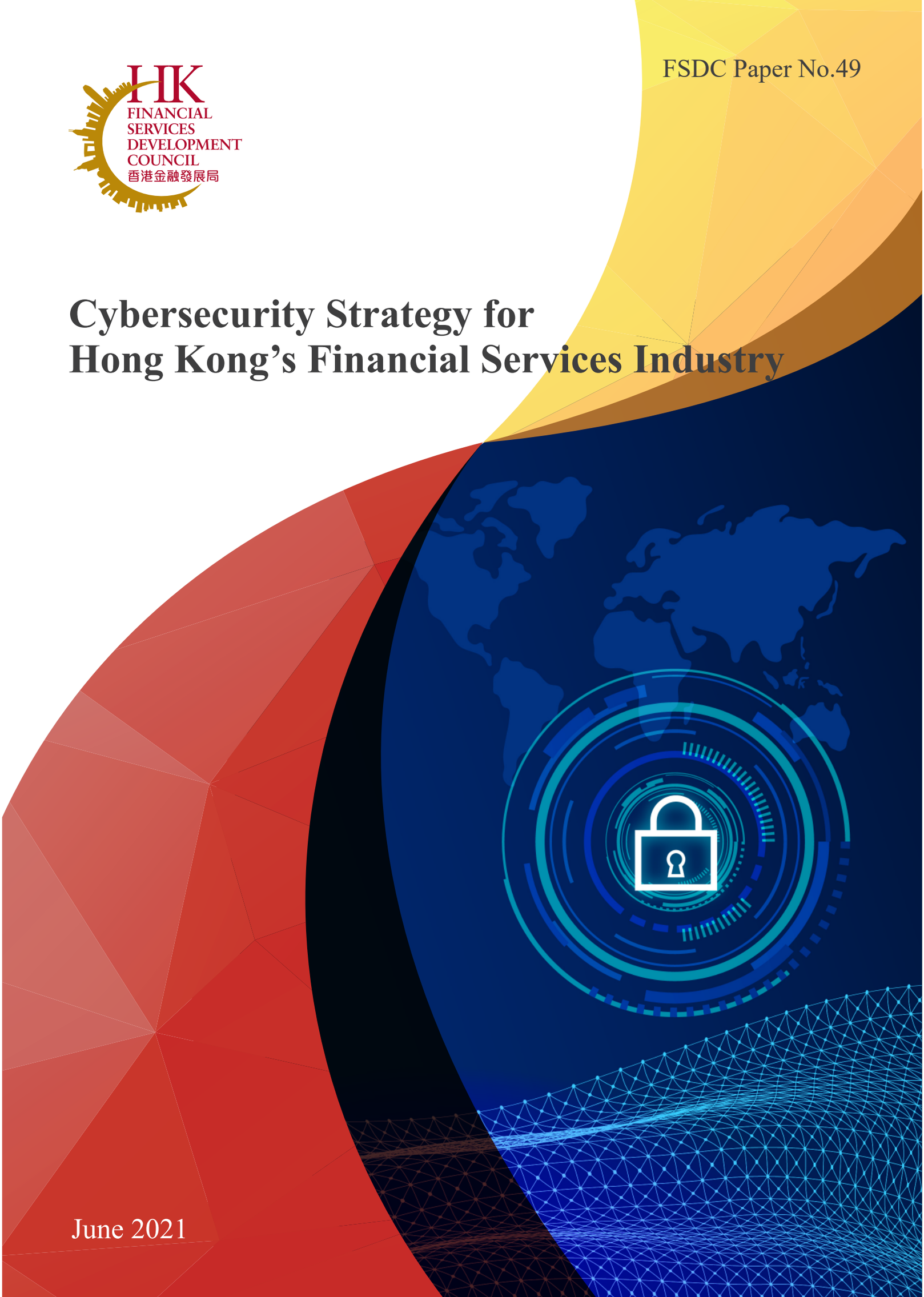
FINANCIAL SERVICES DEVELOPMENT COUNCIL
香港金融發展局

FSDC Paper No.49

Cybersecurity Strategy for Hong Kong's Financial Services Industry



June 2021

Content

Executive Summary

Cybersecurity, or Cyberspace safety, is a cross-industry, cross-boundary subject matter. Among others, financial services industry is a key target of cybercriminals, who have caused tremendous economic, regulatory and reputational harm over the years. As an international financial centre, Hong Kong draws an increasing number of cybercrimes; and to prevent, address and handle cyber risks, the level of readiness among financial institutions in the city is generally on an upward trend.

With developments in the post-COVID-19 era – including licensed virtual financial services, increasing reliance on cloud and online collaboration tools, etc. – the future cyber universe will become more complex, presenting a more urgent need to combat cyber risks.

Based on a comparison on cybersecurity framework of Hong Kong against other jurisdictions' (including Australia, the European Union ("EU"), Japan, Mainland China, Singapore and the United States ("US")), we have summarised as to how Hong Kong fares internationally on four key dimensions – (i) cybersecurity policy and strategy; (ii) legal and regulatory frameworks; (iii) cybersecurity culture (and society); and (iv) cybersecurity education, training and skills.

Hong Kong is keeping up with its peers, but yet to be a leader in the cyberspace safety field. To enhance the city's cyber resilience, we recommend –

On the policy level –

- to develop a dedicated cyberspace safety roadmap with policy priorities for Hong Kong;

On the legal and regulatory level –

- to develop cyberspace protection legislation;
- to harmonise regulations across the financial sector;

On the operational level –

- to enhance talent development; and
- to operationalise preparedness at industry level through industry-wide stress test and data recovery enhancement.

Going hand in hand with these recommendations, both the public and private sectors are encouraged to be fully engaged in the process so that Hong Kong can become an even more competitive international financial centre with adequate cyber resilience and effectiveness.

Cyberspace Safety – a Significant and Growing Issue Globally

Data has become a key asset of the new economy. With its capacity to be sold and exchanged, data drives tremendous value that different players in the economy are striving to seize – for good and bad purposes. Organisations of all sizes, geographic locations and industries are seeking to protect their data "*by preventing, detecting and responding to (cyber) attacks.*" This is "cybersecurity",[1] the subset with the data universe into which this paper looks.

Researching cybersecurity is extremely challenging, as cyber risk is inherently difficult to measure or quantify. **The hidden nature of most sources of cyber risk, together with the unwillingness of a country or an organisation to disclose its vulnerability to risks, has exacerbated the development of an accurate cyber risk analysis.**[2]

Despite the challenge, cybersecurity is increasingly becoming a high priority agenda item because of the alarming harms cyber risk brings. Amongst other consequences, the mounting cost as a result of cyberattacks is pressing the world to pay more attention to this issue. Over the years, the cost of cyber-attacks has surged – as early as 2015, a British insurance company estimated that cyber-attacks would cost businesses as much as US$400 billion a year, globally.[3] By 2018, the estimated cybercrime cost had reached US$600 billion, or 0.8% of the global GDP, according to a study by a US think-tank.[4] A more recent update is that, global losses from cybercrime as of 2019 exceeded US$1 trillion, a 50%+ leap from the previous year.[5] There are multiple reasons for the cost climb, including: the increased ease of committing cybercrimes, an expansion of cybercrime 'centres' across different regions, as well as the growing sophistication among cybercriminals to monetise stolen data.[6]

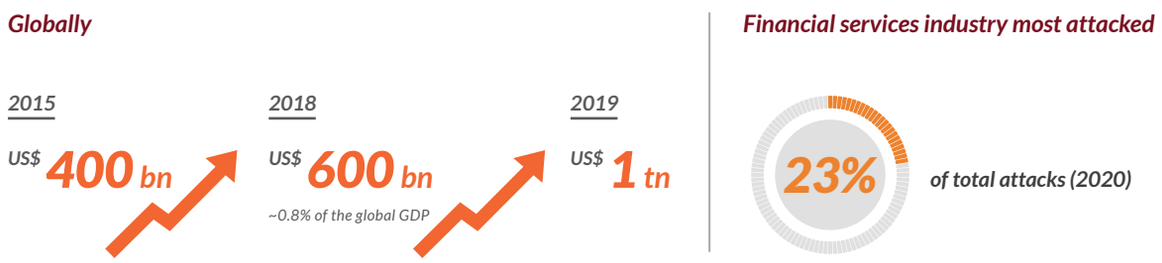
At the enterprise level, the cost of cyberattacks is multifaceted: internal cost activity centres (for example, in detection, investigation and recovery) versus external consequences and costs (for instance, business disruption, revenue loss and information theft); and direct financial losses versus indirect costs (such as legal and regulatory consequences, reputational damage, etc.). Accenture and Ponemon surveyed over 2,600 senior professionals from some 350 enterprises across various industries in 2018.[7] They found that both the average number of security breaches and the average cost of cybercrime have increased steadily: a 67% jump (to 145 breaches in 2018) and a 72% leap (to US$13 million in 2018) in the past five years. In a more recent survey jointly carried out by an insurer and a law firm in 2021, cyberattacks ranked top of the five risks by the surveyed directors working across Asia-Pacific, Europe, the UK and the US – 56% of the respondents rated such cyber risk as very significant or extremely significant to their businesses.[8]

---

[1] National Institute of Standards and Technology, Computer Resources Centre - Glossary: cybersecurity.
Definition set out by the National Institute of Standards and Technology, a non-regulatory agency of the United States Department of Commerce.
[2] United States Department of Homeland Security, Cyber Risk Economics Capability Gaps Research Strategy, October 2018.
[3] Fortune, Lloyd's CEO: Cyber attacks cost companies $400 billion every year, January 2015.
[4] Center for Strategic and International Studies, Economic Impact of Cybercrime: At $600 Billion and Counting - No Slowing Down, February 2018.
[5] McAfee, The Hidden Costs of Cybercrime, December 2020
[6] See footnote 4.
[7] Accenture and Ponemon Institute, Ninth Annual Cost of Cybercrime Study, March 2019.
[8] Global FINEX – Directors and Officers Insurance (D&O) - D&O Liability Survey 2021, Clyde & Co and Willis Towers Watson, April 2021.

The financial services industry is a prime target of cyberattacks, with the banking and insurance sectors being the hardest hit, recording an average cost of some US$18 million and US$15 million in 2018, respectively.[9] Along similar lines, IBM found that the finance and insurance sector has been the most-attacked industry for five consecutive years, with 23% of total cyberattacks and incidents in 2020.[10] Given such statistics, cybersecurity has rapidly climbed in importance on many, if not all, financial institutions' agendas.

Cost of cyber risk on the rise



Sources: Fortune, Center for Strategic and International Studies, McAfee *Source: IBM*

Aside from the heightened cost, cyber risk is threatening also because it is by nature a transnational subject matter. The places of launching and targeting a cyberattack do not, at all, have to be the same and these places can be moved swiftly. Historically, the North American and European markets were common targets by cyberattacks, which then were triggered to develop their security preparedness in earlier days than others. As these markets become harder to attack, this centre of gravity has gradually been expanded to the Asia-Pacific region. In the recent few years, threat levels in Asia have become significantly higher than such in the rest of the world. For example, as pointed out in the LexisNexis report, the Asia-Pacific region saw higher overall attack rates (3%) than the global average of 1.4% in H1 2020.[11] Given such high geographical mobility, cybercrimes are difficult to trace and prosecute.

[9] Ibid.
[10] IBM, X-Force Threat Intelligence Index 2021, February 2021.
[11] LexisNexis Risk Solutions, Cybercrime Report January-June 2020: The Changing Face of Cybercrime, September 2020.

Different countries and regions have started to realise the importance of cybersecurity and have enhanced their cyber resilience accordingly. As reported in the Global Cybersecurity Index 2018,[12] a significant number of Asian countries, on par with their European and American counterparts, have demonstrated their cybersecurity commitments across five assessed "pillars" (legal measures; technical measures; organisational measures; capacity building measures; and cooperation measures). China (covering Hong Kong), Japan and Singapore are three jurisdictions classified as having 'high' commitment to the five pillars. Likewise, in another report by a US think-tank,[13] Hong Kong and Singapore are both considered to have relatively mature cyber regimes, in terms of policies, codes of conduct and standards.

With the onset of the COVID-19 pandemic, the demands on the cybersecurity sector have become even more urgent. As governments, organisations and individuals have been forced to embrace new online activities such as remote working and virtual conferences, cybercriminals around the world have capitalised on this crisis. In April 2020, for example, the World Health Organisation announced that the number of cyberattacks it has encountered recorded a fivefold increase compared to that of the same period in the previous year.[14] This is echoed by another survey report issued by a specialist insurer, with the findings that almost half of the businesses in Europe and North America were targeted by cybercriminals in 2020, who took advantage of the pandemic.[15] Accordingly, 43% of the 6,042 companies in eight jurisdictions surveyed had suffered an online attack in 2020, a 38% year-on-year increment.[16] As for the financial services industry, a number of authorities have called on financial institutions to enhance their cyber resilience efforts. Amongst others, the Financial Action Task Force ("FATF") points out, in its risk and policy response, that there has been a sharp increase in social engineering attacks, which use links to fraudulent websites or malicious attachments to acquire personal payment information of clients.[17] Increased remote transactions, limited familiarity with online platforms, and unregulated financial services, amongst others, could lead to additional vulnerabilities to the global financial system.[18]

[12] International Telecommunication Union, Global Cybersecurity Index ("GCI") 2018, April 2019.
[13] Centre for Strategic & International Studies, Financial Sector Cybersecurity Requirements in the Asia-Pacific Region, April 2019.
[14] World Health Organization, WHO reports fivefold increase in cyber attacks, urges vigilance, April 2020.
[15] Hiscox, Hiscox Cyber Readiness Report 2021, April 2021
[16] Ibid.
[17] Financial Action Task Force, COVID-19-related Money Laundering and Terrorist Financing: Risks and Policy Responses, May 2020.
[18] Ibid.

Is Hong Kong an Obvious Target?

Over the years, there have been various studies on how cyber risks should be assessed. As a result, a number of assessment standards have evolved. However, some of the most widely-adopted standards are more suited for communicating the likelihood and severity of a cyberattack, but rarely for providing the quantum of losses that could occur over a period of time. Likewise, market and credit risk metrics such as value-at-risk, as some suggest, are not relevant to cybersecurity.[19]

Despite the absence of a widely-recognised scientific basis for assessing cyber risks, global business leaders are increasingly focused on cybersecurity issues. According to a report from the World Economic Forum,[20] cyberattack is considered by senior executives to be one of the top 10 risks facing the world.

While cybersecurity is an area of concern for businesses in a wide range of industry sectors, for the purposes of this paper, we intend to focus on its impact on the overall economy and the financial services industry. In this section, we will look into whether Hong Kong, in its capacity as a leading international financial centre in the region, is an attractive target for cyberattacks, and if so, whether the city is sufficiently prepared for this scenario.

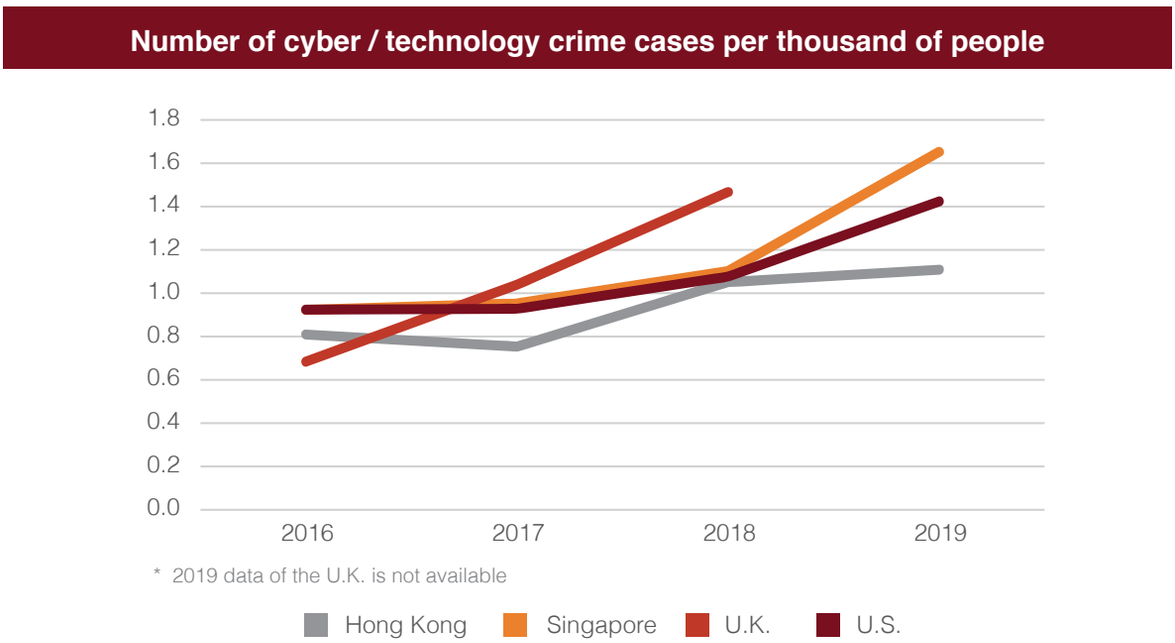
Cyber risk level of, and impact on, Hong Kong

Hong Kong's cyber risk level is palpable and increasing. According to the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT"), the number of cybersecurity breaches continues to be significant. The latest figures published shows that Hong Kong, in 2020 alone, recorded close to 39,000 unique security events, involving malware hosting, phishing and defacement.[21] As for technology crimes, the number has climbed to 8,322 in 2019, i.e., a 6% year-on-year increment, according to Hong Kong Police Force.[22]

How Hong Kong stands internationally in terms of its cyber risk level attracts diverse views. Figure A compares the number of technology crime cases per capita of Hong Kong with that of several other developed economies. Notwithstanding the minor deviation in the definition of technology/cyber/computer-related crimes in different jurisdictions, the number of cases per capita for Hong Kong appears broadly in line with that of the other countries in the survey. Meanwhile, if looking at digital attacks, Hong Kong appears to be one of the targets for cross-boundary events (see Figure B, a screenshot of daily DDoS attacks targeted Hong Kong).

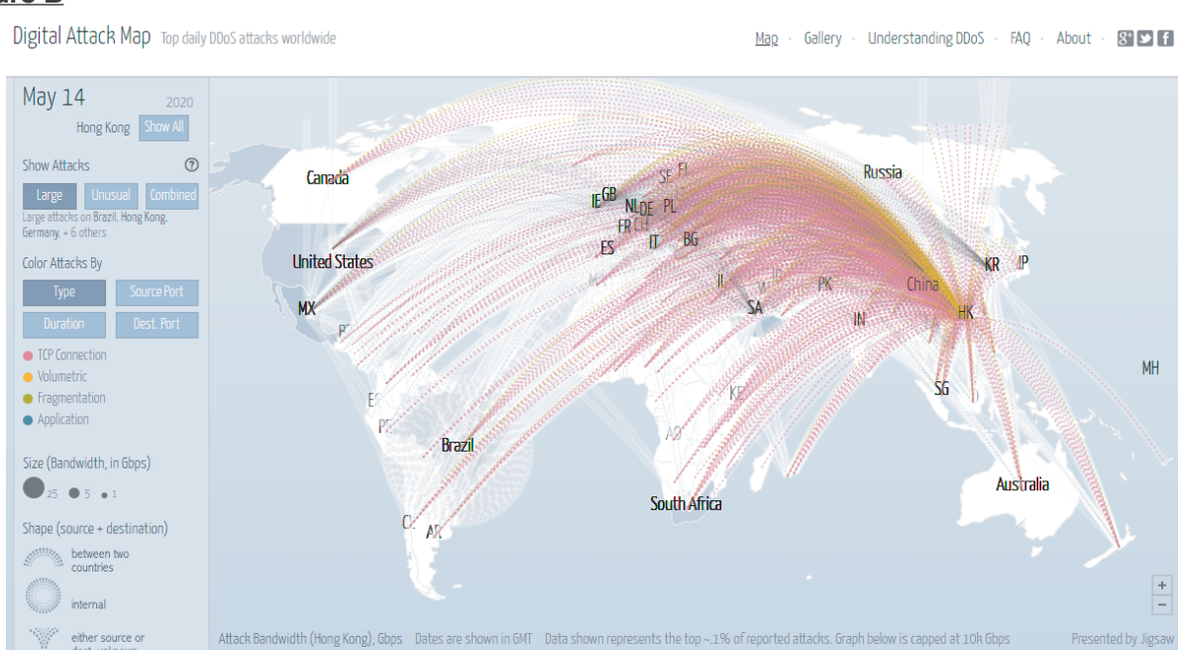
[19] Domenic Antonucci, The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities (p.67-70), May 2017.
[20] World Economic Forum, The Global Risks Report 2021, January 2021.
[21] Hong Kong Computer Emergency Response Team Coordination Centre, Hong Kong Security Watch Report (Q4 2020), February 2021.
[22] Hong Kong Police Force, Law and order situation in 2019, March 2020.

Figure A



Sources: HKSAR Police Force; Singapore Cyber Security Agency (CSA); UK Office for National Statistics (ONS); US Federal Bureau of Investigation (FBI) and Internet Crime Complaint Center (IC3)

Figure B

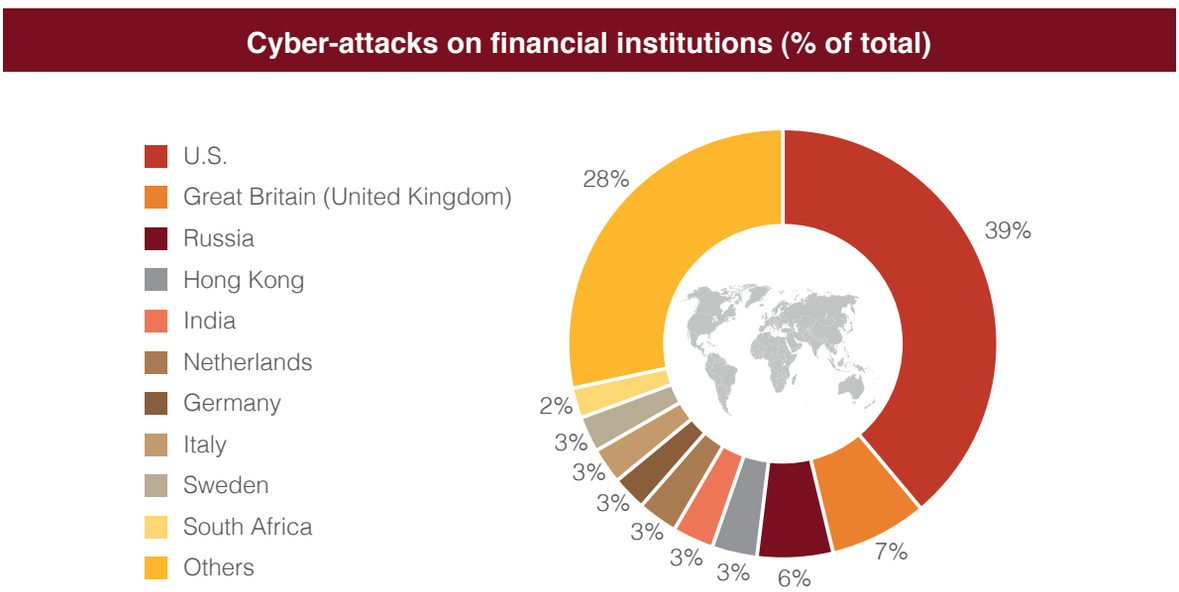


Source: Digital Attack Map, built through a collaboration between Google Ideas and Arbor Networks (accessed on 14 May 2020)

Cyber risks faced by financial institutions in Hong Kong also should not be understated. According to the IMF staff's findings, while advanced economies (including the US and the UK) account for a majority of successful attacks on financial institutions, Hong Kong represented 3% - comparable to counterparts such as Italy and India (see Figure C).[23]

[23] International Monetary Fund, IMF Working Paper – Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, June 2018.

Figure C



Sources: ORX News, IMF staff calculations

The economic losses resulting from cybercrimes also gives more insight into the severity of cyber risks which Hong Kong is facing. A 2018 Frost & Sullivan study commissioned by Microsoft revealed that the potential economic loss in Hong Kong due to cybersecurity incidents may hit US$32 billion, about 10% of Hong Kong's GDP.[24] In particular, a large-sized organisation (i.e., with 500 employees or more) could potentially incur an economic loss of US$24.9 million, over 650 times the average estimated economic loss for a mid-sized organisation (i.e., 250 to 499 employees).[25]

As for actual financial losses, Hong Kong companies and residents lost more than HK$2.9 billion (US$372.63 million) to cybercriminals in 2019.[26,27] In the securities brokerage sector, for example, for the 18 months ended 31 March 2017, the Securities and Futures Commission ("SFC") received close to 30 cybersecurity incidents, most of which involved hackers gaining access to customers' internet-based trading accounts with securities brokers resulting in unauthorised trades totalling more than HK$110 million (US$14.2 million).[28]

Of course, one could argue that the above statistics do not qualify as conclusive evidence to prove that Hong Kong is exposed to greater cyber risk than other major economies, but the number of cybercrimes and amount of financial losses should suffice to suggest at the very least that **Hong Kong is a key target for cyberattacks**. Echoing the LexisNexis report, Hong Kong has emerged as a 'prime target' for cyberattacks, given that the city is a "*significant financial centre and boasts one of the highest per capita incomes globally. These factors, combined with a more advanced digital economy, makes Hong Kong one of the main focuses for cybercrime in the APAC region*".[29]

[24] Microsoft, Cybersecurity threats to cost organizations in Hong Kong US$32 billion in economic losses, June 2018.
[25] Ibid.
[26] InfoSec (under Office of the Government Chief Information Office), Computer Related Crime: Recent Statistics, last updated in March 2021.
[27] A deeper-dive of the recent figures (from Cyber Security and Technology Crime Bureau, Hong Kong Police) include: in 2019, internet deception under general technology crime recorded a total of 5,157 cases accounted for 62% of the overall 8,322 cases of technology crimes; in H1 2020, number of technology crime cases involving virtual currencies recorded a y-o-y increase of 1,060% (58 cases in H1 2020), incurring a total loss of HK$23 million.
[28] Securities and Futures Commission, Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading, May 2017.
[29] See footnote 10.

Hong Kong's cybersecurity preparedness

While the elevated level of cyber risk facing Hong Kong is alarming, that fact should not be used as an excuse to scale back on adopting new technologies. Instead, the focus should be on how to strike a balance between the extent of cybersecurity measures applied and market/business development.

With this, the question to ask is whether Hong Kong is sufficiently prepared to prevent, address and/or handle the cyber risks it is facing. Research and surveys on the overall cybersecurity preparedness of Hong Kong, as an economy or jurisdiction compared to others, is limited. Most researchers or international organisations (such as the International Telecommunication Union ("ITU") – a specialised agency of the United Nations compile their global cybersecurity indices by 'countries', with the result that a market like Hong Kong is often not given a dedicated score or ranking. Nonetheless, survey findings on the level of preparedness within Hong Kong across the business sector which serve as a useful reference.

In short, **the level of preparedness within Hong Kong is uneven**. The Hong Kong Productivity Council and HKCERT developed a framework to compile the Hong Kong Enterprise Cyber Security Readiness Index to keep track of the status of local cybersecurity awareness and readiness in business sectors. In 2020, the overall cybersecurity readiness of Hong Kong enterprises is 46.9 out of 100, falling at the lower end of the "Basic" category, a decrease of 2.4 over the previous year.[30] Of the six sectors studied, the financial services sector demonstrated the highest level of readiness, at 62.9, at the "Managed" category.[31] For companies outside of the financial sector, the level of readiness was much lower with specific weakness identified in relation to non-technical solutions (such as training, awareness building, processes, etc.). This could indirectly threaten financial intuitions in Hong Kong given that cyber risk is a cross-sectoral issue – for example, the availability of private or confidential information about their individuals can be used for potential targeted attacks on their accounts with financial institutions. Further, across the four assessed areas of the Index, human awareness was the one in which all industries scored the lowest.

This uneven level of cybersecurity preparedness is immensely felt by some cybersecurity experts in Hong Kong. Between May and June 2020, the FSDC conducted several rounds of discussions with seasoned cybersecurity practitioners in Hong Kong,[32] who unanimously agree that financial industry of Hong Kong is better prepared than other industries. Yet, even across the financial industry, institutions have varying levels of readiness, with larger institutions being able to afford the increasing resources required to enhance their cybersecurity infrastructures while smaller ones remain static. Working under the common misconception that cybersecurity is interchangeable with 'technology', some institutions have sought IT-related certifications without a sensible purpose.

According to the experts interviewed, the generally weak level of individual/personal awareness towards cyber risks is a key challenge for Hong Kong (and indeed other parts of the world). While institutions tend to place more emphasis on corporate cyber infrastructures, the "human element" is commonly neglected. Individuals – including each and every user of financial services or practitioner within the industry – can largely impact the cyber resilience of the financial services industry. This is demonstrated by the fact that human error has been a primary reason behind many of cybersecurity breaches. These breaches occur due to human errors such as configuration mistakes or arise from subcontracting the work to third parties who have insufficient understanding of the server needs. Particularly, when new (virtual) joiners attempt to challenge traditional financial institutions for market share, some tend to push the systems out at speed, overlooking misconfiguration issues.

[30] Hong Kong Computer Emergency Response Team Coordination Centre, SSH Hong Kong Enterprise Cyber Security Readiness Index 2020 Survey, April 2020.
[31] ibid.
[32] Practitioners with more than 15 years of experience in cybersecurity-related work at financial institutions, universities and FinTech startups.

Hong Kong should maintain a cyber-safe yet business-friendly environment

As explained above, although Hong Kong is a key target of cyberattacks, the city – especially its financial service industry – has some degree of preparedness for these attacks. However, this attack-versus-preparedness battle is constantly evolving as the future cyber universe will only become more complex.

As acknowledged by the World Economic Forum staff and others,[33] cyberattacks will likely become more ubiquitous and sophisticated. With the use of artificial intelligence (e.g., Emotet Trojans), cyber attackers can learn from failed attempts, modify and relaunch even more scalable, customised attacks from which neither a sector nor a financial centre can be immune. The future of cybersecurity will likely be driven by a new class of subtle yet sophisticated attackers.

This is especially a challenge for an international financial centre like Hong Kong, given that the financial services industry is, by its nature, particularly vulnerable to cyber risk and its rapidly evolving nature. Financial institutions place significant reliance on critical financial market infrastructures such as payment and settlement systems, trading platforms, central counterparties, etc. A single point of failure in a piece of critical infrastructure, triggered by a cyber-attack, can have a ripple effect impacting various other parts of the financial system. For example, both the RTGS and SWIFT systems, given their importance to cash and securities payments and settlements, are potential 'single points of failure'.[34] A cyberattack on such systems could result in consequences beyond those systems and their participants to the entire financial markets – e.g., if SWIFT were not able to submit payment instructions, due to cyberattacks, the consequence could be widespread liquidity dislocations.[35] Markets with relatively short settlement cycles (e.g., markets for uncollateralised overnight loans and repurchase agreements) would especially be affected.[36]

While rapid technological development brings more convenience and efficiency to businesses and individuals, it also leads to increasing complexity of cybersecurity issues for Hong Kong. With developments such as the introduction of virtual financial services since 2018 (through, for example, virtual banks and virtual insurers), the use of online/remote virtual services will naturally increase and, thus likely result in cybersecurity becoming more closely intertwined with and indispensable to the financial services industry.[37] In the post-COVID-19 era, financial institutions are experiencing a transformation in how they operate – from a physical, office-based mode more to a virtual/remote mode, through cloud, online collaboration tools, etc. Together with the coming of the fifth generation (5G) network coverage and other Smart City infrastructures, all these rapid changes will exponentially increase the opportunities for hackers and cybercriminals to exploit.

[33] World Economic Forum, 3 ways AI will change the nature of cyber attacks, June 2019.
[34] World Economic Forum, Understanding Systemic Cyber Risk, October 2016.
[35] Ibid.
[36] Ibid.
[37] Other incorporation of technology into financial services, for example in the Know-Your-Client process, is also relevant and being studied by the FSDC separately.

As referenced in the previous paragraph, financial services institutions in Hong Kong have been forced to adapt to a more remote and online business model since the onset of the Covid-19 pandemic. This was an area of concern in the context of investment product sales which have traditionally required some level of face-to-face interaction as part of account opening, anti-money laundering, and suitability procedures, as well as consumer protection safeguards. Those face-to-face requirements also provided some level of protection against cyber risk. Hong Kong financial regulators, including the SFC, Hong Kong Monetary Authority ("HKMA") and Insurance Authority ("IA"), recognised the urgent pressures facing its regulated population as a result of Covid-19 and responded by permitting financial institutions more flexibility in using remote/online solutions, building on moves that the regulators had been making in recent years with the advent of FinTech and online sales platforms.[38] Although these moves assisted financial sector participants in maintaining business levels while employees were working from home, they also exposed such institutions and their staff to a greater degree of cyber risk. The SFC expressly recognised this with its 29 April 2020 circular addressing the management of cybersecurity risks in light of the increased use of remote office arrangements, in which it reminded licensed corporations to "*assess their operational capabilities and implement appropriate measures to manage the cybersecurity risks associated with these arrangements*".[39]

The fast-changing landscape is truly challenging for a financial centre. On the one hand, there is the need for cyber safety; on the other hand, the precautionary (or regulatory) measures cannot go so far that they hinder the further development of the market. In this uphill battle of maintaining a cyber-safe yet business-friendly environment, Hong Kong needs a clear, up-to-date cybersecurity policy direction.

[38] Insurance Authority, Circulars - Temporary Facilitative Measures to tackle the Outbreak of Covid-19, February & March & June 2020 (allowing non face-to-face distribution methods for certain types of insurance policies);
Hong Kong Monetary Authority, Circular - Coronavirus disease (COVID-19) and Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) measures, April 2020 (encouraging the fullest use of reliable digital customer on-boarding); and
Securities and Futures Commission, Circular - Extended deadlines for implementation of regulatory expectations and reminder of order recording requirements under COVID-19 pandemic, March 2020 (alternative order receiving and recording options).

[39] Securities and Futures Commission, Circular - Management of cybersecurity risks associated with remote office arrangements, April 2020.

From precaution to business opportunities for Hong Kong

The value proposition of a robust cybersecurity framework is not limited to the precautionary (or protective) dimension. It can also serve as a foundation of developing business opportunities for the financial services industry.

Development of a cyber-insurance market is one such opportunity. The global cyber insurance market is expanding quickly, with an annual growth rate to be approximately 20% - 25%.[40] In 2019, the market for cybersecurity insurance was at US$7.36 billion; by 2025, it is forecast to reach US$27 billion.[41] While conventional cyber insurance products (such as those covering data breach, extortion, cybercrime and fraud etc.) mainly focus on protecting digital assets against losses caused by cyber risks, the future cyber insurance market will likely be expanded to insure the cyber risks of intangible assets such as cryptocurrency and other digital assets.[42]

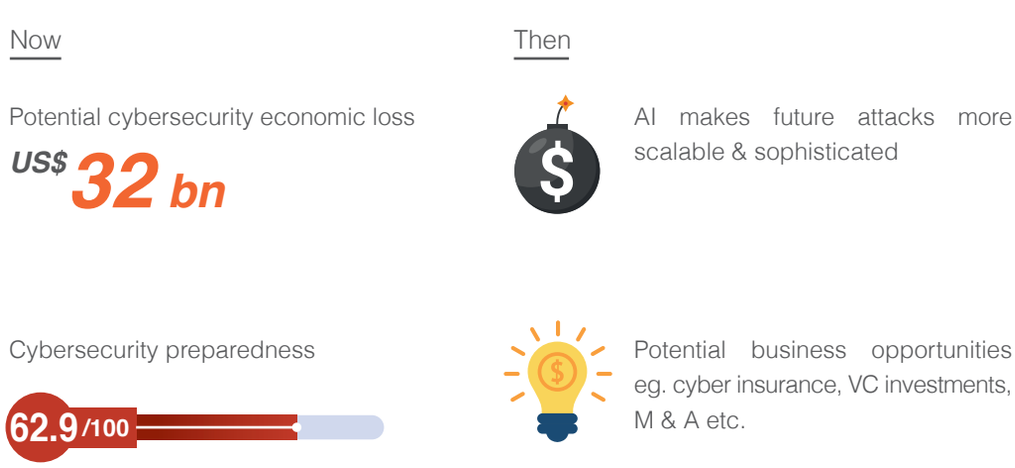
The global demand for cyber-insurance is growing while the take-up remains patchy. For now, the market of cyber insurance is largest in the US and most firms that offer these policies are US-based.[43] According to a survey report issued by a specialist insurer in April this year, a third of the surveyed US firms had standalone cyber insurance cover.[44] In Europe, activities in this regard are also increasing – for example, two prominent insurance firms based in Germany announced, in March 2021, their partnership with a major cloud provider on cyber insurance, combining their cloud-specific security expertise and risk transfer expertise. Meanwhile, that demand is present in Hong Kong as well. In 2018 alone, the city faced over 7,800 cybercrime cases, accounting for more than HK$2.7 billion of financial losses.[45] Another survey conducted by a major insurer indicated that 76% of small- and-medium-sized enterprises in Hong Kong experienced a cyber-incident in 2019, with about a third of those companies taking no further action after the incident. Given the above, several international insurance companies are developing their businesses to serve this underinsured population, with an aim to better measure, mitigate and transfer the increasing cyber-related risks for their clients.[46,47]

[40] KPMG, Seizing the cyber insurance opportunity, July 2017.
[41] Sjouwerman, S. (2020). Cyberheist: The biggest financial threat facing American businesses since the meltdown of 2008. Clearwater, FL: KnowBe4.
[42] Lloyd's, Lloyd's launches new cryptocurrency wallet insurance solution for Coincover, February 2020.
[43] See footnote 40.
[44] See footnote 14.
[45] See footnote 25.
[46] 蘋果日報, QBE：網絡保險查詢大增, June 2019. (in Chinese only)
[47] 明報, 網絡保險興起 AIG：保費年增四成 亞洲網絡攻擊風險高 市場潛力大, December 2018. (in Chinese only)

Venture capital investment in cybersecurity-focused companies is also rising, as are mergers and acquisitions (M&A) activities. Venture capital investors increasingly recognise the business potential that cybersecurity products and applications could bring, for example, through using machine learning to develop security solutions for enhancing client experience. The breadth and depth of the cybersecurity business is being increasingly explored. In 2018, a total of US$6.4 billion in venture capital investment went to cybersecurity companies, according to KPMG.[48] As of Q3 of 2019, cybersecurity companies constituted US$5.8 billion of venture capital investments through a total of 388 deals.[49] Most deal targets were from Israel and Europe. Further, M&A has become a popular exit strategy for many cybersecurity startups. For example, in Q3 of 2019 US-based cybersecurity company Palo Alto Networks acquired container security company Twistlock in an effort to extend its cloud security reach.[50]

In order to address both the need for protection against evolving cyber risks and development of potential business opportunities in the cybersecurity sector, Hong Kong should strive to continually improve and enhance its cybersecurity framework.

Why is cybersecurity relevant to Hong Kong 's financial services industry



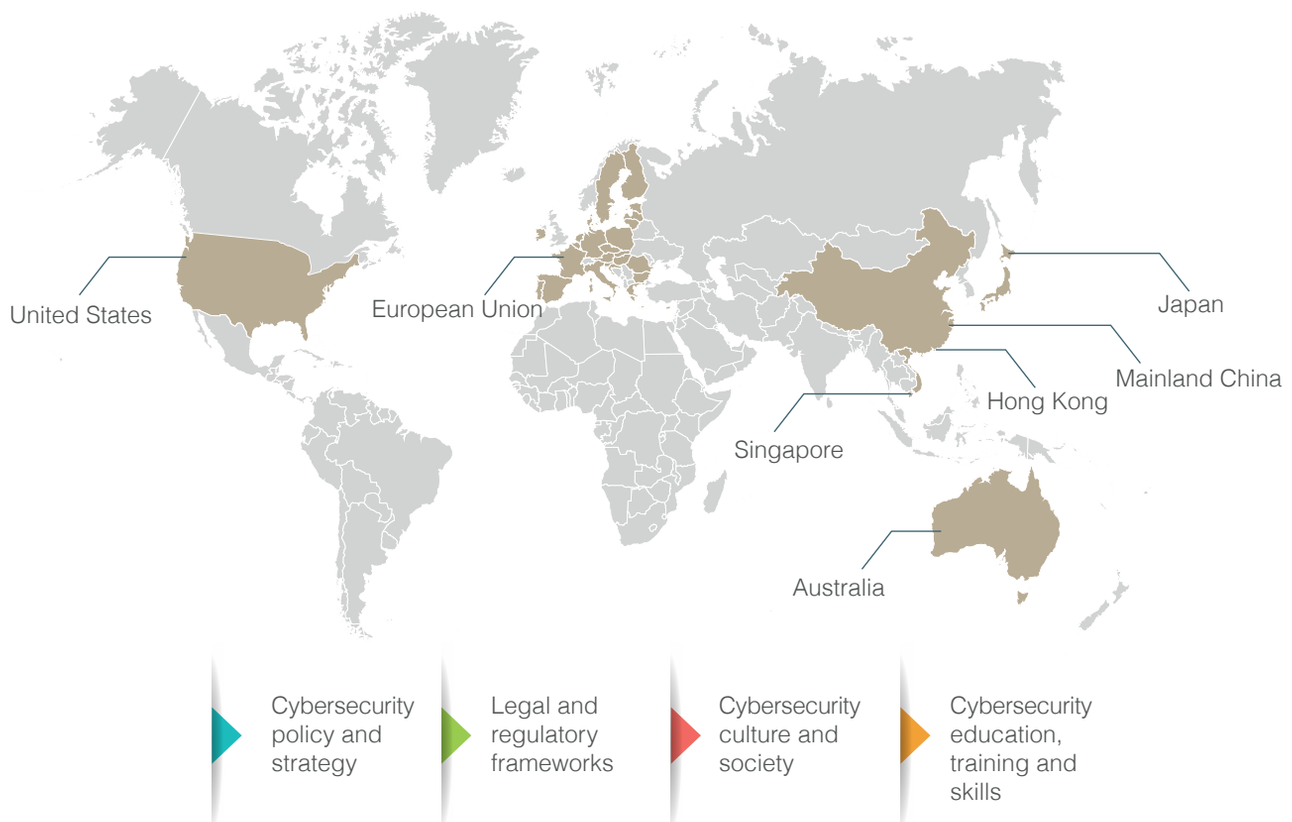
Sources: Frost & Sullivan, Microsoft, Hong Kong Productivity Council, HKCERT, World Economic Forum, KPMG

[48] KPMG, Venture Pulse Q3 2019, October 2019.
[49] Ibid.
[50] Ibid.

Hong Kong Is Keeping Pace but Not a Leader

As mentioned above, cybersecurity is a tricky topic – cyber risk is difficult to measure or quantify, as is the cyber resilience of a particular place. In general, while there is no clear leader in the cybersecurity space, it is fair to say that some jurisdictions are considered relatively 'more developed' than the others. As indicated in various research studies,[51] Australia, the European Union ("EU"), Japan, Mainland China, the US and Singapore are often named as jurisdictions associated with having an advanced cybersecurity framework. Given this, we have conducted a jurisdictional survey of Hong Kong's cybersecurity framework against each of these five jurisdictions.[52]

Drawing reference from part of the Cybersecurity Capacity Maturity Model for Nations developed by the Global Cyber Security Capacity Centre at Oxford University,[53] the jurisdictional survey covers the selected jurisdictions' approaches across four key dimensions: (i) cybersecurity policy and strategy; (ii) legal and regulatory frameworks; (iii) cybersecurity culture (and society); and (iv) cybersecurity education, training and skills. A survey of these approaches is not to suggest one way is better than the other, but at a minimum it can provide a helpful reference for Hong Kong as it considers its way forward to fill the gaps in its framework and keep pace with other leading jurisdictions.



[51] Various research studies, such as "Safe Cities Index 2019" by the Economist in terms of 'digital security', have been considered.
[52] Key features of the cybersecurity frameworks of the selected jurisdictions and Hong Kong and set out in **Annex**.
[53] This is a "first of its kind" model to review cybersecurity capacity maturity across the five key dimensions, with an aim to enabling governments to "self-assess, benchmark, better plan investments and national cybersecurity strategies, and set priorities for capacity development".

Cybersecurity policy & strategy

A common feature of cybersecurity frameworks of other markets is to develop centralised strategy or policy direction dedicated for cybersecurity; meanwhile, **in Hong Kong, cybersecurity policy direction is blended into the broader Smart City Blueprint**. As part of the Smart City Infrastructure, the Government has the vision to enhance its cybersecurity capability to "address new security risks, facilitate collaboration among stakeholders to promote awareness and incident response capability in the community". To this end, the Government publishes policies and guidelines on cybersecurity on a regular basis, groom and attract talent on cybersecurity, and participates in global and regional cybersecurity organisations for enhancing information exchange. Hong Kong adopts a multi-stakeholder approach to strengthen the cyber resilience of Hong Kong. That means, work or obligations related to cybersecurity rests under various government bureaus and agencies.

In comparison, some of the jurisdictions reviewed in the survey have chosen to establish a centralised strategy specifically for cybersecurity related matters. For instance, the EU's strategy, updated in December 2020, sets out their approach on priority areas such as increasing the level of cyber resilience of critical public and private sectors, and enhancing operational capacity to reduce cybercrime (including the establishment of a new Joint Cyber Unit to strengthen cooperation between the EU and its member states). Similarly, following a 2018 update to the US national cyber strategy which itself built upon earlier cybersecurity initiatives by successive administrations, and in the aftermath of the unprecedented SolarWinds cyberattack, the new US administration has acted quickly to outline its cyber strategy, noting that it will "make cybersecurity a top priority, strengthening our capability, readiness, and resilience in cyberspace."[54] Likewise, the Australian government in 2020 launched an updated cybersecurity strategy, replacing the earlier 2016 version. The revised strategy, which has a stronger focus on deterrence and security than the prior version, is accompanied by a AUS$ 1.67 billion investment over 10 years to strengthen cyber resilience and security. Finally, Singapore also took the opportunity in 2020 to announce a "Safer Cyberspace Masterplan", building on its 2016 Cybersecurity strategy and focusing on, amongst other things, securing core digital infrastructure and safeguarding cyberspace activities for its population.

Legal & regulatory frameworks – financial industry specific

In terms of the overall cybersecurity legislation, **Hong Kong does not have a standalone set of cybersecurity legislation or an independent enforcement agency**, as some other leading jurisdictions do. Nonetheless, there are ordinances which address cyber- or computer- incidents. Various sectoral regulators, particularly in the financial sector (e.g., HKMA, IA and SFC), have also introduced cybersecurity regulations and other initiatives for their respective sectors – their approach is rather light-touched and on a micro level. Further, Hong Kong has a personal data privacy and protection framework – in the form of the Personal Data (Privacy) Ordinance ("PDPO").

The EU, Japan, Mainland China and Singapore have a combination of standalone cybersecurity or cyberspace protection legislation (as an umbrella under which other regulations or initiatives are made) and some pieces of financial industry specific regulations/guidance. Apart from a standalone cybersecurity statute, most of these jurisdictions also have data privacy and protection legislation. In particular, the European and Singaporean statutory frameworks provide for mandatory breach notification in cases where there has been a material breach of data privacy/data protection rights (for example, as a result of a large-scale hacking incident).

[54] The White House, Interim National Security Strategic Guidance (March 2021).

In relation to the financial sector, **Hong Kong's financial industry regulations and guidance on cybersecurity / cyberspace protection are sector-specific. Each regulator tends to have its own regulations/guidance for financial institutions that are licensed under their respective purviews**. Some of the key regulations/guidance include:

- The SFC's "Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading" encourages protection of client internet trading accounts through two-factor authentication processes, monitoring and mechanisms,[55] prompt client notification, data encryption and stringent password policies;[56] in relation to COVID-19, the SFC issued a circular in April 2020 reminding licensed corporations to assess their operational capabilities and implement appropriate measures to manage cybersecurity risks associated with remote office arrangements;[57]

- The HKMA has its Cybersecurity Fortification Initiative ("CFI"), comprising: (i) the Cyber Resilience Assessment Framework (C-RAF) (a two-part self-assessment and intelligence-led Cyber Attack Simulation Testing (iCAST) to help AIs evaluate their cyber resilience); (ii) the Professional Development Programme (PDP) (certification scheme and training program for cybersecurity professionals); and (iii) the Cyber Intelligence Sharing Platform (CISP);[58,59] and

- The IA's "Guidance Note on the Corporate Governance of Authorised Insurers" (section 7.17) requires an authorised insurer to identify cybersecurity threats arising from network, email and relevant devices,[60] and its "Guideline on Cybersecurity" sets out the minimum standards of cybersecurity that are expected of an Authorised Insurer.[61]

Mainland China's approach is similar to that in Hong Kong. The China Securities Regulatory Commission and China Banking and Insurance Regulatory Commission, amongst others, have their respective regulations and guidance in relation to cybersecurity.

By contrast, cybersecurity regulations specific to the financial industry in other jurisdictions tend to be all-embracing, mainly owing to their super-regulator structure. For example, the primary set of cybersecurity regulations covering financial institutions in Singapore is the Monetary Authority of Singapore's Technology Risk Management Guidelines (updated in January 2021 to reflect the fast-moving cyber threat landscape) and associated circulars and notices. In Japan, regulations and guidelines in this regard are mainly prescribed by the Financial Services Agency.

---

[55] Securities and Futures Commission, Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading, October 2017.

[56] Securities and Futures Commission, Circular to All Licensed Corporations Alert for Ransomware Threats, May 2017.
Securities and Futures Commission, Circular to Licensed Corporations Engaged in Internet Trading Good Industry Practices for IT Risk Management and Cybersecurity, October 2017.

[57] Securities and Futures Commission, Circular to licensed corporations Management of cybersecurity risks associated with remote office arrangements, April 2020.

[58] The HKMA launched the Cybersecurity Fortification Initiative (CFI) in 2016, with a view to raising the cyber resilience of Hong Kong's banking system. The HKMA

[59] has recently completed a review of the CFI and introduced an enhanced version (CFI 2.0) in November 2020. Major enhancements include incorporating recent international sound practices on cyber incident response and recovery under the Cyber Resilience Assessment Framework (C-RAF) and expanding the certification list under the Professional Development Programme (PDP) to include equivalent qualifications in major overseas jurisdictions.

[60] Hong Kong Monetary Authority also launched the "Enhanced Competency Framework on Cybersecurity" in December 2016 (updated in January 2019) in parallel with the CFI, to enable talent development and facilitate the building of professional competencies and capabilities of those working in cybersecurity. In October 2017, the HKMA issued a circular to CEOs of Registered Institutions requiring them to apply the SFC Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading. Further, HKMA exercises its supervision over authorised institution's information systems through regular on-site examinations, off-site reviews and prudential meetings. HKMA takes a risk-based approach to compliance, requiring different benchmarks and review cycles for institutions with different risk profiles.

[61] Insurance Authority, Guidance Note on the Corporate Governance of Authorized Insurers, October 2016.

[62] Insurance Authority, Guideline on Cybersecurity, June 2019.
Failure to comply with the Guideline does not by itself render an authorised insurer liable to any judicial or other proceedings, but codes or guidelines are admissible in evidence in any proceedings under the Insurance Ordinance before a court. The IA will also have regard to the codes and guidelines when taking disciplinary actions.

Cybersecurity culture

With human error being one of the main causes of cybersecurity incidents, the cultivation of cyber resilience awareness amongst individuals and enterprises is an area of increasing focus. As stated in earlier paragraphs, **the level of preparedness in Hong Kong's business sector for cyber incidents is improving but remains uneven across different industries**. To incentivise organisations to improve their cyber resilience, the Innovation and Technology Bureau has offered subsidies to enterprises of all sizes to put in place cybersecurity measures (subject to certain requirements) under the Technology Voucher Programme since November 2016.[62] This programme focuses more on the technological services and solutions perspective, as opposed to the individual user/practitioner level. To cultivate awareness of collaboration in cyber security, the Partnership Programme on Sharing of Cyber Security Information (Cybersec Infohub) enables industries and enterprises to, amongst others, share information on cybersecurity related matters.[63] Turning more broadly to personal data processing in Hong Kong, there is relatively little engagement of the public as data subjects in promoting their cybersecurity awareness.

Culture takes time to be cultivated and our European counterparts have been early movers in this regard, having put in place data protection legislation since 1998. Under the General Data Protection Regulation ("GDPR") which came into effect in 2016, data subjects in the EU are given a series of rights in relation to the processing of their personal data, including a right to access personal data, right of rectification of personal data, right of erasure of personal data, and a right to object to the processing of personal data.[64] Data subjects in the EU have made use of these data protection rights provided by the GDPR at a swift pace.[65] For instance, an airline was facing a £500 million class action lawsuit in a UK court for non-material damage caused by a security breach.[66] Further, the UK's Information Commissioner's Office announced its intention to fine a hotel group and an airline for data breaches under GDPR.[67,68]

The US takes an alternative approach through developing the cyber workforce of the future and catalysing the next billion-dollar company. For example, New York's Cyber NYC, a US$100m public-private investment, was launched in 2017 aiming at turning the city into a capital of cybersecurity.

As for Australia, a 2018 CEO survey noted that 89% of Australian respondents said they were concerned about cyber threats (up from 80% the previous year); however, only 44% surveyed said they were investing more heavily in cybersecurity protection in order to build trust with customers.[69]

[62] The Bureau has also worked with the Hong Kong Internet Registration Corporation Limited in providing free website scanning services for SMEs. It has maintained the Cyber Security Information Sharing and Collaborative Platform to allow the sharing of cybersecurity intelligence between organisations. Amongst other incentives, the Hong Kong Computer Emergency Response Team Coordination Centre provides free 24-hour hotline services for organisations to report cybersecurity incidents and to give recommendations on how to respond.

[63] Cybersec Infohub is a cross-sectoral, public-private-partnership programme that promotes closer collaboration among local information security stakeholders of different sectors to share cybersecurity information and jointly defend against cyberattacks. More than 360 organisations from a wide spectrum of industries had joined as at January 2021.

[64] Also for information, PDPO of Hong Kong provides for right to request access to personal data and the right to request correction of personal data.

[65] The Law Reviews, The Privacy, Data Protection and Cybersecurity Law Review (Edition 6) - European Union Overview, October 2019.

[66] Ibid.

[67] Information Commission Office, Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, July 2019.

[68] British Broadcasting Company ("BBC"), British Airways faces record £183m fine for data breach, July 2019.

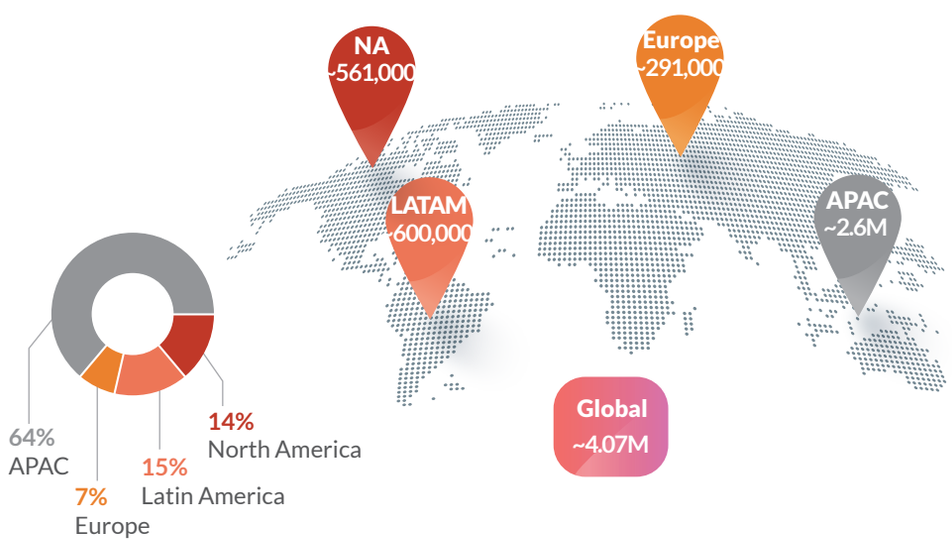
[69] PwC, Infographic: How cyber aware is Australian business?, March 2018.

Cybersecurity education, training & skills

The cyber talent pool has long been considered deficient. According to an international information system security certification consortium called (ISC)2, the shortage of cybersecurity professionals was close to 4.3 million globally and the cybersecurity workforce needs to increase by a staggering 145% to cope with the surge in demand.[70] On the organisation level, about 65% of the surveyed organisations expressed they were experiencing a shortage of cybersecurity staff. On the regional level, APAC experienced the highest talent shortage, at around 2.6 million (see Figure D). **In Hong Kong, of the 98,780 IT employees in 2018, only 1.2% specialised in IT security.**[71]

Figure D

Cybersecurity workforce gap by region



Source: "Cybersecurity Workforce Study 2019", (ISC)²

The relatively narrower talent gap in Europe can be attributed to a number of reasons. As some cybersecurity experts pointed out, in various European countries, military defence training has incorporated a strong emphasis on cybersecurity, which to some extent helps the countries groom a sustained pool of cybersecurity experts. Further, Europe's cybersecurity education & training strategy is generally considered organised and structured, and thus effective. The European Union Agency for Cybersecurity ("ENISA"), the EU agency overseeing cybersecurity, supports many initiatives for raising awareness of and providing education on cybersecurity issues. These include (amongst other things) the development of Cybersecurity Training material and a European Cybersecurity Skills Framework, and guidance for improving cyber security culture within private sector organisations. To enhance the competency of practitioners, a number of cybersecurity certification schemes have evolved, aimed at providing a comprehensive set of rules, technical requirements and standards to assess the knowledge of scheme participants.

Comparatively, in Asia, capacity-building initiatives related to cybersecurity have a shorter history.

[70] (ISC)², Cybersecurity Workforce Study 2019, November 2019. As supplementary information, various markets conducted their research to gauge the talent shortage issue. In the 12 months that ended in August 2018, there were more than 300,000 unfilled cybersecurity jobs in the U.S., according to CyberSeek, a project supported by the US-government-involved National Initiative for Cybersecurity Education. In addition, the UK government published a research report in March 2020, suggesting that close to 400,000 cybersecurity-related job postings were yielded in the UK between September 2016 and August 2019 (a 3-year period).

[71] Legislative Council, Building cyber security talent (ISE15/20-21), 22 January 2021.

In Hong Kong, the government-supported Cyber Security Information Portal ("CSIP") and Cybersechub.hk are the main tools. The former provides advice and step-by-step guidelines for SMEs and other general users to conduct health check on computers, mobile devices and websites, as well as to learn tips and techniques to guard against cyber-attacks;[72] whereas the latter is a platform for industries and enterprises to exchange cybersecurity information.[73] To cultivate the awareness of businesses and the public on cybersecurity, the Government and the private sector organise regular seminars and workshops, amongst other initiatives.[74]

That said, **Hong Kong does not have an educational institution dedicated to cybersecurity training**, as some other jurisdictions do. For example, Australia established the Academic Centres of Cyber Security Excellence ("ACCSE") in 2016 to address the national shortage of highly-skilled cyber security professionals by encouraging more students to undertake studies in cyber security and related courses;[75] Mainland China plans to open 4-6 cybersecurity academies by 2027;[76] and Singapore has established the Cyber Security Associates and Technologists (CSAT) Programme to train and up-skill fresh ICT professionals and mid-career professionals for Cyber Security job roles.[77]

In relation to industry-specific training, the current offerings in Hong Kong are rather fragmented. **On the positive side, the banking sector has made a good start with an enhanced competency framework on cybersecurity.** The framework, developed by the HKMA and other sector stakeholders, facilitates the building of professional capabilities of banking staff engaged in cybersecurity duties. Banks can refer to the HKMA's guide which contains details of the qualification structure, recognised certificates and continuing professional development requirements to equip relevant staff with the appropriate skills, knowledge and behaviours.[78] As for the rest of the financial industry (such as the securities and insurance sectors), institutions can refer to various cybersecurity workshops, for example such co-hosted by the SFC, the Hong Kong Police Force and the Hong Kong Computer Emergency Response Team Coordination Centre, that cover key topics (such as cybercrime prevention tips) on a macro basis. However, with the absence of guidance similar to HKMA's, it depends largely on the financial institutions' or the staffs' own initiatives in taking corresponding training to fulfil the high-level competency regulatory requirements.

---

[72] Cybersecurity Information Portal, About Us, last updated in September 2020.

[73] Cybersec Infohub, About Us, last updated in November 2019.

[74] Apart from seminars and workshops to encourage and support the industry in information security training, the Government also works with professional bodies to promote professional accreditation in information security among IT practitioners and encourages tertiary education institutions to provide more information security courses in relevant disciplines.

[75] Academic Centres of Cyber Security Excellence ("ACCSE"), Program Guidelines, last updated in May 2017.
The ACCSE program gives recognition to Australian universities that successfully demonstrate high-level cyber security education and training competencies, research capability and strong connections to government and the business sector.

[76] Ministry of Education of the People's Republic of China, 關於印發《一流網絡安全學院建設示範項目管理辦法》的通知, August 2018. (in Chinese only)

[77] Cyber Security Agency of Singapore, Cyber Security Associates and Technologists Programme, last updated in May 2020.

[78] Hong Kong Monetary Authority's Guide to Enhanced Competency Framework on Cybersecurity, last updated in January 2019.

On the tertiary and continuing education level, universities in Hong Kong were some of the first in Asia to incorporate industry-ready cybersecurity elements into the curriculum (e.g., MSc Cyber Security) to help develop new talent. However, as understood from the FSDC's interviews with seasoned cybersecurity practitioners, those businesses that can afford to hire cybersecurity staff prefer experienced-hires, instead of fresh graduates. Meanwhile, smaller enterprises tend to conflate Information Technology and Cybersecurity as the covering the same subject matter, thus further depressing the market for cybersecurity specialists.[79] In light of the above factors, new cybersecurity graduates frequently consider switching to another field given the lack of entry-level opportunities in the cybersecurity field.

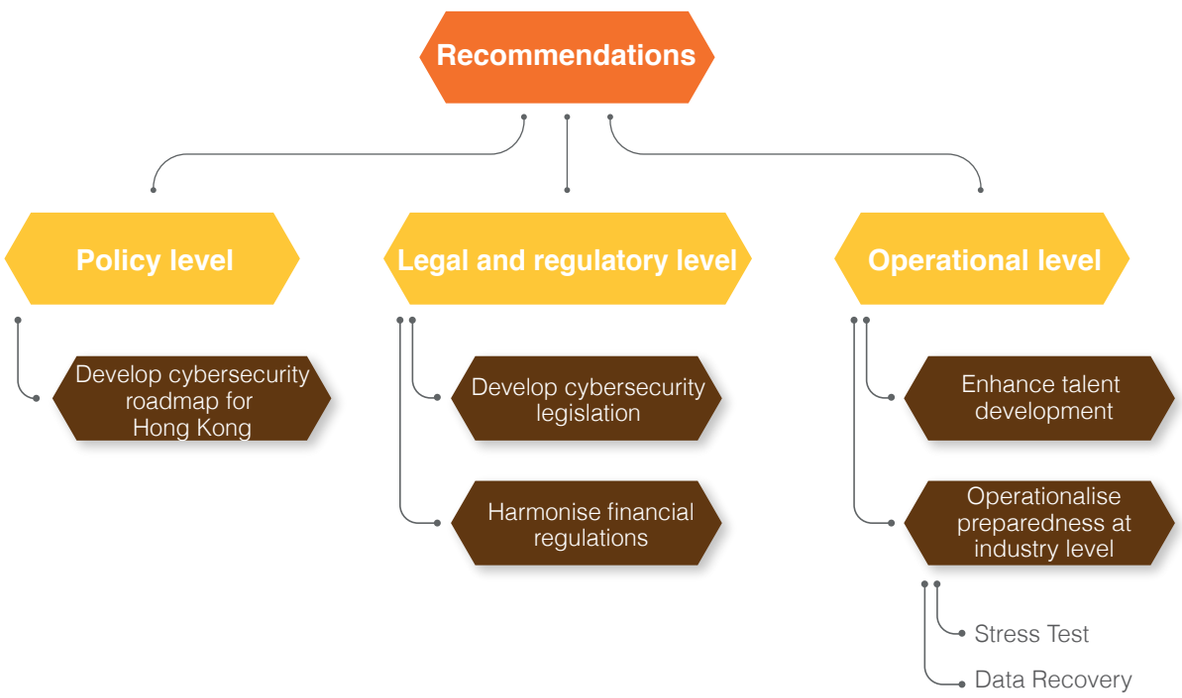
On attracting non-local talents, the Government's Technology Talent Admission Scheme provides a fast-track arrangement for eligible technology companies and institutes to admit overseas and Mainland technology talent (including cybersecurity talent) to undertake research and development work. Also, the Government's Talent List of Hong Kong covers experienced cybersecurity specialists. Eligible applicants who meet the requirements of the Talent List may enjoy immigration facilitation under the Quality Migrant Admission Scheme. Qualifiers under the scheme are not required to have secured an offer of local employment before their entry to Hong Kong; they may also bring their dependents to the city for settlement.

[79] As understood from seasoned practitioners, the skillsets possessed by information technology professionals and cybersecurity professionals are fairly different – with the former being good at 'building' IT infrastructures whereas the latter at dissecting parts to identify errors and potential risks.

Recommendations

Taking into consideration Hong Kong's cybersecurity exposure and the approaches followed by other major jurisdictions, we have mapped out a number of recommendations which we believe will facilitate the enhancement of Hong Kong's cybersecurity capacity and enable it to positively distinguish itself from its global counterparts. At the core of this objective is the need for Hong Kong to formulate a more strategic view on cybersecurity which reflects both the needs of the city as a whole and its position as a leading international financial centre.

The recommendations relate to three broad "levels": (i) policy level; (ii) legal and regulatory level; and (iii) operational level. They are not intended to be implemented sequentially, thus reflecting the reality that some recommendations may take longer to complete than others.



Policy level

(1) Develop a dedicated cyberspace safety roadmap with policy priorities for Hong Kong

Having the element of cyberspace safety incorporated into the holistic Smart City Blueprint is a good start for Hong Kong, both in terms of facilitating related policy formulation and enhancing the overall cybersecurity capabilities. Yet, as cyber threats continue to increase globally at a rapid pace, the city may require policy considerations with priorities and actionable items in the short, medium and longer terms in a more explicit manner under a dedicated set of roadmap, in addition to the existing approach by way of an annual update of the work plan.

Currently, documents in the public domain indicate what the Government has done but there is not as much detail on what the Government plans to do in terms of cybersecurity. For example, we are aware that the Government and its agencies have conducted plenty of seminars and workshops to enhance capabilities among practitioners and the community, but how Hong Kong plans to extend its advantage in the cybersecurity ecosystem and to strengthen its standing as a trusted city with sound cybersecurity infrastructure are perhaps areas that citizens or different industries would be interested in knowing too. While we appreciate the Government's various work initiatives in cybersecurity, it is important to get these initiatives known by the market and by the public so that they can prepare, act and respond accordingly.

With reference to other jurisdictions, there is usually a structured nation/city-wide strategy on cybersecurity, spelling out actionable items under a range of areas, for example – strengthening governance of cyberspace safety by introducing a new act within a certain timeframe, and making Government systems more secure by committing to allocate a certain percentage of government expenditure to cybersecurity. This kind of strategy is, to date, not obviously seen in the public domain of Hong Kong and not well heard of, at least, within the financial services industry. Clearer work plans with policy priorities over a longer time horizon can facilitate different stakeholders, including businesses in Hong Kong, to coordinate and make their part of contribution correspondingly.

Apart from policy priorities, clearer delegation at the organisational/departmental level is considered instrumental. While we understand that cyberspace safety is a cross-sectoral subject matter that can be relevant to more than one government bureau or agency, lucidly-defined accountabilities placed under one overarching governance body can serve both efficiency and comprehensiveness. Workable options for this proposed overarching governance body include: (i) establishing an independent commission (similar to the Australian Signals Directorate,[80] or the Cyber Security Agency of Singapore);[81] or (ii) setting up a cross-bureau/agency working group to coordinate both regulatory and enforcement actions. With such formation, all initiatives related to cybersecurity — from local capacity building, infrastructure review to international partnership — can be brought under a single agency.

The financial services industry, as one of the major pillars of Hong Kong's economy, should play a key role in facilitating the setting of key policy priorities and promoting the ongoing public-private collaboration.

[80] Established as a statutory agency to house the Australian Government's cybersecurity functions.
[81] As part of the Prime Minister's Office and managed by the Ministry of Communications and Information, the Agency oversees cybersecurity strategy, operation, education and so on for Singapore.

Legal and regulatory level

(2) Develop cyberspace protection legislation

As described in this paper, many of the leading jurisdictions in cybersecurity have an omnibus cybersecurity / cyberspace protection law as a core element of their cybersecurity framework. In addition to providing Hong Kong citizens and businesses with a higher degree of legal certainty and protection, a comprehensive cyberspace protection statute would also provide clarity in respect of cross-border data processing and transfers.

Hong Kong should consider introducing its own omnibus Cyberspace Protection Ordinance that covers the following objectives at a minimum:

- identifying and defining 'critical information infrastructure';
- establishing a framework for accountability (including investigating, reporting and enforcement of cyber incidents, including such in the civil and/or criminal litigation manner);
- defining and mandating the type(s) of cyberspace protection information sharing between public and private sectors (for example, about the types of incidents/threats they are facing); and
- establishing a light-touch licensing framework for cybersecurity service providers, where appropriate.

The introduction of such legislation can go hand in hand with the effective operation of the previously mentioned cyberspace safety roadmap.

In addition to the proposed omnibus cyberspace protection ordinance, other related statutes should be reviewed on a regular basis to ensure that they remain fit for purpose and aligned with international standards. These would include ordinances covering cyber-related crimes as well as legislation in relation to other relevant areas such as personal data protections.

(3) Harmonise financial regulations

Given the interconnectedness across different sectors within the financial system, cyber incidents faced by one sector can easily have a spill-over effect on other sectors. An effective cybersecurity framework requires a coordinated approach amongst various financial regulators.

In Hong Kong, financial institutions are generally regulated by the respective financial regulators which license/authorise them to carry out certain business activities in a particular sector. While this institutional architecture has the merits of imposing rules and regulations that are tailored to the needs of and circumstances faced by the particular sector, the potential differences across financial regulations of different sectors may confuse the market, thus hampering the city's business-friendliness.

In respect of cybersecurity, Hong Kong has various sets of regulatory guidance in place – as covered in earlier paragraphs, the HKMA, IA and SFC have their respective guidelines/circulars to assist their licensed/authorised institutions to handle cybersecurity issues. Some degree of coordination is seen – for example, the HKMA issued a circular in 2017 to CEOs of Registered Institutions requiring them to apply the SFC's Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading – but more efforts towards coordinating policy responses have not been made.

A potential area for coordination/harmonisation relates to the reporting timeframe in cases where a cyber incident is detected. Currently, the SFC asks its licensed corporations to report to the SFC "immediately" upon happening of any material cybersecurity incident including ransomware attacks;[82] whereas the IA asks insurers to report the incident "as soon as practicable, and in any event no later than 72 hours from detection" of a relevant incident.[83] While we appreciate that the regulatory approaches adopted by the various regulators are catered for the unique business operations and nature of each sector within financial services, some market participants – especially those who work directly in cybersecurity tasks – express the view that a single reporting timeframe would ease the compliance burden of financial market participants answering to multiple regulators.

A harmonisation exercise across financial sector regulation covering cybersecurity issues would require the efforts of various regulators. An effective means of achieving such coordination can be in the form of a cross-agency steering group. A recent example of such a group is the Green and Sustainable Finance Cross-Agency Steering Group established in May 2020 to,[84] amongst other things, facilitate policy direction and coordination to ensure Hong Kong has a cohesive and comprehensive green and sustainable finance strategy. If implemented in the cybersecurity realm, we would expect for such a steering group to include, at a minimum, the SFC, the HKMA and the IA.

[82] See footnote 54.
[83] See footnote 59.
[84] This Steering Group was initiated by the HKMA and the SFC; other members are the Environment Bureau, the FSTB, HKEX, the Insurance Authority and the Mandatory Provident Fund Schemes Authority.

Operational level

(4) Enhance talent development

Talent shortage has been identified as a critical issue, particularly in Asia. A quick yet costly fix to the talent shortage problem is to import talent from other markets, such as Europe. However, as stated earlier, only the largest financial institutions can afford the high expenses incured. To a certain extent, this explains why the banking sector has been able to achieve a higher level of cybersecurity competency than other sectors.

With the HKMA's introduction of the enhanced competency framework, the market has generally observed an improvement in the cyber resilience of the banking sector. However, given the high level of inter-connectivity among various financial sectors, the banking sector's progress could be undermined if the other sectors do not demonstrate a comparable degree of resilience. Given the above, we recommend that other financial regulators, including the SFC and the IA, consider joining hands to build on the HKMA's competency enhancement framework and develop it into an overarching structure with specialised streams of expertise to meet evolving supervisory requirements in different sectors (some being bespoke while others sharing common features). For example, a list of recommended/approved cybersecurity certification schemes for staff working in the various financial sectors would be a useful starting point.

As cybersecurity is not a direct source of revenue generation, financial institutions (especially corporations with small business operations) may still be reluctant to deploy significant resources to improve their cyber resilience. One approach to help overcome this challenge would be for the Hong Kong SAR Government to provide incentives, such as training subsidies to eligible staff or institutions if they enroll in a cybersecurity certification schemes recognised/approved by the regulators. Specifically, the Government could implement a subsidy programme similar to what it recently did in relation to FinTech professionals – in that case, a new HK$120 million wage subsidy plan was launched on 1 July 2020 to encourage companies in the financial sector to hire 1,000 financial technology professionals over the next 12 months by subsidising the salary of one full-time new hire with HK$10,000 every month for a year as part of the FinTech Anti-epidemic Scheme for Talent Development (FAST).[85]

A longer-term alternative would be for Hong Kong to establish a cybersecurity training institute, consistent with the approach taken by other jurisdictions (i.e., Australia, Mainland China and Singapore). However, this option would require a more in-depth feasibility study by the Government.

[85] South China Morning Post, Hong Kong launches US$15.5 million subsidy plan to encourage companies to hire 1,000 fintech professionals, July 2020.

(5) Operationalise preparedness at industry level

Stress Test

In order to assess Hong Kong's capacity to withstand and tolerate cyberattacks, we recommend that the Government conduct a series of cyber stress tests across the financial services sector.

Works on cyber risk stress testing in Hong Kong have been in silos and are largely focused on the banking sector. The Office of the Government Chief Information Officer (OGCIO), the Cyber Security and Technology Crime Bureau (CSTCB) under the Hong Kong Police Force, and HKCERT have worked closely with different stakeholders to conduct cyber incident drills. For instance, CSTCB offered cyber security drills for virtual banks to raise their preparedness and readiness for cyber security attacks prior to commencing their operation in November 2019. The HKMA also conducts the C-RAF (a two-part self-assessment) and intelligence-led Cyber Attack Simulation Testing (iCAST) to help banking institutions to evaluate their cyber resilience. At the industry-led level, there are annual cyber crisis simulations such as the Whole Industry Simulation Exercise ("WISE"). Conducted in October 2019, the latest WISE drew participants from banks, securities firms, asset management firms and clearing houses with operations in Hong Kong. In the four-hour exercise, crisis-management teams from some 40 financial institutions participated in a simulation in which the fact pattern changed every five to ten minutes[86], with support by regulators[87]. Banks participated in both iCAST and WISE reportedly found the two exercises useful in assessing their cyber resilience. They indicated that there is value in both regulator- and industry-led initiatives, with the former (iCAST) benefitting from wider industry participation, while the latter (WISE) provided valuable insight through confidential institution-specific reports which help banks to pro-actively identify potential weak spots in advance of regulatory audits.

However, stress tests focussing on only a couple of financial sectors are not adequate for a financial centre of Hong Kong's prominence. Given the increasing interconnectedness of different sectors within financial services, as well as the constantly evolving nature of complex cyberattacks, an industry-wide stress test covering all relevant sectors is highly recommended. Further to this recommendation, we would expect that the HKMA, the SFC and the IA coordinate, for example under the FSTB's spearhead, to develop such a stress test as a matter of high priority.

A useful example in this regard is the Hamilton Series in the US. Led by the US Treasury, the Series involves simulations of different types of cyberattacks against the financial services sector, including on individual segments of that sector (for example, equities markets, payment systems, and exchanges). The results of those tests are then used to improve public and private sector policies, procedures and coordination.

[86] Reuters, Hong Kong banks compare pandemic stress test with epidemic reality, February 2020.

[87] The HKMA joined by providing comments on the drill scenarios and interacting with a few participating banks throughout the drill exercise, in order to rehearse its communication and collaboration with the banks in handling the scenarios; meanwhile, the SFC representatives participated in the exercise as Regulatory and Industry Support and Observers.

In planning an industry-wide stress test, Hong Kong's financial sector regulators could either organise the exercise themselves (which would likely ensure greater participation), or encourage financial institutions to plan and conduct their own industry-wide exercise (for example, through subsidising the cost incurred in organising the stress test). While the latter approach has the benefit of allowing financial institutions to conduct the exercise in an environment without fear of regulatory scrutiny, we would recommend that this be a regulator-led exercise given the gravity and nature of the cyber risks facing the industry. For the purposes of reserving flexibility, a 'baseline approach' could be adopted whereby only mission-critical systems and interconnected areas are covered, allowing room for each financial regulator to carry out contingency planning according to their respective operational considerations (as per iCAST and WISE).

Data Recovery

A key question for the Hong Kong financial industry to consider is whether it has in place a suitable cyber incident response mechanism, including an effective and comprehensive data recovery plan. Amid the increasing frequency and severity of cyber threats and incidents, financial institutions, as well as governments and regulators, around the world are exploring ways to best approach data recovery.

Currently, financial institutions in Hong Kong rely predominantly on their own infrastructures to store and recover data, with a view to minimising business disruption and data loss in case of a cyber-incident. Given the nature and volume of data involved, an industry-led initiative is considered to be a more realistic option, at least in the near term.

One of the examples that Hong Kong financial industry participants should consider is the Sheltered Harbour initiative in the US. Driven by the financial industry, this initiative allows the recovery of customer account information in the event of a cyber-incident. Under Sheltered Harbour, participating institutions can store data directly themselves or by third parties. When a cyber-incident occurs, the previously stored data is validated, formatted, encrypted and transmitted through industry-established, standardised file formats. The underlying information is able to be restored and accessible to the impacted participating institution within a week. The merit of Sheltered Harbour is that it can provide an additional layer of protection for financial institutions, which is missing in many markets (including Hong Kong).[88] The initiative is extensively quoted in a recent Bank of England Future of Finance report, indicating that the UK might be considering a similar approach.

[88] Bank of England, The future of finance report, June 2019.

Conclusion

Cyberattacks cause tremendous economic, regulatory and reputational harm to governments and businesses globally. The financial services industry is a prime target of cybercriminals.

As an international financial centre, Hong Kong attracts an increasing number of cybercrimes. In response, the level of readiness among financial institutions to prevent, address and handle cyber risks is considered to have generally increased.

With developments in the post-COVID-19 era – including licensed virtual financial services, increasing reliance on cloud and online collaboration tools, etc. – the future cyber universe will only become more complex and the need to combat cyber risks more urgent. Naturally, this attack-versus-preparedness battle for Hong Kong, and indeed the rest of the world, will be ever growing.

To keep pace with international cybersecurity standards, Hong Kong should consider the cybersecurity frameworks of those jurisdictions widely considered to be leaders in the field. Building on the various approaches taken by Australia, the EU, Japan, Mainland China, Singapore and the US, this paper suggests a number of recommendations that Hong Kong can consider as key steps towards enhancing its cybersecurity framework –

On the policy level –

- to develop a dedicated cybersecurity roadmap with policy priorities for Hong Kong;

On the legal and regulatory level –

- to develop cyberspace protection legislation;
- to harmonise regulations the financial sector;

On the operational level –

- to enhance talent development; and
- to operationalise preparedness at industry level through industry-wide stress test and data recovery enhancement.

The above recommendations could be proceeded in parallel in light of the urgency to present, address and handle cyber risk. We believe that these policy recommendations should lead to a more effective and resilient cybersecurity infrastructure for Hong Kong. However, the ultimate success of the initiative to improve Hong Kong's cybersecurity position relies on full engagement and partnership with the private and public sectors. As such, we very much encourage input from and collaboration with these parties.

Annex – Jurisdictional Survey of Cybersecurity Frameworks

Dimension 1 – Cybersecurity Policy and Strategy

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
Although there is no stand-alone cybersecurity strategy document, cybersecurity policy direction is incorporated into the Smart City Blueprint of Hong Kong. The Government also publishes policies and guidelines on cybersecurity on a regular basis, and participates in global and regional cyber-security organisations for enhancing information exchange. OGCIO and other government-supported organizations have been established to defend against and respond to cyber threats and incidents. The OGCIO has developed and maintained a	The Australian Government launched Australia's Cyber Security Strategy 2020 on 6 August 2020, replacing Australia's 2016 Cyber Security Strategy. The revised strategy, developed by the Department of Home Affairs, is more robust from an enforcement, security, and deterrence perspective than the 2016 strategy which was developed by the then Prime Minister and more focused on economic opportunities and innovation. Under the new strategy, the government will invest AUD1.67 billion over 10 years to achieve the vision of creating a more secure online world for Australia.	The EU Cybersecurity Strategy (first announced in 2013) details actions to address challenges under five priority areas: achieving cyber resilience; drastically reducing cybercrime; developing cyber defense policy and capabilities; developing industrial and technological resources; and establishing a coherent cyberspace policy for EU. In September 2017, the EU updated its Cybersecurity Strategy to further improve the protection of European critical infrastructure and to boost the EU's digital self-assertiveness towards other regions of the world.	The cabinet-led Cybersecurity Strategy Headquarters established in 2015 under the Basic Act on Cybersecurity (2014) is responsible for developing strategies for cracking down on cyber-attacks and mitigating any damage caused. The National Center of Incident Readi-ness and Strategy for Cybersecurity ("NISC") announced its National Strategy for Cybersecurity in July 2018 (covering a three-year period), which identified an increasing need for reinforcing cybersecurity measures across Japan. Among other things, it aimed to improve the cybersecurity of Japanese critical	China started to form its cybersecurity strategy as early as the end of 2012. On 28 December 2012, the Standing Committee of the National People's Congress ("SCNPC") issued a decision to strengthen the protection of information on networks, with a focus on protection of personal information collected, processed and applied by "network service providers" and other entities "during the course of business". On 7 November 2016, the SCNPC issued the PRC Cybersecurity Law, which became effective on 1 June 2017. Around the same time as and corresponding to the	The Cybersecurity Security Agency of Singapore ("CSA") was established in 2015 to oversee Singapore's cybersecurity strategy, education and outreach, as well as industry development. The CSA is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information. CSA issued the Singapore's Cybersecurity Strategy Report in 2016, which sets out Singapore's vision, goals and priorities for cybersecurity. Singapore's cybersecurity strategy aims to create a resilient and trusted cyber environment, and is underpinned by four pillars:	In 2003, the Department of Homeland Security's National Strategy to Secure Cyberspace was released by the George W. Bush administration to highlight the role of public-private engagement and provided suggestions to improve collective cybersecurity for businesses, educational institutions and individuals. In 2008, the Bush administration launched Compre-hensive National Cybersecurity Initiative ("CNCI"). CNCI aimed to strengthen cybersecurity education, bolster the deployment of intrusion detection and prevention systems throughout

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
comprehensive set of information technology security policies, standards, guidelines, procedures and relevant practice guides for use by government departments. These procedures and guidelines were developed with reference to international standards, industry best practices, and professional resources. Financial regulators have taken the lead in developing cybersecurity initiatives for the financial services industry. See Dimension 2 for more details.	The vision set out in the 2020 strategy will be delivered through: (i) action by governments to strengthen the protection of Australians, businesses and critical infrastructure from the most sophisticated threats; (ii) action by businesses to secure their products and services and protect their customers from known cyber vulnerabilities; and (iii) action by the community to practice secure online behaviours. The lead agency for cybersecurity is the Australian Cybersecurity Centre ("ACSC") which was established in 2014. ACSC manages a national framework of Joint Cybersecurity Centres	Most recently, the EUset out its revised Cybersecurity Strategy in December 2020. The strategy, which was accompanied by proposals for a revised Network and Information Security Directive and a proposed directive on the resilience of critical entities, contained concrete proposals for regulatory, investment and policy initiatives in three areas: (i) resilience, technological sovereignty and leadership – actions to increase the level of cyber resilience of critical public and private sectors, and the launch of a network of Security Operations Centres across the EU; (ii) building operational capacity to	infrastructure and encourage Japanese business to pursue cybersecurity best practices.	issuance of the PRC Cybersecurity Law, the CAC (defined below) announced a National Cybersecurity Strategy in December 2016, with the key tasks identified as: defending cyberspace sovereignty; protecting critical information infrastructure ("CII"); and elevating cyberspace defense capabilities. The Central Leading Group for Cyberspace Affairs was created in 2014 by President Xi. It supports the principle that cybersecurity is integral to national security. In 2018, this group evolved into the Central Cyberspace Affairs Commission ("CCAC"), also known as the Cyberspace Administration of China ("CAC"). Following the issuance and mplementation of the PRC Cybersecurity	(i) strengthening the resilience of Singapore's critical information infrastructure ("CII"); (ii) mobilizing businesses and the community to create a safer cyberspace by countering cyber threats, combating cybercrime and protecting personal data; (iii) developing a vibrant cybersecurity ecosystem comprising a skilled workforce, technological-ly-advanced companies and strong research collaborations so as to support Singapore's cybersecurity needs and be a source of new economic growth; and (iv) stepping up efforts to forge strong interna-tional partner-ships to address	the federal government, and better coordinate cybersecurity research and development within the United States. President Obama, recognizing the importance of strengthening cybersecurity policy, evolved and updated the CNCI through 60-day Cyber Policy Review, in which the National Security Council ("NSC") and Homeland Security Council reviewed government activities and cybersecurity programs and ultimately produced a report that summarized its findings. As a result, the executive branch was directed to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships; invest in relevant cutting-edg-eresearch and development; and

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
	where the agency collaborates with industry, government and academic partners on current cybersecurity issues. One of the primary financial regulators, the Australian Prudential Regulatory Authority (APRA), announced a new Cyber Security Strategy for 2020-2024 designed to complement Australia's 2020 Cyber Security Strategy. For details, see Dimension 2 under *Financial Regulatory*.	prevent, deter and respond – establishment of a new Joint Cyber Unit, to strengthen cooperation between EU bodies and Member State authorities; and (iii) advancing a global and open cyberspace through increased cooperation. The European Union Agency for Network and Information Security ("ENISA") is the EU's center of cybersecurity expertise. It supports Member States in responding to large-scale cross-border cyber incidents, as well as supporting the development and implementation of EU cybersecurity law and policy, including European cybersecurity certification schemes.		Law, China has introduced new laws and regulations that set out stricter requirements, including various national standards to regulate companies (including Chinese affiliates of foreign companies) that set up their cloud infrastructure, including servers, virtualized networks, software, and information systems in China. A draft of the PRC Data Security Law was released for public comments in July 2020. The draft legislation is the first Chinese law aimed at regulating the collection, processing, control and storage of data involving national security, business secrets and personal data. In October 2020, a draft PRC Personal	international cybersecurity and cybercrime issues. In addition, the CSA issues an annual publication which reviews the cyber landscape in Singapore and the initiatives introduced in the year in furtherance of Singapore's four-pronged cybersecurity strategy. The latest Singapore Cyber Landscape 2019 was issued on 26 June 2020. In February 2020, the Singapore government announced that it would set aside S$1 billion over the next three years to build up the government's cyber and data security capabilities and to safeguard citizens' data and CII systems. In October 2020, the Singapore government	promote cybersecurity awareness and digital literacy. President Obama also established the role of a cybersecurity coordinator who would play a central role in developing cybersecurity policy, report to the National Security Advisor, and have regular access to the President. (the Trump administration removed this position in 2018). The Obama administration also released the Cybersecurity Strategy and Implementation Plan ("CSIP") in 2015 which aimed to strengthen government systems and data by identifying and addressing critical cybersecurity gaps and emerging priorities. CSIP was followed in February 2016 by Cybersecurity National Action Plan ("CNAP") which included the following

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
		In July 2020, ENISA announced its new strategy, outlining the Agency's path towards achieving a high common level of cybersecurity across the EU. The strategy is based on seven strategic objectives that will set the priorities for ENISA, including: (i) empowered and engaged communities across the cybersecurity ecosystem; (ii) cybersecurity as an integral part of EU polices; (iii) effective cooperation amongst operational actors within the Union in case of massive cyber incidents; (iv) cutting-edge competences and capabilities in cybersecurity across the Union; (v) a high level of trust in secure digital solutions; (vi) foresight on emerging and future for Europe.		Information Protection-Law ("Draft PIPL") was published for consultation. If passed, the Draft PIPL would be the first comprehensive national level personal information protection law in the PRC. Once the draft Data Security Law and the Draft PIPL are formally issued, they will form, along with the PRC Cybersecurity Law, a comprehensive legal framework for cybersecurity and data protection in China.	announced Singapore's Safer Cyberspace Masterplan 2020, building on the 2016 Cybersecurity Strategy and outlining a blueprint for the creation of a safer and more secure cyberspace in Singapore. It comprises three strategic thrusts: (i) securing core digital infrastructure, (ii) safeguarding cyberspace activities and (iii) empowering its own cyber-savvy population.	initiatives: a proposed $3.1 billion Information Technology Modernization Fund; establishment of a federal Chief Information Security Officer (CISO); continued identification and review of highest value and most at-risk IT assets; and an increase in government-wide shared services for IT and cybersecurity. President Obama also lead efforts related to a variother cybersecurity-related policies during his Presidency, such as military cyber operations and international strategy. In May 2017, the Trump Administration issued the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure ("Order"). The Order required agency heads to adhere to the National Institute

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
						of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cyber Security ("NIST Cybersecurity Framework") in order to manage each agency's cybersecurity risk. In September 2018, the White House issued the National Cyber Strategy outlining the government's plan to protect networks and systems, to nurture a secure and thriving digital economy, and to strengthen US ability to deter and punish malicious use of cyber tools. In November 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018 which created the Cybersecurity and Infrastructure Security Agency (CISA), a new stand-alone federal agency,

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
						created to protect the nation's criticalin-frastructure. That law rebranded the Department of Homeland Security's National Protection and Programs Directorate (NPPD) as CISA and transferred resources and responsibilities of NPPD to the newly created agency. CISA's mission is to build the national capacity to defend against cyber attacks and work with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies. In the spring of 2021, the Biden Administration announced six priorities for Cybersecurity & Infrastructure Security Agency in

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
						2021, including (1) tackling ransom-ware,(2) improving cybersecurity training at the Department of Homeland Security, (3) bolstering the resilience of industrial control systems1, (4) protecting transportation systems, (5) safeguarding election systems, and (6) advancing international capacity-building efforts. The Biden Administration is also reportedly considering an executive order requiring software vendors to notify federal government customers in the event of a cybersecurity breach following revelations of a breach of technology provider SolarWinds that affected several government agencies.

Dimension 2 – Legal & Financial Regulatory Frameworks

Legal

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
No "omnibus" cybersecurity ordinance or agency/regulator. Section 161 of the Crimes Ordinance, enacted in 1993, expanded the scope of existing criminal offences under various ordinances to cover comput-er-related criminal offences. The Personal Data (Privacy) Ordinance ("PDPO") sets out the data privacy and protection framework for Hong Kong. There is currently no mandatory requirement to notify the Privacy Commissioner for Personal Data ("PCPD") or the data subject of a data breach under the PDPO. However, in January 2020, the	No "omnibus" cybersecurity law. The Criminal Code Act 1995, as amended by the Cybercrime Act 2001, is the principal legislation criminalizing cyberattacks in Australia. The Tele-communi-cations Sector Security Reform (under the Tele-com-munications and Other Legislation Amendment Act 2017) applies to cyber threats targeted at critical infrastructure and specific sectors. The Privacy Act 1988 regulates how the private sector and government agencies handle personal information. Entities subject to the Privacy Act 1988 are	The Cybersecurity Act entered into force in 2019 to strengthen the mandate of ENISA and establish an EU-wide cybersecurity certification framework. The Directive on Security of Network and Information Systems ("NIS Directive") aims at tackling network and information security incidents and risks across the EU. In December 2020, in conjunction with the revised Cybersecurity Strategy, the Commission adopted a proposal for a revised Directive on Security of Network and Information Systems ("NIS2 Directive"). The proposal, which builds on and repeals the current NIS Directive, modernises the existing legal	The Basic Act on Cybersecurity was enacted in 2014 to set out the roles and responsibilities of national and local governments within the overall national cybersecurity policy. It also provides that cyber business and infrastructure-related businesses should take voluntary measures to enhance cybersecurity. In December 2018, Japan's Parliament passed a bill to amend the 2014 Basic Act on Cyber-security to fortify cybersecurity in preparation for Japan hosting the Tokyo Olympics & Paralympics. Several other laws (e.g., the Penal Code and the Act on the	The Cybersecurity Law came into effect in 2017. It is the first national-level law addressing cybersecurity in China (including data protection in such context). It provides various security protection obligations for network operators and imposes heightened security obligations for CII operators. The law also introduces a general requirement for the reporting and notification of actual or suspected material personal information breaches. The National Security Law adds cyberspace and information security as important elements of national security. Cybercrime is covered	The Cybersecurity Act 2018 (No. 9 of 2018) ("Cybersecurity Act") which came into effect on 31 August 2018, creates a legal framework for the oversight and maintenance of national cybersecurity in Singapore. The Cybersecurity Act establishes a regulatory framework for the, protection of CII against cybersecurity threats, authorizes the CSA to investigate and respond to cybersecurity threats and incidents and establishes a cybersecurity information sharing framework. Aside from the Cybersecurity Act, other key pieces of legislation include the Personal Data Protection Act 2012	There is no single overarching cybersecurity law in the US. The statutory framework is fragmented, with industry and information-specific requirements. Key federal statutes that address electronic security include the following: • The Electronic Communications Privacy Act of 1986, last amended in 2008, establishes legal requirements for acquisition or use of communications in transit and in electronic storage, as well as criminal and civil causes of action for violations of these requirements. • The Computer Fraud and Abuse Act, first enacted in 1986 and last amended in 2008,

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
PCPD indicated that a mandatory breach notification is likely to be included in upcoming amendments to the PDPO. The timing for those amendments has yet to be confirmed.	subject to its mandatory data breach notification regime and must handle and use personal information in compliance with the 13 Australian Privacy Principles contained in schedule 1 of the Privacy Act. The Security of Critical Infrastructure Act 2018 ("Critical Infrastructure Act") seeks to manage national security risks (e.g. sabotage, espionage and coercion) posed by foreign entities and was implemented as a response to increased cyber connectivity in relation to critical infrastructure. In November 2020, major amendments to the Critical Infrastructure Act were proposed by the government, in alignment with the newly revised Cybersecurity Strategy. The proposals would,	framework. Among other things, it introduces stricter security and notification obligations and harmonises sanctions regimes across the EU by requiring member state to impose administrative fines for breaches. Also in December 2020, the EU announced a proposed directive on the resilience of critical entities ("CER Directive"). The proposed directive will expand both the scope and depth of the existing EU rules on critical infrastructure to cover 10 sectors, including banking and financial market infrastructure. The CER directive will also introduce an enforcement mechanism designed to ensure that member state authorities have the powers to conduct on-site inspections of critical entities and	Prohibition of Unauthorized Computer Access) also cover different types of cybercrime and cybersecurity. The key data protection legislation is the Act on the Protection of Personal Information ("APPI"). On 5 June, 2020, the Japanese legislature passed several amendments to the APPI that will expand protections for personal data and impose new obligations on all businesses using personal data for business purposes. Importantly, there will be an obligation to notify the Personal Information Protection Commission of certain data breaches (though the threshold for reporting obligations has not yet been decided). The amendments will go into effect within two years of 5 June, 2020.	under the PRC Criminal Law. As mentioned above in Dimension 1, China is also in the midst of the legislative process to finalize the PIPL and the PRC Data Security Law.	(No.26 of 2012) ("PDPA"), and the Computer Misuse Act (Chapter 50A) ("CMA"). The PDPA, which is administrated by the Personal Data Protection Commission ("PDPC"), governs the collection, use, disclosure and care of personal data. In particular, the PDPA requires organisations to make reasonable security arrangements to protect personal data in its possession or under its control to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks. In January 2021, the PDPC announced that certain sections of the Personal Data Protection (Amendment) Act 2020 would take effect from 1 February 2021. These include three key changes:	establishes criminal and civil causes of action for a range of cybercrimes. • The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires that covered medical entities in the healthcare industry implement technical and non-technical safeguards to protect and secure individuals' "electronic protected health information" ("e-PHI"). • Section 5 of the Federal Trade Commission ("FTC") Act prohibits "unfair and deceptive acts or practices" by entities with respect to misrepresentations about a company's protection of consumers' personal information.

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
	among other things, (i) introduce new government powers to intervene in response to cyberattacks and obtain information from critical infrastructure entities if it is deemed to be in the national interest, (ii) add a number of additional sectors to the definition of "critical infrastructure," including financial services, and (iii) imposing positive security obligations on owners and operators of critical infrastructure assets.	to impose penalties for non-compliance. The EU will look to implement the new cyber-security strategy in the coming months. The NIS2 and CER Directive will require further review and adoption by EU institutions before being sent to the member states for implementation. The General Data Protection Regulation ("GDPR") is the consolidated EU law on data protection, setting out a comprehensive network of obligations and rights relating to the processing of personal data. Widely viewed as the gold standard of data protection legislation, the GDPR contains robust data breach notification requirements.			(i) a mandatory data breach notification for data breaches with a threshold based on level of harm or scale; (ii) introduction of offences concerning mishandling of personal data by individuals; and (iii) an expansion of the consent network. Further changes as a result of the amendments expected to take effect after February 2021 include increased financial penalties for organizations. The CMA is the principal legislation on cybercrime in Singapore – certain cyber activities, such as hacking, denial-of-service attacks, and infecting computer systems with malware, are criminalized. The CMA also covers unauthorized access, use or modification of	The FTC has published guidance on best practices for safeguarding information as well as insight into its enforcement actions in the cybersecurity context. • The Federal Information Security Modernization Act of 2014 ("FISMA 2014") requires federal government agencies and contractors to create and put in place cybersecurity programmes. In response to FISMA, the National Institute of Standards and Technology (NIST) of the United States Department of Commerce published the NIST Cybersecurity Framework. • The Cybersecurity Information Sharing Act of 2015

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
					computer, computer materials and computer services.	("CISA Act") enhances sharing of information about cybersecurity threats. CISA Act provides a process for companies to receive protections from liability and public records disclosure when sharing information with federal law enforcement about cybersecurity attacks. There is no omnibus privacy/data protection statute in the US. Instead, privacy issues are governed by a patchwork of different state and federal rules. There is no central authority to enforce these rules; the closest equivalent for federal privacy law enforcement is the FTC, however, prosecution for cybersecurity related incidents is uncommon. In relation to data breach notification,

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
						each state has their own data breach notification laws with varying definitions of “personal information.”

Financial Regulatory

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
The Securities and Futures Commission ("SFC") has issued to licensed corporations a range of guidelines and circulars related to cybersecurity risks. Topics include mitigation of hacking risks associated with internet trading of securities and futures and raising awareness of ransomware. The Hong Kong Monetary Authority ("HKMA") launched its Cybersecurity Fortification Initiative ("CFI") in respect of the banking sector in 2016, comprising (i) the Cyber Resilience Assessment Framework (a two-part self-assessment and cyber attack simulation testing); (ii) certification scheme and training program; and (iii) the Cyber Intelligence	The Australian Prudential Regulation Authority ("APRA") issued mandatory regulations in 2019 (Prudential Practice Guide CPG CPS 234 Information Security ("Prudential Standard")) which aim to ensure that APRA-regulated entities meet certain cybersecurity requirements in order to be resilient against emerging information security threats. The key requirements of this Prudential Standard are that an APRA-regulated entity must: • clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals; • maintain an	The NIS Directive aims to ensure that operators in sectors deemed essential (including providers of financial market infrastructure services) are taking appropriate measures to manage cybersecurity risks. As mentioned above, a new NIS2 directive was proposed in late 2020 which would impose stricter obligations on the covered sectors. In response to the European Commission's FinTech Action plan of March 2018 where cybersecurity issues where a recurring theme, the Joint Committee of the European Supervisory Authorities (comprising the European Banking Authority, European Securities and Markets Authority,	The PPC and the Financial Services Agency ("FSA") issued "Guidelines for Personal Information Protection in the Financial Field." These Guidelines require financial institutions and others to develop necessary and suitable cybersecurity management measures, with the focus on preventing data leakage, loss or damage. In October 2018, the FSA issued updated "Policy Approaches to Strengthen Cybersecurity in the Financial Sector" to address increasing digitalization, as well as challenges presented by the Tokyo Olympics. In June 2020, the	Under the Cybersecurity Law, financial institutions have additional cyber-security requirements to meet given that they are consi dered to be CII operators. At the financial regulatory level, financial institutions are generally required to protect client confidentiality, and implement enhanced protections over AML information and personal financial information. Cybersecurity is also an important regulatory focus, among others, in regulations issued by relevant financial regulators on IT system development, outsourcing and operations of various financial institutions.	Financial institutions in Singapore are subject to the regulatory oversight of the Monetary Authority of Singapore ("MAS"). One of the key regulatory focus areas of the MAS is to build a cyber-resilient financial sector. In this regard, the MAS has issued three key sets cybersecurity-focused notices and guidelines: the Technology Risk Management Guidelines; Notices on Technology Risk Management; and Notices on Cyber Hygiene. These notices and guidelines generally set out obligations of the financial institutions relating to (a) system reliability, availability and recoverability, (b) notification to the	The Gramm-Leach-Bliley Act ("GLBA") enacted in 1999, in conjunction with implementing regulations published by financial services regulators, requires financial institutions to employ technical, physical and administrative safeguards to protect non-public personal information of consumers from unauthorised access or use. The comprehensive security program developed by each company is unique and appropriate to the size of the company, and scope of the company's activities and information. GLBA regulations further require certain financial institutions to notify regulators

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
Sharing Platform. An enhanced version (CFI 2.0) was introduced in November 2020. The HKMA also introduced a competency framework that facilitates cybersecurity talent development for the banking sector. Further, it issued a circular to require CEOs of registered institutions (i.e. authorized institutions that are also registered with the SFC) to apply the relevant SFC guidelines mentioned above. As part of its supervisory functions, the HKMA also conducts on-site exams and off-site reviews of the information systems of authorised institutions. The Hong Kong Insurance Authority requires insurers to identify cybersecurity threats, and has issued guidelines	information security capability commensurate with the size and extent of threats to its information assets; • implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets; and • notify APRA of material information security incidents. As referenced in Dimension 1, APRA announced a new Cybersecurity Strategy for 2020-24 designed to complement Australia's 2020 Cyber Security Strategy. The new strategy comprises three primary focus areas: (i) establishing a baseline of cyber controls e.g., embed non-negotiable cyber practices,	and the European Insurance and Occupational Pensions Authority) in April 2019 published their advice to the European Commission on strengthening EU cyber and information security regulation in the financial sector. These initiatives include: • Developing an EU oversight framework for 3rd party providers active in financial services with a focus on cloud services providers; and • Developing an EU-wide framework for testing cyber resilience of important financial institutions. In September 2020, the European Commission adopted a digital finance package, including a digital finance strategy and legislative proposals on	FSA published the Financial Sector Cybersecurity Report which described the current status and common challenges identified in the course of conducting monitoring of progress with the 2018 Policy Approach document. Among other things, the report noted that cyber risks surrounding financial institutions have increased further due to the COVID-19 pandemic and the postponed Tokyo 2020 Olympics and Paralympics. In response, the FSA will encourage small and medium FIs to maintain and improve the effectiveness of their basic cybersecurity management systems through cooperation with their industry groups and upgrade their incident response capabilities through cyber exercises. With regard to larger	China's central bank, the People's Bank of China, released its new Personal Financial Information Protection Technical Specification on 13 February 2020, which took effect immediately. This industry standard sets forth additional privacy and cybersecurity requirements on the life cycle of personal financial information collected and processed by financial industry institutions.	MAS of IT security incidents and malfunction of critical systems, and (c) the security of customer information, and also provide for key risk management principles and best practice standards to guide financial institutions in establishing a sound and robust technology risk management framework. On 18 January 2021, the MAS issued revised Technology Risk Management guidelines to take into account the fast-changing cyber threat landscape and financial institutions' increased reliance on cloud technologies, application programming interfaces, and rapid software development. The new guidelines apply to all banks, payment services firms, brokerage and insurance firms.	and data subjects after breaches of non-public personal information. The US Securities and Exchange Commission ("SEC") also uses its civil law authority to bring cyber-related enforcement actions. SEC rule 30 applies to brokers, dealers and investment companies registered with the SEC cybersecurity measures. The SEC also set up the Division of Enforcement's Cyber Unit in 2017 to focus on, among other things, cybersecurity controls at regulated entities; and issuer disclosures of cybersecurity incidents and risks. The SEC issues guidance to help investors protect themselves from cyber threats. The Sarbanes-Oxley

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
setting out the minimum standard of cybersecurity expected of an insurer.	facilitate better sharing of cyber information and enable more effective incident response processes; (ii) enabling boards and executives of financial institutions to oversee and direct correction of cyber exposures; and (iii) rectifying weak links within the broader financial eco-system and supply chain by advocating cyber-assessment and assurance, and harmonising the regulation and supervision of cyber across the financial system. The Australian Securities and Investments Commission ("ASIC") assesses the IT management systems of financial	crypto-assets and digital resilience. The European Commission published its draft Digital Operational Resilience Act (DORA), to ensure that financial-sector information and communications technology systems can withstand security threats and that third-party ICT providers are monitored. As noted above, the proposed CER directive designates companies in the banking and financial markets infrastructure sector as "critical entities," meaning such companies will have to undertake common reporting measures, including entity-level risk assessments and incident notifications, as well as implementing other technical and organisational measures. They will also be subject to on-site inspections by	institutions, the FSA will encourage them to upgrade risk management regarding group-wide and global cybersecurity and further advance cybersecurity countermeasures.			Act requires any publicly traded company in the United States to issue an annual Internal Control Report certifying that the company maintains adequate internal controls for financial reporting, including, the security and integrity of the company's information systems. Notably, executives can face criminal penalties for noncompliance. The Commodity Futures Trading Commission (CFTC) Regulations require all CFTC registrants to adopt policies and procedures that implement administrative, technical and physical safeguards to protect customer information. The New York Department of Financial Services Cybersecurity Requirements requires regulated

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
	entities and provides guidance related to cyber risks.	national authorities.				entities to implement and maintain cybersecurity programs that meet specified requirements, conduct periodic testing and risk assessments, employ and train qualified cybersecurity personnel, monitor third-party vendor compliance with cybersecurity controls, and report certain cybersecurity incidents to New York State.

Dimension 3 – Cyber Culture

Hong Kong

The Hong Kong Enterprise Cybersecurity Readiness Index is issued by the Hong Kong Productivity Council and measures the status of local cyber security awareness and cyber-readiness in business. The most recent version was published in May 2020 and reported an Overall Readiness level of 46.9 (with 100 being the highest level of readiness), a slight decrease from the 2019 survey, potentially due to the need to prioritize business resources in the current challenging business environment. The survey further revealed that:

- except for NGOs and schools, the overall readiness index for all industries fell as

Australia

An annual Cyber Threat Report (July 2018 to June 2020) published by the Australian Cyber Security Centre ("ACSC") found that of the 2,266 cyber security incidents reported during the reporting period:

- the largest proportion were assessed as being 'Category 5 – Moderate Incident' (36.5%) followed by 'Category 4 – Substantial Incident' (33.3%); and
- the most common type of cyber security incident was 'malicious email' (27%), followed by 'compromised system' (24.4%) which describes incidents where an adversary has

EU

A survey of the attitudes of Europeans towards cybercrime survey was published by the European Commission in January 2020 and reported that:

- awareness of cybercrime is rising, with 52% of respondents stating they are fairly well or very well informed about cybercrime, up from 46% in 2017;
- respondents are growing less confident about their capacity to stay safe online: 59% think they can protect themselves sufficiently against cybercrime, down from 71% in 2017;
- more than a third of the respondents have received fraudulent emails or phone calls

Japan

A 2018 survey of Japanese public opinion by the Pew Research Center published in July 2019 highlighted that:

- 81% of the respondents say attacks on computer systems launched from other countries are a major threat to Japan, representing a 10% points increase since 2016;
- Cyberattacks are ranked as the top international worry among Japanese citizens every year since 2016; and
- 84% of the Internet users in Japan voiced concern about cyberattacks.

Mainland China

The 44th statistical report on China's Internet development by the China Internet Network Information Center (published in September 2019) reported that:

- up to 30 June 2019, 99.1% of the 854 million population in China who were Internet users accessed to the Internet via mobile network; and
- in the first half of 2019, a significant number of internet users consumed online services, e.g. online food ordering and delivery: 421m users; online shopping: 639m users; online payment: more than 633m users; online streaming services: more than 759m users;

Singapore

A 2019 Cybersecurity Public Awareness survey by the Singapore Cyber Security Agency (published in August 2020) found that:

- the level of concern for cyber incidents is high;
- most respondents agreed that everyone has a role to play in ensuring cybersecurity;
- there continued to be room for improvement in respondents' cyber hygiene, e.g. the majority did not install security applications in their devices despite knowing the risks;
- respondents faced difficulty in identifying phishing emails, i.e. only 4 % of respondents

US

A survey by the Pew Research Center published in October 2019 reported that Americans:

- vary substantially on their understanding of technology-related issues by educational level as well as by age, and
- vary on their understanding of technology-related issues depending on the topic. For instance, over 60% of Americans survey correctly answered questions related to phishing scams and cookies, while only 30% of them correctly answered a question related to URL or website encryption.

An earlier Pew survey published in January 2017 reported the following:

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
compared with 2019; • financial services sector continued to be the most vigilant, with readiness at the "managed" level; • the readiness level of all other industries, such as NGOs, information and communication technology, manufacturing and professional services, is "basic"; • larger enterprises have generally adopted more comprehensive cybersecurity measures; and • more enterprises encountered external cyberattacks in 2020 than in 2019 with phishing emails being the top type of attacks.	accessed or modified a network, account, database or website without authorisation.	asking for personal details in the last three years; and • 10% of the respondents say cybersecurity concerns make them less likely to make purchases online.		and nearly 40% of the total Internet users used ride-hailing services. In a September 2020 survey by the PRC cybersecurity authorities, around 88.5 percent of respondents said they will be cautious in giving permission to mobile apps to access mobile phone sensors and data. Other findings included the fact that half of the respondents said they would carefully read the privacy policy popping up when opening an app for the first time or before updating it. The survey also showed 77.8 percent of respondents agreed that regulators should increase punishment for violations and 72.2 percent proposed legislation on personal data protection.	could identify all the phishing emails correctly; and • many respondents continued to think that cyber incidents would not happen to them.	• Americans generally fail to follow cybersecurity best practices in their own digital lives, e.g. password management; • 64% of Americans surveyed have personally experienced a major data breach; • A relatively large percentage of the public lack trust in key institutions (e.g. federal government, social media sites) to protect their personal information; and • Americans are not always vigilant in the context of mobile security, e.g. 28% of the respondents who are smartphone owners report that they do not use a screen lock or other security features, while around one in ten people reported that they never

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
						install updates to their smartphone's apps or operating system.

Dimension 4 – Cybersecurity Education, Training and Skills

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
A number of government-supported platforms have been set up to provide information and guidelines in relation to cybersecurity, including: • the Cybersecurity Information Portal; • Cybersec Infohub; • Hong Kong Emergency Response Team Coordination Centre (HKCert); • Government Computer Emergency Response Team Hong Kong (GovCert.HK); and • Cybersecurity and Technology Crime Bureau under the Hong Kong Police Force. The government has also launched various initiatives to promote information sharing and collaboration among local	As part of the Australian cyber-security strategy, various government initiatives have been established: • The Australian Cybersecurity Growth Network and Cyber.gov.au portal undertakes initiatives to grow the domestic cybersecurity industry and to raise awareness of cybersecurity risks respectively; • Academic Centres of Cybersecurity Excellence are set up to encourage more students to undertake studies in cybersecurity and related courses; and • Voluntary Cybersecurity Guidelines are being developed to promote good cybersecurity practice across	ENISA supports many initiatives for raising awareness of and educating about cybersecurity issues, including: • Guidance for improving cybersecurity culture; • "European Cyber-security Month" campaign which is organized once a year; • Recurring initiatives meant directly for students, such as the yearly 'European Cyber Security Challenge'; • To promote cybersecurity education and address the cybersecurity skill shortage, maintenance of a crowd-sourcing database of cybersecurity related education programmes; • Development of proper mechanisms	Cybersecurity education and training programs have been created in Japan by a wide range of organizations, including government body and research/ educational institutions. For example: • a cyber-defense program (CYDER) initiated by the Ministry of Internal Affairs and Communications in 2013 focuses on competence in dealing with cyberattacks on government offices, administrative agencies, as well as large companies; and • a program to equip university students with the basic skills needed for IT security engineers (SecCap) offered by a consortium of	The government plans to establish a number of "world-renowned" cybersecurity schools by 2027 to build a strong group of professionals to combat cyberattacks. As of 2019, 11 universities have been selected to participate in this initiative. The 2020 China Cybersecurity Week sponsored by the Office of the Central Cyberspace Affairs Commission offered a wide range of activities. The campaign's main event included a forum on cybersecurity, to promote good practices and increasing awareness of the implementation and application of national cybersecurity standards. Collaboration among	The CSA oversees cybersecurity strategy, education and outreach and industry development, and works with government agencies as well as partners from the private sectors in these aspects. The Cybersecurity Awareness Alliance, a public-private partnership which is co-chaired by the CSA, aims to build a positive cybersecurity culture and to increase cybersecurity awareness. The CSA has also introduced various programmes and initiatives to promote cybersecurity education, such as: • the Cybersecurity Associates and Technologists Program and the	NIST, a unit of the US Commerce Department, is the leading educational and outreach organization within the United States. Through events, presentation and the promulgation of written resources such as cybersecurity and incident response frameworks, NIST aims to enable the development of cybersecurity solutions and technologies that strengthen the United States' security capabilities. As part of the CNCI initiatives, the National Initiative for Cybersecurity Education ("NICE") was established in 2010 as a partnership between government, academia, and the private sector to address cybersecurity needs related to public awareness,

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
information security stakeholders in different sectors. One such initiative is "Cybersec Infohub," the objective of which is to facilitate cross-sector collaboration for better visibility of cyber threats globally and locally. The programme has been operating for more than a year and more than 360 public and private organisations from various sectors have joined the programme as of January 2021. The programme provides organisations with reference in gathering cyber security information and meeting with information security stakeholders to share the latest security trends and best practices. On the industry level, the banking sector has an enhanced competency framework on cybersecurity.	different organisations. In addition, to increase the number of skilled cyber security professionals, Box Hill Institute with industry support have developed two national cyber security qualifications: a Certificate IV in Cyber Security and an Advanced Diploma of Cyber Security. These are the first nationally-recognised cyber security vocational education qualifications in Australia. The Cybersecurity Strategy 2020 will involve the government investing AUD1.67 billion over ten years to introduce various initiatives, including: • Greater collaboration to build Australia's cyber skills pipeline; • Stronger partnerships with industry through the Joint Cyber Security	and consistency for cyber incident and crisis management; and • Development of a European Cybersecurity Skills Framework to create a common understanding of the roles, competencies, skills and knowledge in order to address the cybersecurity skills shortage. The European Cybersecurity Organisation ("ECSO") was created in 2016 in order to act as the Commission's counterpart in a contractual public-private partnership covering Horizon 2020 in the years development at European level. 2016 to 2020. ECSO carries out various activities aiming at community building and industrial development at European level.	Japanese universities. The Japanese Defense Ministry announced in early 2021 that they would hold its first competitive cybersecurity talent search in which participants compete to show their understanding of cybersecurity and ability to apply that knowledge. The contest is part of the government's search for talent to strengthen the country's cyber defenses. The Cybersecurity Strategy Headquarters promotes measures to develop security standards, raise awareness, strengthen failure response frameworks, and manage and address risks. The Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency,	the industry, academia and the Chinese government has also helped in the cultivation of cybersecurity talent.	Cybersecurity Career Mentoring Programme have been launched to train and up-skill ICT professionals and to attract students and young professionals to pursue a cybersecurity-related career respectively; • ICE71, a cybersecurity startup hub that aims to strengthen Singapore's growing cybersecurity ecosystem by developing and accelerating cybersecurity start-ups from early to late stages, through partnerships with Institutes of Higher Learning, large local enterprises and global cybersecurity accelerators; • the SG Cyber Women initiative, which is targeted to encourage more females, from as young as	education, professional development, and talent management. NIST was tasked as the lead for NICE to support its functions by promoting the initiatives. The National Initiative for Cybersecurity Careers and Studies, launched in 2013, is an online national resource portal for cybersecurity education, training, and career opportunities. CyberCareers.gov provides updated cybersecurity information and resources to support federal employees, students and academics. In 2015, the United States Department of Justice computer Crimes and Intellectual Property Cybersecurity Unit issued a "Best Practices for Victim Response and Reporting of Cyber Incidents" report,

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
On the tertiary and continuing education level, universities in Hong Kong were some of the first in Asia to incorporate industry-ready cybersecurity elements into the curriculum. On attracting non-local talent, the Government's Technology Talent Admission Scheme provides fast-track arrangement to admit cybersecurity professionals. Its Talent List also facilitates cybersecurity specialists to apply for immigration.	Centre program; • Advice for small and medium enterprises to increase their cyber resilience; and • Improved community awareness of cyber security threats.		Japan (IPA) have together issued "Cybersecurity Management Guidelines" to urge companies to recognise cybersecurity risks and develop company-wide measures.		pre-tertiary age, to join the cybersecurity profession; and • the CSA Cybersecurity Co-Innovation and Development Fund, which provides funding support to companies working on cybersecurity challenges. The inaugural Singapore Cybersecurity Education Symposium ("SCES"), organised by the CSA, held on 19 to 20 November 2020, was the first-of-its-kind in the region. The event is one of the key initiatives under the SG Cyber Educators programme, which objective is to grow a passionate pool of secondary and tertiary school teachers, and Education & Career Guidance counsellors to be familiar with cybersecurity to interest and guide	which was later updated in 2018. This report provides guidance to organizations as to how to prepare for and respond to cyber incidents lawfully and through adequate incident response planning. In 2016, as part of the CNAP, President Obama invested $62 million to advance the following: offer scholarships for Americans who wish to obtain cybersecurity education; develop a Cybersecurity Core Curriculum for cybersecurity education; and strengthen the National Centers for Academic Excellence in Cybersecurity Program to increase the number of participating academic institutions and students. In May 2017, the Trump administration

Hong Kong	Australia	EU	Japan	Mainland China	Singapore	US
					their students to make cybersecurity a choice for their education and career. CSA has announced that it will continue to expand into new areas through the introduction of two new programmes to nurture top young talent and leaders. The two new programmes are SG Cyber Olympians and SG Cyber Leaders. More details on both programmes will be released soon.	tasked various cabinet secretaries to jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce, including cybersecurity-related education curricula, training, and apprenticeship programs. In May 2019, President Trump issued an Executive Order on America's Cybersecurity Workforce, which established a federal cybersecurity rotational assignment program among cybersecurity practitioners in the Department of Homeland Security and other agencies. The Executive Order also promoted the use of the NICE Framework for cybersecurity workforce knowledge and skill requirements.

Note: This table is non-exhaustive and intended only to give an indication of some of the key features of the cybersecurity frameworks of the listed jurisdictions as of March 2021.

Acknowledgement

The FSDC would like to thank the following experts and professionals for their valuable input:

Mr Jim Lai
Mr Philip Chiu
Ms Eva Kwok
Mr Steve Wong
Ms Karen Chan
Mr Victor Ho
Mr Henry Shek

About the FSDC

The FSDC was established in 2013 by the Hong Kong Special Administrative Region Government as a high-level, cross-sectoral advisory body to engage the industry in formulating proposals to promote the further development of the financial services industry of Hong Kong and to map out the strategic direction for the development.

The FSDC has been incorporated as a company limited by guarantee with effect from September 2018 to allow it to better discharge its functions through research, market promotion and human capital development with more flexibility.

Contact us

Email: enquiry@fsdc.org.hk
Tel: (852) 2493 1313
Website: www.fsdc.org.hk