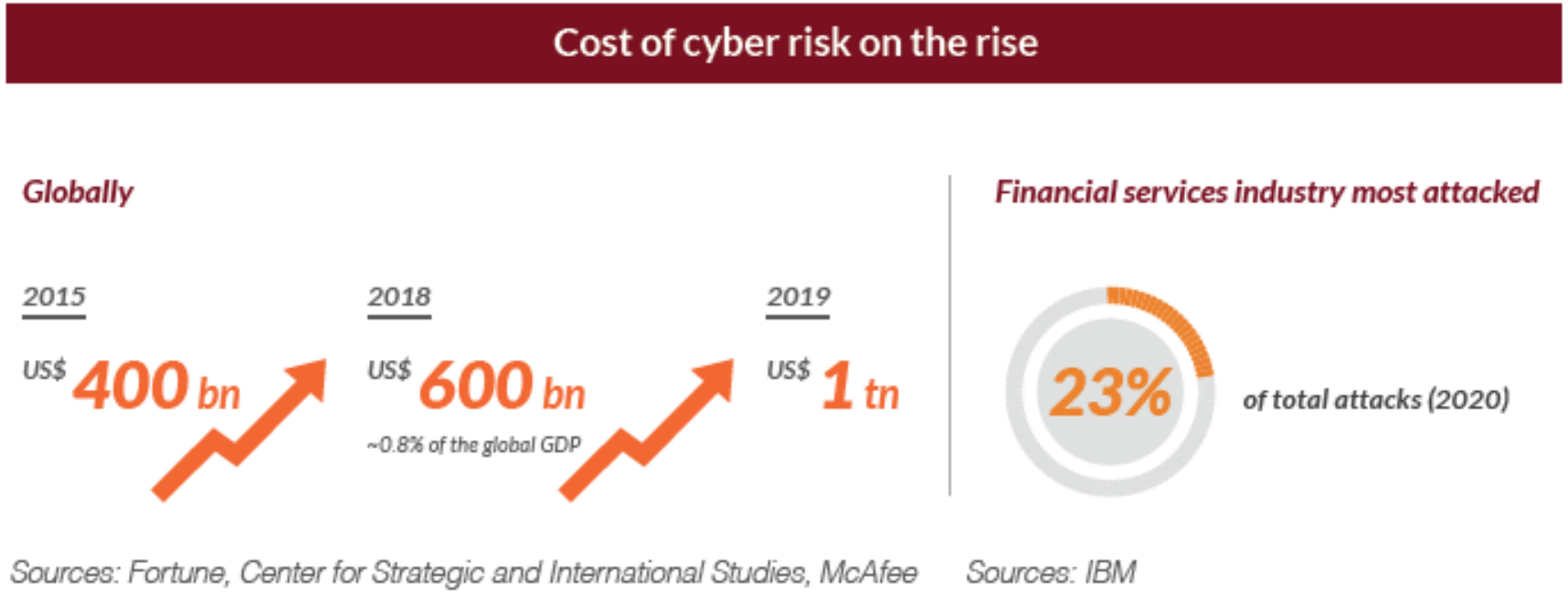
FSDC Industry Exchange Series Webinar on the Launch of Report

"Cybersecurity Strategy for Hong Kong's Financial Services Industry"

10 June 2021

Cybersecurity – a Significant and Growing Issue Globally

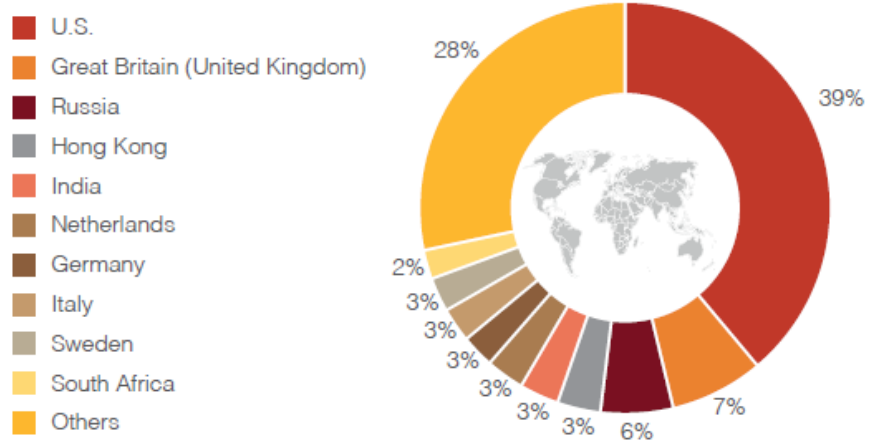
- The mounting cost as a result of cyberattacks is pressing the world to pay more attention to cybersecurity. With the onset of the COVID-19 pandemic, the demands on the cyberspace safety have become even more urgent.
- Financial services industry by its nature is particularly vulnerable to cyber risk. The industry has been a prime target of cyber attacks over the years and tremendous economic, regulatory and reputational harm have been caused.



Is Hong Kong an Obvious Target?

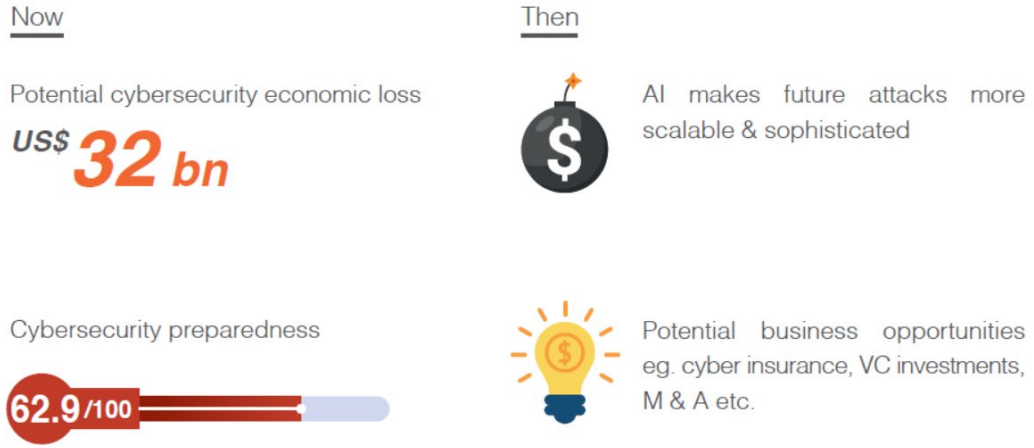
- As an international financial centre, Hong Kong is an attractive target for cyberattacks and the level of economic losses resulting from cybercrimes is on an upward trend. While the level of cybersecurity preparedness within Hong Kong is uneven, the financial services sector demonstrated the highest level of readiness among various sectors.
- With the use of artificial intelligence, cyberattacks will likely become more ubiquitous and the future cyber universe will become more complex. The value proposition of a robust cybersecurity framework is not limited to the precautionary dimension and can also serve as a foundation of developing business opportunities for the financial services industry.

Cyber-attacks on financial institutions (% of total)



Sources: ORX News IMF staff calculations

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



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

Policy Recommendations

Recommendations

RECOMMENDATIONS

POLICY LEVEL

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

LEGAL AND REGULATORY LEVEL

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

OPERATIONAL LEVEL

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

Recommendation 1 (Policy Level)
Develop a dedicated cyberspace safety roadmap with policy priorities for HK

- Incorporating the element of cyberspace safety into the holistic Smart City Blueprint is a good start for Hong Kong. Yet, 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.
- 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.
- While it is understandable that cyberspace safety is a cross-sectoral subject matter that can be relevant to more than one government bureau or agency, workable options for this proposed overarching governance body include:

  (i) establishing an independent commission (similar to the Australian Signals Directorate, or the Cyber Security Agency of Singapore); or

  (ii) setting up a cross-bureau/agency working group to coordinate both regulatory and enforcement actions.

Recommendation 2 (Legal & Regulatory Level)
Develop cyberspace protection legislation

- Many of the leading jurisdictions in cybersecurity have an omnibus cybersecurity / cyberspace protection law as a core element of their cybersecurity framework.
- 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.
- 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.

Recommendation 3 (Legal & Regulatory Level)
Harmonise regulations across the financial sector

- 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 respect of cybersecurity, Hong Kong has various sets of regulatory guidance in place. The HKMA, SFC and IA each have their respective guidelines/circulars to assist their licensed/ authorised institutions to handle cybersecurity issues. Some degree of coordination is seen, 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.
- An effective means of achieving such coordination can be in the form of a cross-agency steering group.

Recommendation 4 (Operational Level)
Enhance talent development

- 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.
- 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.
- Financial institutions (especially corporations with small business operations) may be reluctant to deploy significant resources to improve their cyber resilience. One approach to help overcome this challenge would be for the Hong Kong Government to provide incentives, such as training subsidies to eligible staff or institutions if they enrol in a cybersecurity certification schemes recognised/approved by the regulators.
- 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 optional would require a more in-depth feasibility study by the Government.

Recommendation 5 (Operational Level)
Operationalise preparedness at industry level

- 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. 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.
- 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. In planning an industry-wide stress test, Hong Kong's financial sector regulators could either organise the exercise themselves, or encourage financial institutions to plan and conduct their own industry-wide exercise.
- 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.

Conclusion

- Cyberattacks cause tremendous economic, regulatory and reputational harm to governments and businesses globally and 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.
- 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.
- This paper suggests a number of recommendations that Hong Kong can consider as key steps towards enhancing its cybersecurity framework. Such recommendations could be proceeded in parallel in light of the urgency to present, address and handle cyber risk.
- 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.

Panel Discussion

Jurisdictional Comparison - Cybersecurity Policy & Strategy

Hong Kong

- 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 cybersecurity organisations for enhancing information exchange.
- OGCIO and other government-supported organisations have been established to defend against and respond to cyber threats and incidents.
- Financial regulators have taken the lead in developing cybersecurity initiatives for the financial services industry.

EU

- The EU Cybersecurity Strategy was first announced in 2013 and the latest update was made in December 2020.
- The ENISA announced its new cybersecurity strategy in July 2020.

US

- The Department of Homeland Security's National Strategy to Secure Cyberspace was released in 2003.
- The Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure was issued in 2017.
- The Cybersecurity and Infrastructure Security Agency Act of 2018 was signed into law in 2018.

Mainland China

- The PRC Cybersecurity Law came into effect in 2017.
- A draft of the PRC Data Security Law was released for public comments in July 2020.
- A draft PRC Personal Information Protection Law was published for consultationIn October 2020.

Singapore

- The "Safer Cyberspace Masterplan" was announced in 2020.

Jurisdictional Comparison - Legal & Financial Regulatory Frameworks

Hong Kong

- 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 computer-related criminal offences.
- The Personal Data (Privacy) Ordinance sets out the data privacy and protection framework for Hong Kong.
- The SFC has issued to licensed corporations a range of guidelines and circulars related to cybersecurity risks.
- The HKMA launched its Cybersecurity Fortification Initiative in 2016.
- The IA requires insurers to identify cybersecurity threats, and has issued guideline setting out the minimum standard of cybersecurity expected of an insurer.

EU

- The Cybersecurity Act entered into force in 2019 to strengthen the mandate of ENISA and establish an EU-wide cybersecurity certification framework.
- The General Data Protection Regulation is the consolidated EU law on data protection.

US

- There is no single overarching cybersecurity law in the US. The statutory framework is fragmented, with industry and information-specific requirements.
- 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.
- The Gramm-Leach-Bliley Act was enacted in 1999.
- The SEC uses its civil law authority to bring cyber-related enforcement actions.

Mainland China

- Cybercrime is covered under the PRC Criminal Law.
- PBOC released its new Personal Financial Information Protection Technical Specification in February 2020.

Singapore

- The Technology Risk Management guidelines was revised in 2021 to take into account the fast-changing cyber threat landscape.

Jurisdictional Comparison - 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).

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.

US

- A survey by the Pew Research Center published in October 2019 reported that Americans have varied understanding of technology-related issues depending on the topic.
- An earlier Pew survey published in January 2017 reported that Americans generally fail to follow cybersecurity best practices in their own digital lives, e.g. password management.

Mainland China

- In a September 2020 survey by the PRC cybersecurity authorities, around 88.5% of respondents said they will be cautious in giving permission to mobile apps to access mobile phone sensors and data.

Singapore

- The 2019 Cybersecurity Public Awareness survey by the Singapore Cyber Security Agency found that the level of public concern for cyber incidents is high.

Jurisdictional Comparison - Cybersecurity Education, Training and Skills

Hong Kong

- A number of government-supported platforms have been set up to provide information and guidelines in relation to cybersecurity.
- The government has also launched various initiatives to promote information sharing and collaboration among local information security stakeholders in different sectors.
- 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.

EU

- ENISA supports many initiatives for raising awareness of and educating about cybersecurity issues, including: issuing the Guidance for improving cybersecurity culture, organizing the annual "European Cybersecurity Month" campaign, etc.

US

- The National Initiative for Cybersecurity Education was established as a partnership between government, academia, and the private sector to address cybersecurity needs related to public awareness, education, professional development, and talent management.
- The National Initiative for Cybersecurity Careers and Studies is an online national resource portal for cybersecurity education, training, and career opportunities.

Mainland China

- 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 was organised in September 2020.

Singapore

- The Cybersecurity Awareness Alliance is a public-private partnership aiming to build a positive cybersecurity culture and to increase cybersecurity awareness.

Q&A