Information Technology and Broadcasting

Research Office
Legislative Council Secretariat

Statistical Highlights

ISSH18/2022

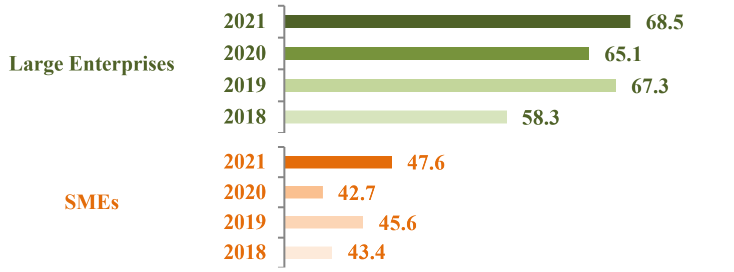
Cyber security challenges of SMEs in Hong Kong

Figure 1 – Usage of the Internet and adoption of e-commerce by enterprise size[a]

	2017		2019		2021	
	Large (%)	SMEs (%)	Large (%)	SMEs (%)	Large (%)	SMEs (%)
Using the Internet	99.8	87.4	99.5	90.1	100.0	95.6
Having a web presence	88.2	32.5	88.1	37.3	91.6	42.9
Receiving orders online	19.1	7.3	24.1	8.7	26.1	11.0
Placing orders online	34.1	21.0	35.2	20.9	37.3	24.7

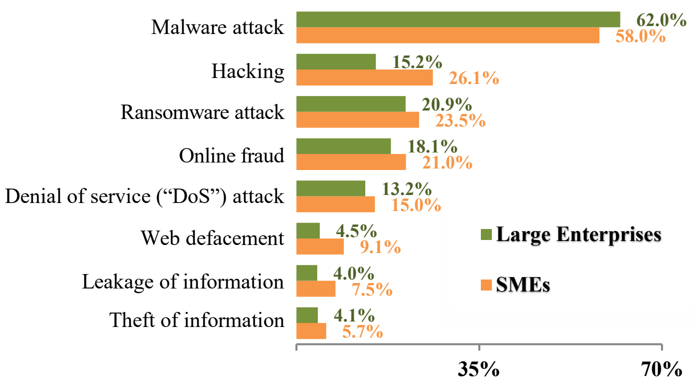
Note: (a) Enterprises are categorized into large enterprises and SMEs based on their number of persons engaged. Large enterprises are (i) manufacturing units with more than 100 workers; or (ii) non-manufacturing units with more than 50 workers. Other enterprises are defined as SMEs.

Figure 2 – Cyber Security Readiness Index, 2018-2021[a]



Note: (a) Graded on a scale from 0 to 100, the index evaluates the comprehensiveness of cyber security measures on four areas, namely (i) policy and risk assessment; (ii) technology control; (iii) process control; and (iv) human awareness building.

Figure 3 – Proportion of enterprises having encountered cyber security incidents [a], [b]



Notes: (a) During the survey period, 1 024 large enterprises and 26 929 SMEs encountered cyber security incidents. An enterprise may encounter more than one type of incident.

(b) Percentages in the figure refer to the proportion of enterprises having encountered a specific type of cyber security incident among all enterprises of corresponding sizes having encountered cyber security incidents.

Highlights

- As the vast majority of businesses in Hong Kong are small and medium-sized enterprises ("SMEs"), their vitality and business performance are crucial to the Hong Kong's economy. In recent years, there is a rising share of SMEs using digital channels and having web presences (**Figure 1**), closing the digital gap with large enterprises. The outbreak of the COVID-19 pandemic in early 2020 fuelled the trend, with more SMEs developing e-commerce channels for taking orders and/or making purchases.

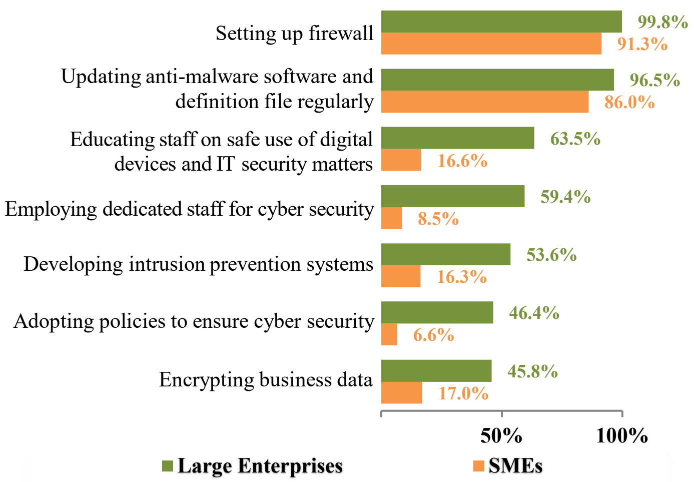
- However, SMEs have lagged their larger peers in terms of cyber security readiness. According to the annual surveys conducted by Hong Kong Productivity Council ("HKPC"), the Cyber Security Readiness ("CSR") score of SMEs has remained below 50 since the first survey conducted in 2018 (**Figure 2**), and the shortfall vis-a-vis large enterprises had widened from the level in 2018 as large enterprises appear to have strengthened their cyber defence capabilities.

- According to another survey conducted by Census and Statistics Department between 2020 and 2021 on information technology ("IT") usage of business sector, about one in every 12 SMEs encountered cyber security incidents during the survey period. Analyzed by type of incidents, "malware attack" was the most common incident among SMEs, followed by "hacking", "ransomware attack" and "online fraud" (**Figure 3**). Moreover, the prevalence of hacking, web defacement attacks and leakage of information was noticeably higher among SMEs versus large enterprises.

- Technology crimes are also a growing concern for businesses. According to the Hong Kong Police Force, total technology crime cases posted an annual growth of about 25%, reaching some 16 200 cases in 2021. A recent modus operandi of technology crime involves the infiltration of SMEs' email systems by fraudsters through impersonating business partners (e.g. suppliers) and/or senior managers of the victim companies and send emails to their staff requesting money transfer for business needs to accounts controlled by fraudsters. In 2021, the monetary loss related to such email fraud cases exceeded HK$1.5 billion, accounting for half of total loss arising from technology crimes. Over 70% of the victims of email fraud cases were SMEs.

Cyber security challenges of SMEs in Hong Kong (cont'd)

Figure 4 – Selected cyber security measures adopted by enterprise in 2021[(a), (b)]



Notes: (a) An enterprise may adopt more than one measure.
(b) Percentages in the figure refer to the proportion of enterprises having put in place a specific cyber security measure among all enterprises of corresponding sizes that have adopted cyber security measures.

Figure 5 – Major difficulties faced by enterprises in addressing cyber security risk in 2021

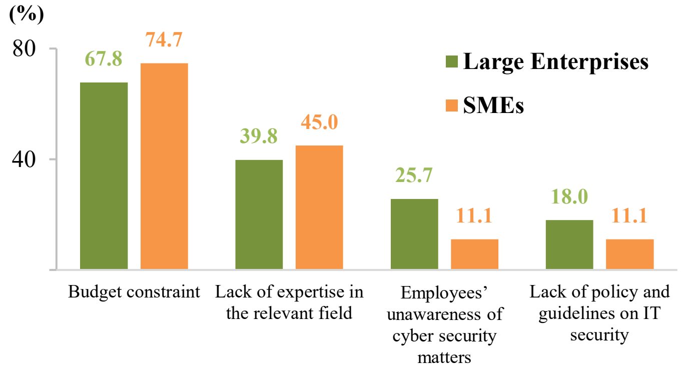
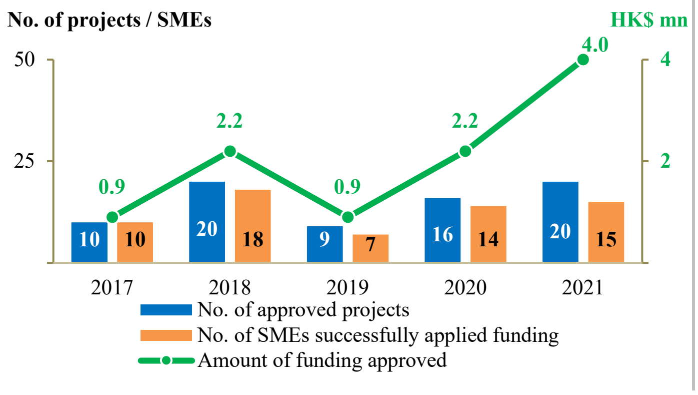


Figure 6 – Cyber security solutions subsidized by TVP, 2017-2021



Highlights

- Enterprises' investment in specific areas of cyber security may also reflect their attitudes toward safety in the digital realm. While SMEs could basically match up with large enterprises in setting up firewall or updating anti-malware software and definition file regularly, they have lagged visibly behind in staff-related areas such as employing cyber security specialists, providing IT security trainings or guidelines for staff, and adopting cyber security policies (**Figure 4**).

- Even though HKPC recommends business establishments to put more effort into addressing the weaker areas such as "Cyber Security Awareness Training" and "Cyber Threat Detection", a smaller proportion of SMEs expressed concern over the need to raise employees' awareness and develop IT security guidelines when compared with large enterprises (**Figure 5**). This may be one of the reasons why they tend to spend less on security measures related to human resources. Meanwhile, regardless of company size, "budget constraint" and "lack of expertise" are cited as the two biggest obstacles to address cyber security concerns.

- Hong Kong enterprises can leverage on various resources from the Government and other organizations to strengthen cyber security. For example, they can apply funding support from the Technology Voucher Programme ("TVP"), which was launched in 2016 to support non-listed local enterprises to develop their IT systems including raising cyber defence capabilities. According to the Office of the Government Chief Information Officer ("OGCIO"), TVP approved a total of 75 cyber security related projects during 2017-2021, of which 64 successful applicants were SMEs (**Figure 6**).

- Apart from funding support, OGCIO, in collaboration with other non-government organizations, has been supporting SMEs to raise cyber security awareness through measures ranging from setting incident reporting hotline and organizing IT safety seminars, to offering free scanning services for SMEs' websites and providing online self-assessment tools on cyber security readiness. For example, OGCIO works with the Hong Kong Internet Registration Corporation Limited to develop sector-specific training materials for SMEs to build up employees' cyber security awareness by the end of 2022.

Data sources: Latest figures from Innovation and Technology Bureau, Census and Statistics Department, Hong Kong Police Force, Office of the Government Chief Information Officer, Hong Kong Productivity Council and Hong Kong Computer Emergency Response Team Coordination Centre.

Research Office
Research and Information Division
Legislative Council Secretariat
30 June 2022
Tel: 3919 3181

Statistical Highlights are compiled for Members and Committees of the Legislative Council. They are not legal or other professional advice and shall not be relied on as such. Statistical Highlights are subject to copyright owned by The Legislative Council Commission (The Commission). The Commission permits accurate reproduction of Statistical Highlights for non-commercial use in a manner not adversely affecting the Legislative Council. Please refer to the Disclaimer and Copyright Notice on the Legislative Council website at www.legco.gov.hk for details. The paper number of this issue of Statistical Highlights is ISSH18/2022.