Information Technology and Broadcasting

Research Office
Legislative Council Secretariat

Statistical Highlights

ISSH23/20-21

Cyber security of enterprises in Hong Kong

Figure 1 – Major concerns under WFH arrangement, 2020

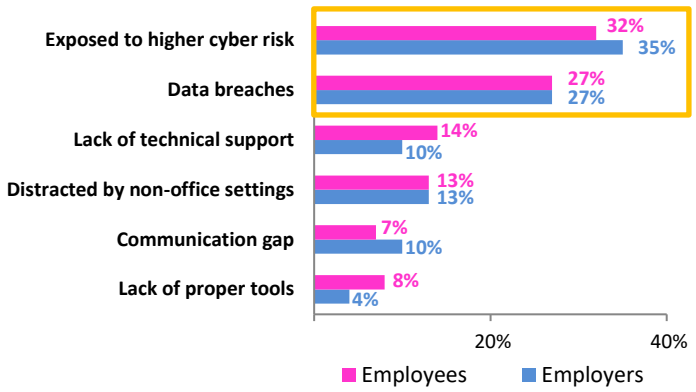


Figure 2 – Corporate email scams, 2011-2020

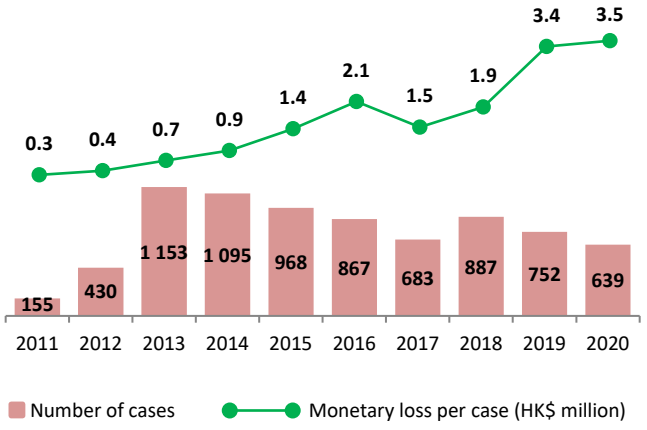
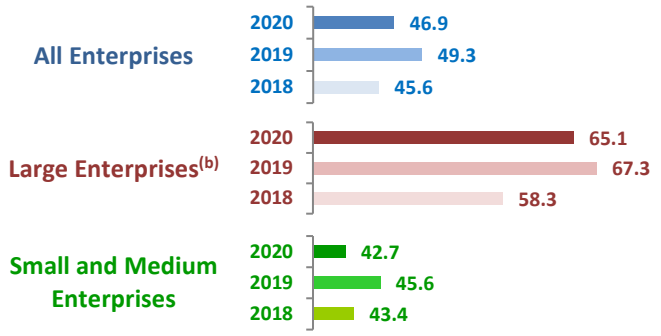


Figure 3 – Cyber Security Readiness Index, 2018-2020[(a)]



Notes: (a) Graded on a scale from 0 to 100, the index evaluates the comprehensiveness of cyber security measures on four areas, namely (a) security policy and assessment; (b) threats detection and technical solutions; (c) data security and risk management; and (d) security awareness education.

(b) Manufacturing establishments with more than 100 employees and non-manufacturing establishments with more than 50 employees are categorized as Large Enterprises.

Highlights

- In the wake of the Coronavirus Disease 2019, many businesses and employers have begun to increasingly rely on their employees working from home ("WFH") via various digital platforms. According to a survey published by Hong Kong Internet Registration Corporation in October 2020, 64% of companies adopted remote working and about 80% of individual respondents began to WFH in the first half of 2020 in Hong Kong. The survey also found that cyber risk and data breaches were the top two concerns for both employers and employees under WFH arrangement (**Figure 1**).

- Computer-related crimes, such as corporate email scam ("CES"), are also a growing concern for corporates in Hong Kong. CES refers to the sending of fictitious emails to the staff of victim companies, enticing them to transfer money to bank accounts designated by fraudsters. According to the Hong Kong Police Force, there were 639 cases of CES in 2020, involving a total loss of HK$2.2 billion (or HK$3.5 million per case) (**Figure 2**). Recent modus operandi of CES involves the infiltration of email systems by fraudsters, who pretend to be senior management of the victim companies and send emails to their staff to order money transfer for business needs. Staff members who are not aware of the scams may proceed with the transfer without verifying the identity of the sender, causing companies' monetary losses.

- Notwithstanding the cyber threats, local enterprises have not improved much in cyber security in recent years, according to surveys conducted by Hong Kong Productivity Council ("HKPC"). The surveys measure the cyber security readiness ("CSR") of business sector, which has been below 50 since the first survey conducted in 2018. The index even declined from 49.3 in 2019 to 46.9 in 2020 (**Figure 3**). According to HKPC, the decline was due to factors such as economic downturns amid the pandemic and the development of China-US relations, making companies to concentrate on business survival instead of cyber security. Analysed by company size, large enterprises had higher CSR scores than small and medium-sized enterprises ("SMEs").

Figure 4 – Level of support for staff under WFH arrangement

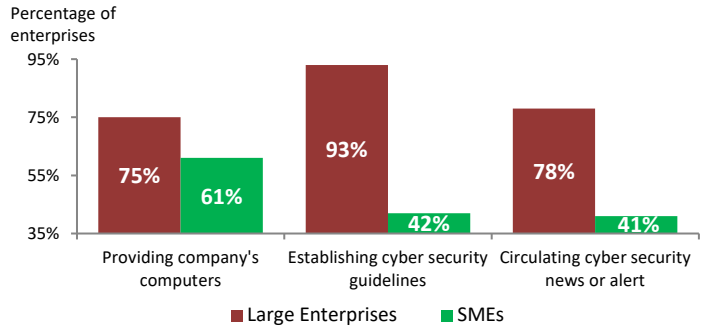


Figure 5 – Percentage share of enterprises with Investment Plans for Cyber Security in the coming 12 months, 2019-2020

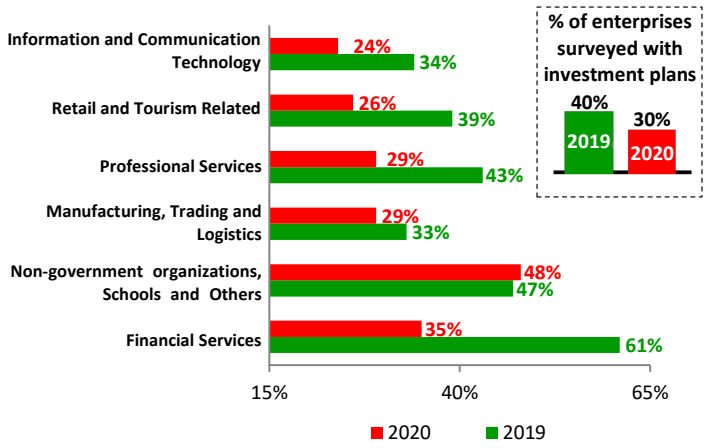
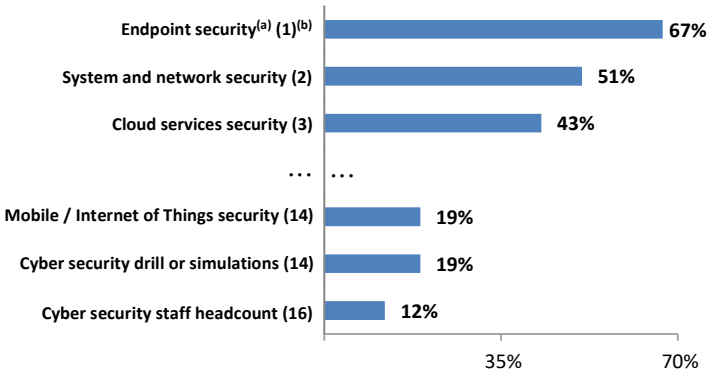


Figure 6 – Areas of cyber security investment in the coming 12 months, 2020



Notes: (a) Endpoint security refers to the practice of protecting enterprises' networks from malicious activities originated from desktops, laptops and other mobile devices.

(b) Figures in the parenthesis represent how enterprises rank the priorities of cyber security investment.

Highlights

- Large enterprises tend to be more resilient against cyber threat. They usually have more resources to implement cyber security measures in terms of providing company's computers for their staff, establishing cyber security guideline, and circulating cyber security news or alert (**Figure 4**). The provision of company's computers is of particular importance for cyber security. Without company's computers, staff members have to log in companies' email systems or networks through personal devices, which may not have standard security settings or anti-virus software.

- Enterprises' budgets on cyber security investment also reflect their attitudes toward safety in the cyber world. HKPC's 2020 survey revealed that a mere 30% of the companies surveyed had investment plans for cyber security in the next 12 months, compared with 40% in 2019 (**Figure 5**). Analysed by sector, the decline was almost across the board and most pronounced in the financial services sector (down from 61% in 2019 to 35% in 2020).

- Among companies with plans to enhance cyber security capability, "endpoint security" and "system and network security" were the prioritized areas of investment when upgrading their information technology ("IT") infrastructures (**Figure 6**). Meanwhile, enterprises were less likely to invest in non-technical areas. Among them, 19% would invest in cyber security drill or simulations and 12% in hiring more cyber security staff. The latter arouses the concern over the availability of cyber security professionals in Hong Kong. According to the latest statistics available, there were a mere 1 118 or 1.2% of IT employees specializing in IT security in 2018. The majority of these specialists were employed by the IT products and services suppliers (48% of the total) and the financing and business-related sectors (36%).

Data sources: Latest figures from Census and Statistics Department, Hong Kong Police Force, Hong Kong Productivity Council, Hong Kong Computer Emergency Response Team Coordination Centre and Hong Kong Internet Registration Corporation Limited.

Research Office
Information Services Division
Legislative Council Secretariat
30 April 2021
Tel: 2871 2145