HKPC Hong Kong Productivity Council 香港生產力促進局

HKCERT

Sponsored by SSH.COM

HKECSRI 2019

This study report is conducted independently by the Hong Kong Productivity Council (HKPC) with the framework of the index developed with the support from Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT).

SSH Hong Kong Enterprise Cyber Security Readiness Index 2019 Survey

Sponsored by SSH.COM

Content

1. Introduction

1.1 Background

With the change of modern lifestyles, Information Technology (IT) has inevitable become a crucial essence in our daily lives. Individuals and business parties are now inter- or intra-connected through the “cyber world” network. However, similar to the real world, the cyber world is also exposed to various security threats, which can cause immense impact and damage.

The HKSAR Government launched the Hong Kong Smart City Blueprint back in December 2017, which aimed to make use of innovation and technology to address urban challenges and enhance Hong Kong’s sustainability, efficiency and safety. The promotion of digital transformation among industry and citizens, more intensive network communications, as well as the use of big data will provide opportunities for both users and attackers. Cyber security readiness hence is of utmost importance for us to cope with the technological changes.

1.2 SSH Hong Kong Enterprise Cyber Security Readiness Index

Against the above background, the Hong Kong Productivity Council (HKPC) , with the support from the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), constructed the Hong Kong Enterprise Cyber Security Readiness Index (HKECSRI), so as to keep track of the local cyber security awareness and readiness in business sectors, raise public awareness, facilitate policy formulation and support preventive measures to tackle cyber threats.

This year, the framework is adopted the second time. With the sponsorship of SSH Communications Security (SSH.COM), the index is named “**SSH Hong Kong Enterprise Cyber Security Readiness Index”** (the Index); whilst the **SSH Hong Kong Enterprise Cyber Security Readiness Index Survey 2019** (the Survey) was independently conducted by HKPC including the methodology, design of questionnaire and the execution of the interview.

1.3 Special Topic

The Survey has incorporated a special theme this year for a more in-depth study. In 2019, the Survey will look at “Access Management – Internal & Third Party”.

Nowadays, data and system become one of the most valuable assets of a company in supporting business operation and development strategy. Yet, many companies are still allowing internal or external parties to freely access these valuable assets, reflecting excess trust in employees or third-party vendors. Such omission of robust system to manage and monitor the access from unnecessary parties may pose high risk to cybersecurity issues, eventually encouraging intentional and unintentional wrong-doings.

It is hence worthwhile to study the status of access management, raise the awareness on the issues and facilitate the planning of security strategy among Hong Kong enterprises.

1.4 Structure of Report

This report sets out the approach and methodology in conducting the Study, whereby we provide the Survey findings and then present the results of data analysis.

Following this introductory chapter, the rest of this document is structured as follows:

- Chapter 2 - Describes the methodology of the Study in detail;
- Chapter 3 - Presents the Survey results, data analysis and major findings;
- Chapter 4 - Draws conclusions and recommendations.

2. Methodology

2.1 Framework of the SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI)

The SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI) is set to assess the comprehensiveness of security measures of the respondents. There are four key areas in the comprehensiveness assessment: policy and compliance, process, technology, and human awareness.

Components of SSH-HKECSRI

The SSH-HKECSRI combines the sub-indices from below four aspects:

Overall SSH-HKECSRI = Average of the Sub-Indices (rounded off to one decimal place)

Assessing the maturity of current security measures adopted in the four mentioned major aspects, the index is calculated from 0 to 100. The higher the number, the more mature the security measures adopted.

Index Score (0 – 100)	Level	Description
0 – 20	Unaware	Organisation is unaware of cyber security investment necessary for business strategy. This level is characterised by the lack of security risk assessment to understand vulnerabilities and the impact on the organisation, and, lack of policy and controls to secure the business.
20.1 – 40	Ad-hoc	Organisation starts to be conscious about cyber security investment. This level is characterised by inconsistent, reactive and ad-hoc measures in response to security attacks. Some security controls are applied but not in a managed manner (planned, documented and repeatable process).
40.1 – 60	Basic	Organisation has built awareness to protect the business' investment against cyber attacks and ensure continuity. This level is characterised by the existence of some form of cyber security functions, basic security policy and procedure, implementation of technology controls but without central management and fine-grain access control; also security awareness education being provided to limited staff only.
60.1 – 80	Managed	Organisation is aware enough to manage security in a planned and controlled manner. This level is characterised by the existence of an organised full-time cyber security function, more comprehensive security policy and procedure, ownership of business processes with cyber security responsibility in place, centrally managed technology controls as well as mandatory and monitored access control; also user awareness education being provided to all general staff.
> 80	Anticipated	Organisation is aware of keeping abreast of the emerging cyber security threats and compliance requirements. This level is characterised by the full and open support of the Board of Directors for the cyber security function, more proactive than the Managed level to achieve higher readiness and to measure performance by benchmarking. A comprehensive security function is established within the organisation and communicated with external parties frequently. Organisation is aware of the global threat landscape and the security advancement outside the organisation, as well as keeps abreast of any risks related to business or technological changes.

2.2 Sample Distribution

Data is collected by telephone interview each year with no less than 350 Enterprises, at least 50 of which are large enterprises[1]. The sample is randomly selected from publicly available directories and the HKSAR Census database.

To guarantee that the view of every targeted industry is captured and represented in the study while considering the actual proportion in the population, quota sampling is adopted to cover six main categories according to the major economic activities in Hong Kong, namely:

1. Financial Services,
2. Retail and Tourism Related,
3. Manufacturing, Trading and Logistics,
4. Information and Communication Technology,
5. Professional Services and
6. Public Sector, Healthcare, NGO and Others.

[1] Manufacturing establishments with larger than 100 employees; and non-manufacturing establishments with larger than 50 employees, are regarded as Large Enterprises

The coverage of each category is referenced to Hong Kong Standard Industrial Classification (HSIC) version 2.0.

Category	Coverage
1. Financial Services	Banking/ Securities/ Insurance/ Other financial services
2. Retail and Tourism Related	Retail/ Food & Beverage/ Accommodation/ Travel Services
3. Manufacturing, Trading and Logistics	Manufacturing/ Import & export/ Wholesales/ Logistics
4. Information and Communication Technology	Information and Communication Technology
5. Professional Services	Legal/ Accounting/ Auditing/ Company secretary/ Consultancy, etc.
6. Public sector, Healthcare and Others	Public Sector/ Healthcare/ NGOs /Others

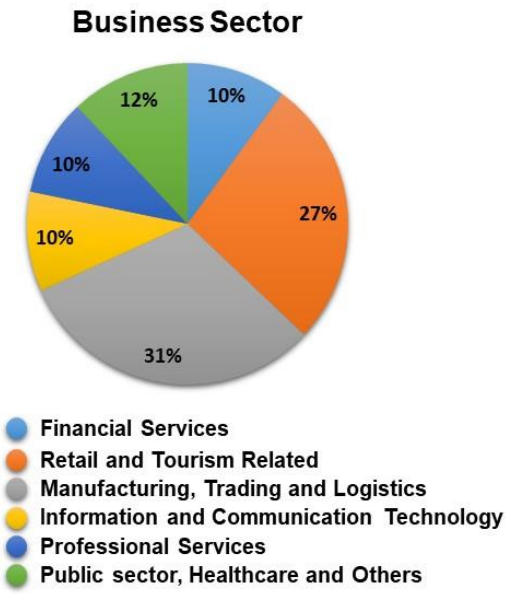
2.3 Profile of Respondents

The Survey successfully gauged the views of management-level or IT-responsible officers from 350 companies in Hong Kong.

As shown in Figure 1, at least 10% of response is collected from each business category; 31% is from “Manufacturing, Trading and Logistics” while 27% from “Retail and Tourism Related”, with the consideration of the numbers of establishments in those categories.

Among the 350 respondents, 296 of them were Small and Medium Enterprises (SMEs) and 54 were Large Enterprises.

Figure 1



	Size of Company (Number of Staff)						
	1-5	**6-20**	**21-50**	**51-100**	**101-200**	**201-500**	**>500**
Financial Services	9%	46%	31%	9%	3%	3%	0%
Retail and Tourism Related	26%	36%	20%	5%	5%	2%	5%
Manufacturing, Trading and Logistics	9%	39%	35%	12%	5%	0%	0%
Information and Communication Technology	11%	46%	29%	6%	6%	3%	0%
Professional Services	6%	37%	43%	9%	3%	3%	0%
Public sector, Healthcare and Others	12%	24%	37%	20%	5%	0%	2%
All Business Categories	**14%**	**38%**	**31%**	**10%**	**5%**	**1%**	**2%**

3. Findings

This chapter presents the Survey findings and data analysis for the study which is divided into four sub-sections as follows:

1. Cyber Security Environment
2. SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI)
3. Special Topic : Access Management – Internal and Third Party
4. Investment Plans for Cyber Security

We have interviewed 350 respondents in the Study, including 296 SMEs and 54 Large Enterprises.

3.1 Cyber Security Environment

This sub-section discusses the cyber security environment of the 350 interviewed companies, including:

- Views on the Importance of IT System & Data
- Type of Data Stored
- Cyber Attacks Experienced in the Past 12 Months

3.1.1. Views on the Importance of IT System & Data

The summerised view is calculated from the average score obtained. The respondents based on their perception of importance to rate the importance of IT system and data in the business sectors on a 0 - 4 marks scale, while “0” representing “not that important” and “4” representing “extremely important”.

All respondents treated IT system and data as an important matter; 95% of them rated “Important” or above while over half (54%) stated IT system and data as “Extremely important”, which is similar with that of last year’s with 97% rated “Important” or above.

All Business Categories	Not that important (0 mark)	Somewhat important (1 marks)	Important (2 marks)	Very important (3 marks)	Extremely important (4 marks)	Average score (0 – 4 marks)
2019	2%	3%	11%	29%	54%	**3.3**
2018	1%	2%	14%	25%	59%	**3.4**

For the Year on Year results, all business sectors think that IT system and data is seen important, with the average scores respectively being 3.3 in 2019 and 3.4 in 2018. In 2019, “Financial Services” and “Information and Communication Technology” are having the highest awareness with an average score of 3.5; whilst “Manufacturing, Trading and Logistics” and “Professional Services” are having low awareness relatively with an average score of 3.2 each.

Business Category	Not that important (0 mark)	Somewhat important (1 marks)	Important (2 marks)	Very important (3 marks)	Extremely important (4 marks)	Average score (0 – 4 marks)
Financial Services	0%	6%	9%	17%	69%	3.5
Retail and Tourism related	2%	2%	14%	30%	52%	3.3
Manufacturing, Trading and Logistics	3%	5%	13%	32%	48%	3.2
Information and Communication Technology	0%	3%	9%	20%	69%	3.5
Professional Services	3%	3%	9%	40%	46%	3.2
Public sector, Healthcare and Others	0%	0%	10%	32%	59%	3.5

Comparing the views of SMEs and large enterprises, it is noted that large enterprises (average score 3.5) in general regard IT system and data more important than SMEs (3.3) do.

Company Size	Average score (0 – 4 marks)
SME	3.3
Large Enterprises	3.5

3.1.2. Types of Data Stored

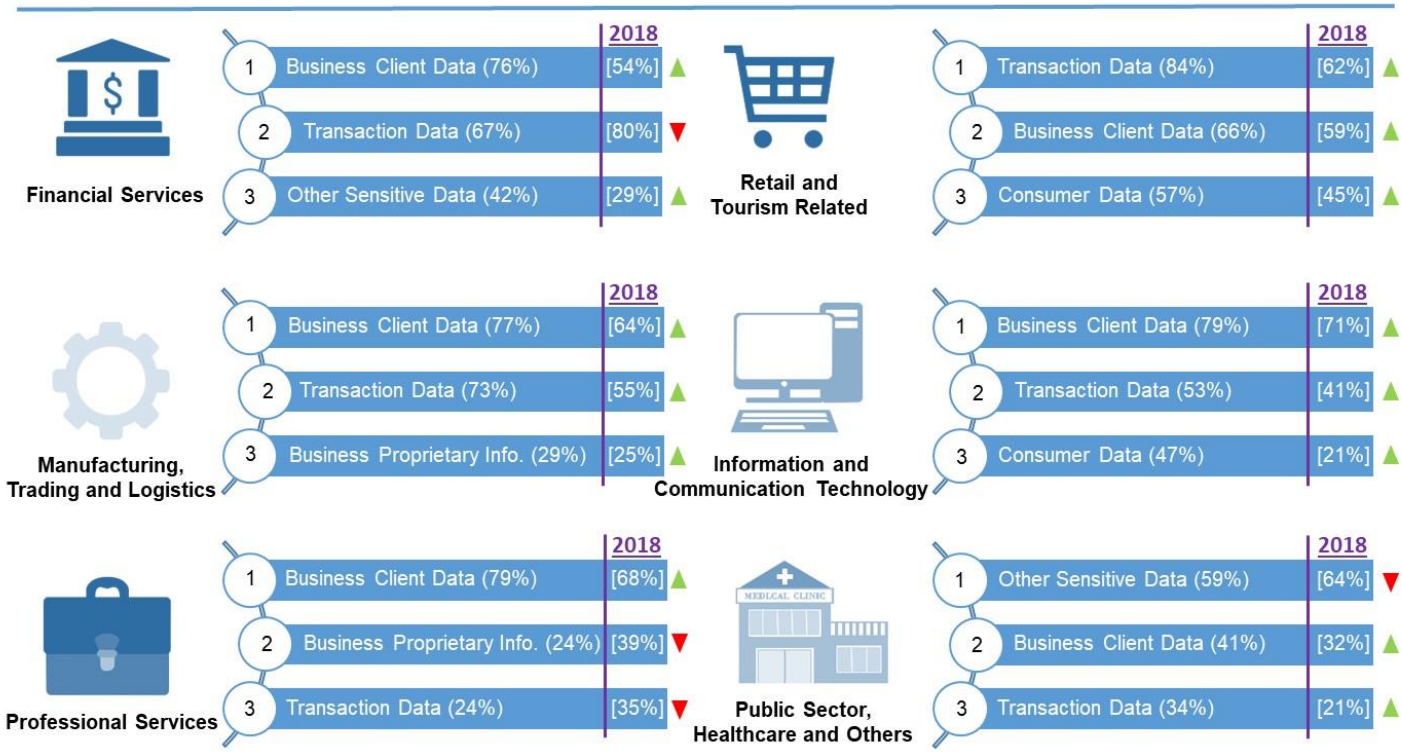
There are various types of data involved in daily business operations which are categorised as below for the analysis of the types of data stored.

- Consumer Data (e.g. ID number/ credit card number/ contact details)
- Business Client Data (e.g. contact details/ credits/ etc.)
- Transaction Data (e.g. payment information/ purchased items/ etc.)
- Business Proprietary Information (e.g. intellectual property, contracts, business confidential documents/ etc.)
- Other Sensitive Data (e.g. patient data/ membership data, etc.)

Different business categories stored different types of data. The majority of "Retail and Tourism Related" businesses stored "Transaction Data"; while "Public Sector, Healthcare and Others" mainly stored "Other Sensitive Data" such as patient or membership data. The other categories, namely "Financial Services", "Manufacturing, Trading and Logistics", "Information and Communication Technology" and "Professional Services", mainly stored "Business Client Data".

Comparing to 2018, it is noted that the industries have been storing more data in terms of the volume and types – data is certainly one of the most valuable assets in companies.

Type of Data Stored (Top 3)



3.1.3. Cyber Attacks Experienced in the Past 12 Months

3.1.3.1 External and Internal Attacks

Respondents were asked if they have encountered three specific types of attacks/incidents in the past 12 months. Among 60% of the respondents who had such cyber incidental experience, the most common type was the external attacks - such as phishing e-mail, ransomware and malware, accounted for 41%; while internal incidents (11%) and incidents caused by external partners (8%) were comparatively less common.

Compared to the findings from last year, higher number of respondents encountered attacks or incident. Companies are found to be exposing to more cyber security risks, with those related to external parties being more common.

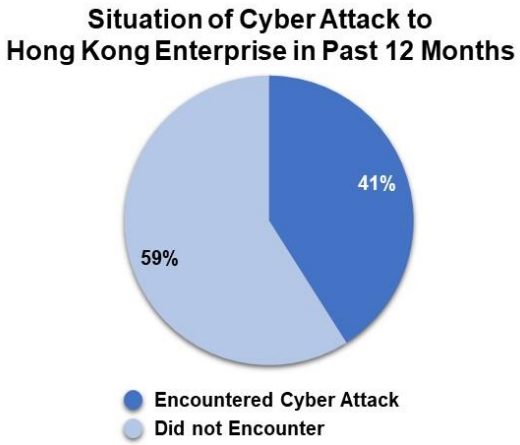
Type of Attacks/Incidents	Encountered Incidents		
	2019	2018	
External Attacks (e.g. Phishing Email, Ransomware, Malware)	41%	26%	▲
Internal Incidents (e.g. Loss of equipment, abuse of usage, unintended mistake)	11%	3%	▲
Incidents caused by External Partners (e.g. abuse of usage, data leakage)	8%	3%	▲

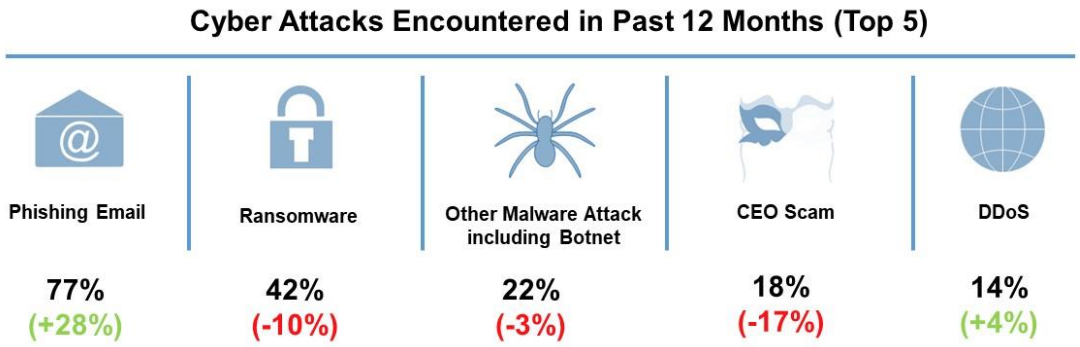
3.1.3.2 Form of Cyber Attacks Experienced

41% of the respondents encountered external attacks in past 12 months which can be classified into various criteria including:

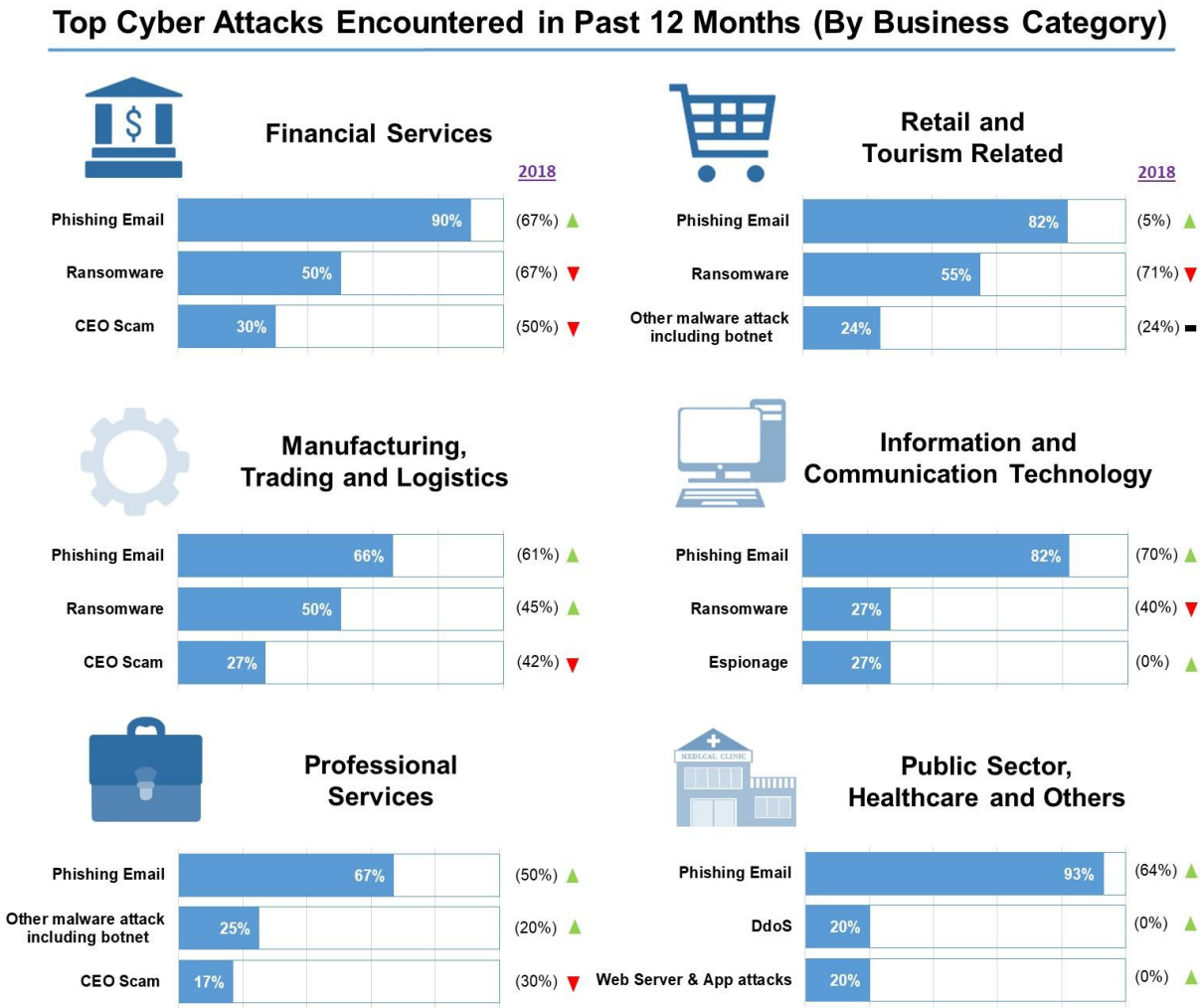
- Ransomware
- Other malware attack, including botnet
- Data/ credential leakage or theft
- Espionage
- CEO scam
- Phishing email
- DDoS (Distributed Denial of Service)
- Web server & app attacks
- Attack on other services like POS (Point of Sale) / remote access / CCTV (Closed-circuit television)
- Hacking targeting corporate service accounts
- Others

This year, the most common form of attack encountered was “Phishing Email” (77%), followed by “Ransomware” (42%), “Other malware attack” (35%), “CEO Scam” (18%) and “DDoS” (14%). A significant increase is noted in “Phishing Email” when comparing to last year.





Looking into the business categories, “Phishing Email” was the common issue faced by the six major industries, detailed below:



3.2 The SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI)

3.2.1 Indicators of SSH-HKECSRI 2019

The SSH-HKECSRI comprises of four sub-indices, which measures the comprehensiveness of security measures:

1. Policy & Assessment
2. Technology Control
3. Process Control
4. Human Awareness

Each sub-index has its own indicators, below are for 2019:

Sub-index	**Indicators of each Sub-index** Score (1 – 100)	**Sub-index Score**
Policy & Assessment	- Security risk assessment - Security Policy and practice	1 – 100
Technology Control	- Threat detection technology - Patch management - Security hardening	1 – 100
Process Control	- Data backup management - Privilege access management - Third party risk management	1 – 100
Human Awareness	- Cyber security awareness education	1 – 100
SSH-HKECSRI		**Average of sub-indices**

Each indicator has different expected activities which are mapped to the comprehensiveness levels of 0 to 4 (level 4 being the most comprehensive). Each level is assigned with a score as follows:

Level 0: 0

Level 1: 25

Level 2: 50

Level 3: 75

Level 4: 100

The sub-index score is the sum of the average of scores of all the indicators of that sub-index.

Below is the details of comprehensive levels of each indicator.

Security measures adopted in the past 12 months					
Comprehensiveness Levels	**0**	**1**	**2**	**3**	**4**
Marks allocated (0 – 100)	0	25	50	75	100
1.1 Security Risk Assessment	None	Only when project starts	Also when system changes	+1 for each of following: * Review critical IT systems regularly * Assess security risks of non-IT projects	
1.2 Security Policy and Practice	None	Security policy / guideline document is in place	Staff needs to acknowledge it	+1 for each of following: * Have a security policy / guideline to classify data according to sensitivity * Have a security / guideline on the responsibility of security incident response	
2.1 Cyber Threats Detection	None	Normal firewall and antivirus	+1 for each of following, max. 3 marks * IDS/IPS * Consolidated event logs of multiple systems * Acquire threat intelligence * Shared threat intelligence with others * Other relevant ones		
2.2 Patch Management	None	Occasionally when some people told to do	It is done regularly	+1 for each of following: * Have a central patch management * Verify and test the patch before deploying in production environment	
2.3 Security Hardening	None	Occasionally when some people told to do	It is done whenever new system is deployed	+1 for each of following: * Disable / remove unnecessary service / features of systems * Turn on logging / alert for errors for systems	
3.1 Privileged Access Management	None	Yes	Record in access log	Review access log when needed	Regular review of access log
3.2 Data Backup Management	None	Yes, but not regularly	Yes, at least weekly	+1 for each of following: * Keep offline/offsite copy * Conduct recovery drill exercise	
3.3 Third Party Risk Management	None	+1 for each of following, max. 4 marks * Basic network separation for protection * Steps to mitigate potential cyber risks from outsourcing * 3rd party required to give timely notification of their cyber incidents by contract or policy * Policies and controls for third parties in pace * Security risk assessment includes cyber risks related to partners and related information flow * Involve partners and contractors in company-side security awareness training			
4. Cyber Security Awareness Education	None	Only for new comers	Also for general staff	Cyber security drill exercise	C-level management openly involved

3.2.2 SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI) for 2019

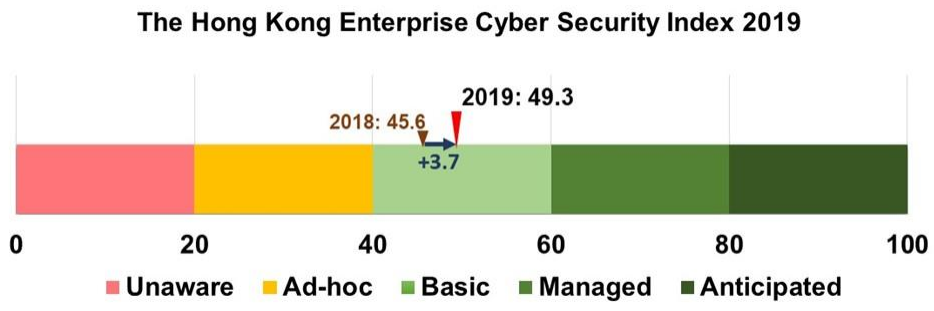
The index measures the overall cyber security capability in terms of composite security measures.

Overall SSH-HKECSRI = Average of Sub-Indices

The overall sub-indices are reordered below. The SSH-HKECSRI was then calculated by the average of the 4 sub-indices, assuming all indicators are of equal weightings.

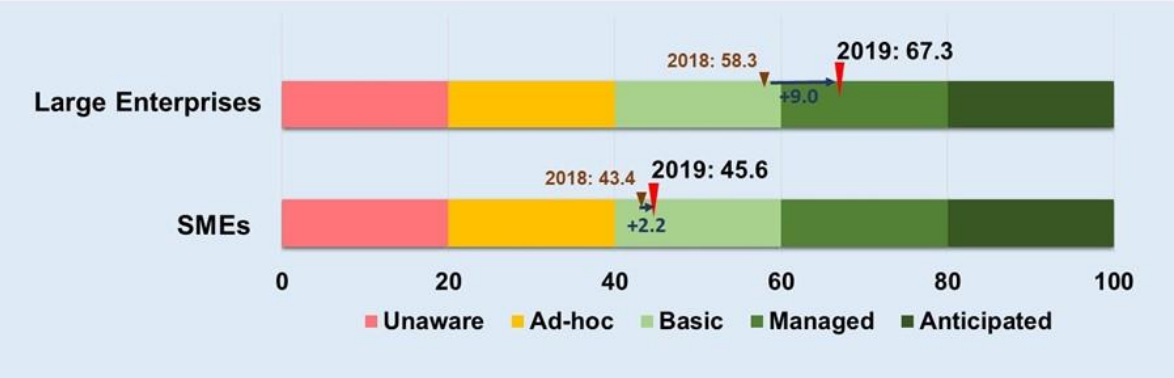
Component of Index	2019	2018	YoY Change
Policy & Assessment	**48.5**	49.4	-0.9
Technology Control	**63.4**	36.9	+26.6
Process Control	**55.7**	57.3	-1.5
Human Awareness	**29.5**	38.8	-9.3
SSH-HKECSRI = average of sub-index scores	**49.3**	45.6	**+3.7**

The **SSH Hong Kong Enterprise Cyber Security Readiness Index 2019** (SSH-HKECSRI 2019) is reported as **49.3** that the overall cyber security capability was "**Basic**" according to the ruler below. Comparing with last year's, the index has increased 3.7 yet remained at the "Basic" level.



When considering the company size, large enterprises has moved from upper "Basic" level to "Managed" level at 67.3 while SMEs remained in the lower "Basic" level at 45.6, despite a slight increment of 2.2.

HKECSRI by Organization Size



The scores of sub-indices and indicators for different business categories are listed in the following table. The bottom row shows the sub-index for each business category. The top two measures of each business category are highlighted in green.

	Average Rating for Business Categories						
Indicators of Sub-indices	FS	RT	MTL	ICT	PS	PHO	All
1. Policy & Assessment	**66.6**	**42.9**	**43.9**	**58.2**	**47.1**	**50.9**	**48.5**
1.1 Security Risk Assessment	64.0	39.7	40.4	61.4	42.6	46.3	45.6
1.2 Security Policy and Practice	69.3	46.2	47.5	55.0	51.5	55.6	51.5
2. Technology Controls	**71.6**	**51.1**	**53.3**	**58.1**	**54.0**	**58.5**	**55.7**
2.1 Cyber Threat Detection	65.0	43.4	41.6	49.3	46.4	47.0	46.3
2.2 Patch Management	75.7	57.4	66.7	79.3	67.9	72.4	67.2
2.3 Security Hardening	82.4	75.3	72.4	82.4	79.5	81.1	76.9
3. Process Control	**74.4**	**58.7**	**60.2**	**70.3**	**64.6**	**66.8**	**63.4**
3.1 Privileged Access Management	72.8	48.1	57.5	62.1	60.0	59.8	57.5
3.2 Data Backup Management	95.0	80.6	85.7	88.6	87.1	92.1	86.4
3.3 Third Party Risk Management	47.1	24.7	16.8	23.6	15.0	23.8	23.3
4. Human Awareness	**51.4**	**23.4**	**25.7**	**36.4**	**26.4**	**31.1**	**29.5**
4.1 Cyber Security Awareness Education	51.4	23.4	25.7	36.4	26.4	31.1	29.5
Average Sub-index	**66.0**	**44.0**	**45.8**	**55.8**	**48.0**	**51.8**	**49.3**

FS: Financial Services **RT:** Retail and Tourism related **MTL:** Manufacturing, Trading and Logistics

ICT: Information and Communication Technology **PS:** Professional Services **PHO:** Public sector, Healthcare and Others

All: All Business Categories

Process Control and Technology Control were top two most popular measures which were adopted across business categories. It is worth noting that the indicators in Process Controls vary drastically. While “data backup management” and “privileged access management” had excellent adoption across business categories, “third party risk management” was not impressive.

For “Technology Controls”, “Patch Management” and “Security Hardening” were widely adopted, whilst “Cyber Threat Detection” was still in a growing stage. Yet, it scored above 50 (out of 100) in the “Financial Services” industry implying that most companies were still using preventive measures rather than threat intelligence-based measures.

Overall speaking, only the “Financial Services” industry has the average sub-index score above 50. Other industries were comparatively putting fewer resources in the area of cyber security - which is the key success factor for safety.

The order of Enterprise Cyber Security Readiness Index by business category is shown below. While “Financial Services” industry reached “Managed” level (60.1 – 80), the rest of them were in the “Basic” level (40.1 – 60).

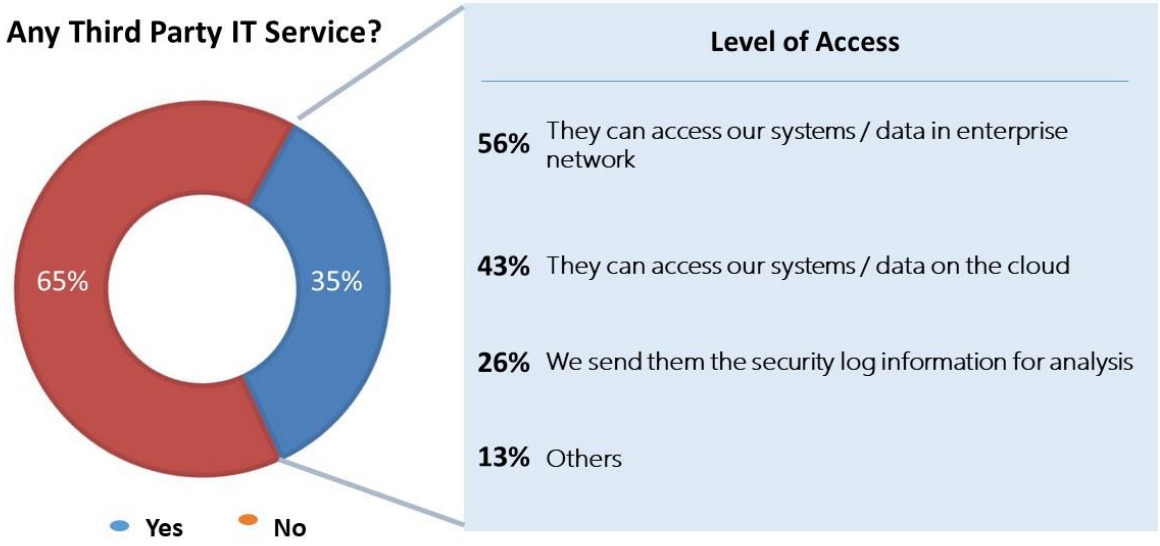
Enterprise Cyber Security Readiness Index by business category

	2019 Index	2019 Level	2018 Index	2018 Level	YoY Change	Change in Level
Financial Services	**66.0**	**Managed**	60.5	**Managed**	+5.5	**Unchanged**
Information and Communication Technology	**55.8**	**Basic**	51.6	**Basic**	+4.1	**Unchanged**
Public sector, Healthcare NGO and Others	**51.8**	**Basic**	45.5	**Basic**	+6.4	**Unchanged**
Professional Services	**48.0**	**Basic**	49.5	**Basic**	-1.5	**Unchanged**
Manufacturing, Trading and Logistics	**45.8**	**Basic**	41.9	**Basic**	+3.9	**Unchanged**
Retail and Tourism related	**44.0**	**Basic**	41.3	**Basic**	+2.7	**Unchanged**
SSH-HKECSRI (All Business Categories)	**49.3**	**Basic**	**45.6**	**Basic**	+3.7	**Unchanged**

3.3 Special Topic: Access Management – Internal & Third Party

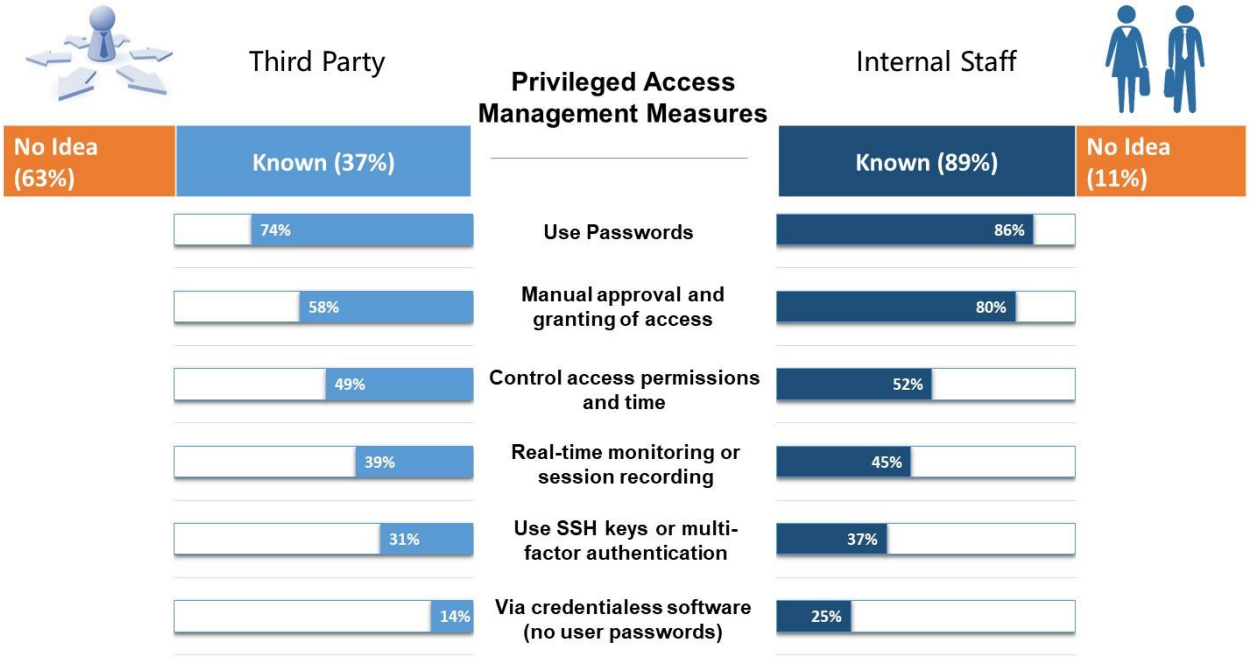
In addition to the standard SSH-HKECSRI, the Survey also includes one special topic. In 2019, the special topic was “Access Management – Internal & Third Party”.

3.3.1 Third Party Access to Corporate System/Data



It was worth to note that 35% of the respondents used or adopted third party IT services, in which over half (56%) allowed service providers to access into their systems or data in their enterprise network, while 43% allowed the service providers access their systems or data the on the cloud.

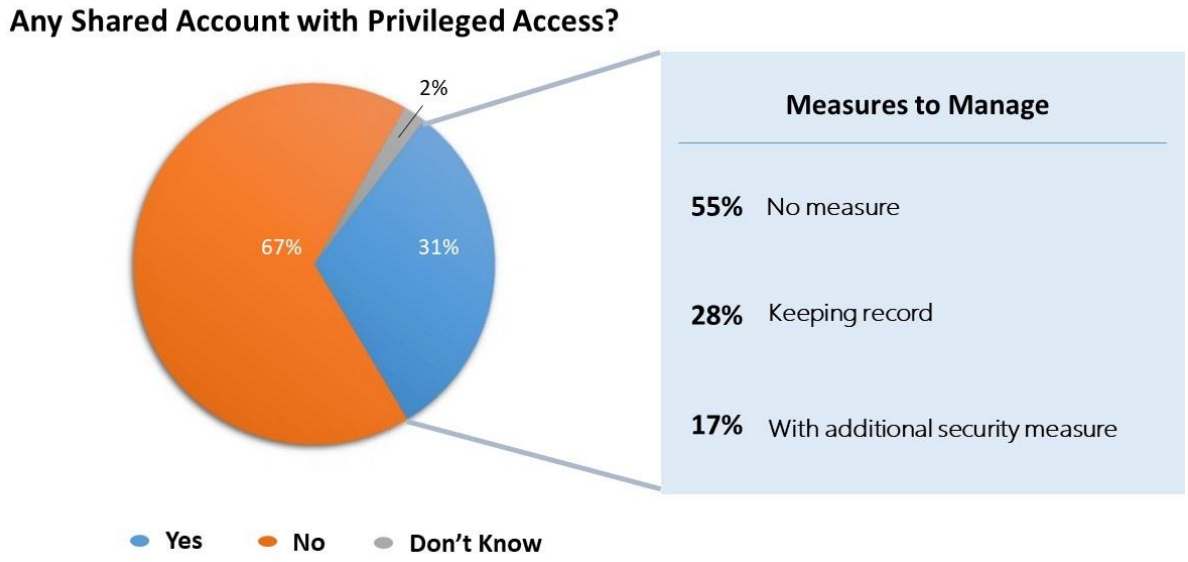
3.3.2 Privileged Access Management



Regarding the privileged access management, 89% of respondents knew the measures adopted for internal staff; while only 37% could tell that for third party.

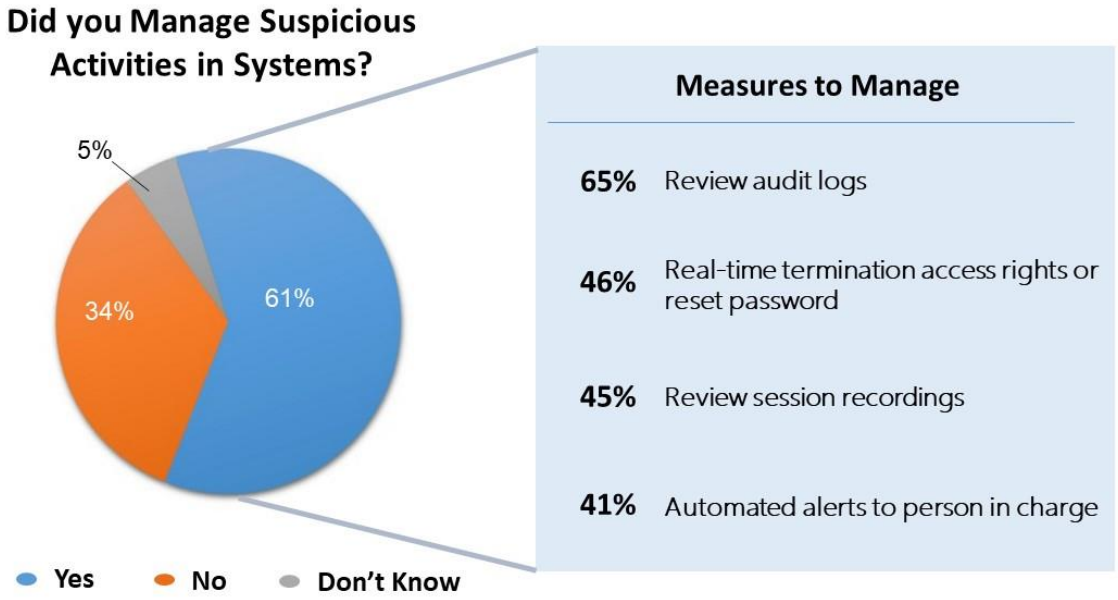
In terms of popularity, measures adopted for the internal staff and third party were in the same order. The most popular measure was the traditional tactic to “Use passwords”, followed by the use of “Manual approval and granting of access”, as well as “Control access permission and time”. While the advanced measures providing better management and granularity of control such as “Real-time monitoring or session recording”, “Use SSH keys or multi-factor authentication” and “Via credentialess software (no user passwords)” were less adopted.

3.3.3 Shared Account with Privileged Access

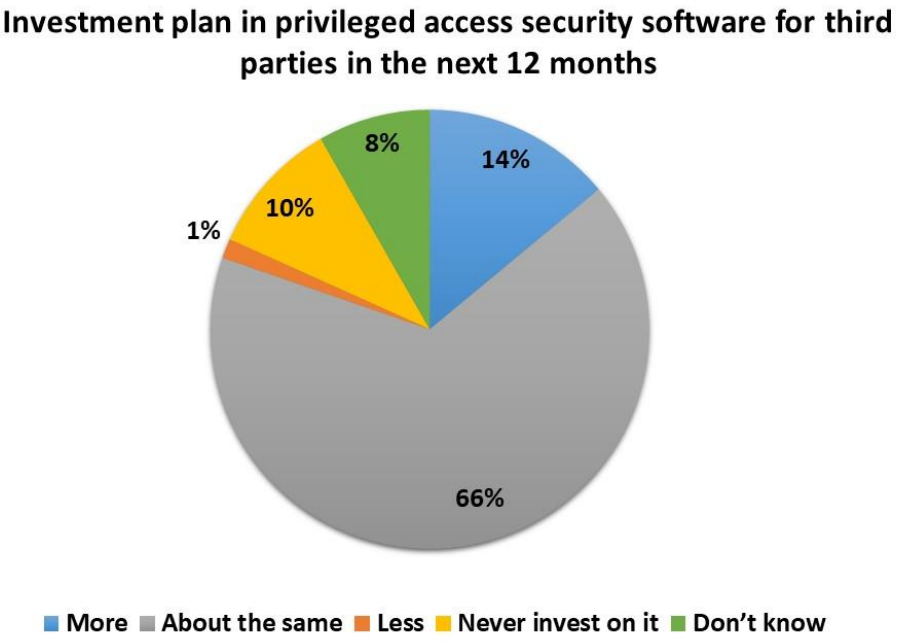


More than half of the respondents had no shared account with privileged access. Among the 31% who had shared accounts with privileged access, over half had no measures to manage the shared accounts.

3.3.4 Managing Suspicious Activities in Systems



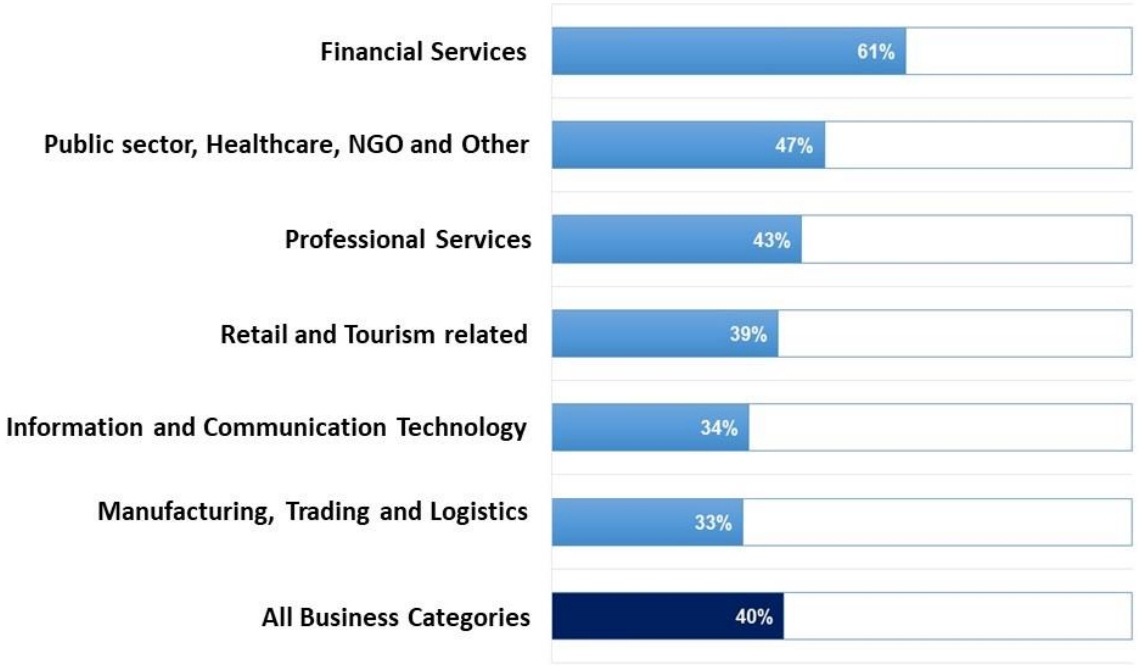
3.3.5 Investment Plan in Privileged Access Security Software



Most of the respondents (66%) would have about the same investment in privileged access security software for third parties in the coming 12 months, while 14% would have more investment. It is worth noting that 10% never invested in privileged access and 8% did not know about that.

3.4 Investment Plans for Cyber Security in the Coming 12 Months

40% of the respondents were planning to enhance cyber security in the coming 12 months. While the "Financial Services" industry (61%) was seen most proactive, the "Information and Communication Technology" (34%) and "Manufacturing, Trading and Logistics" (33%) industries were less active.



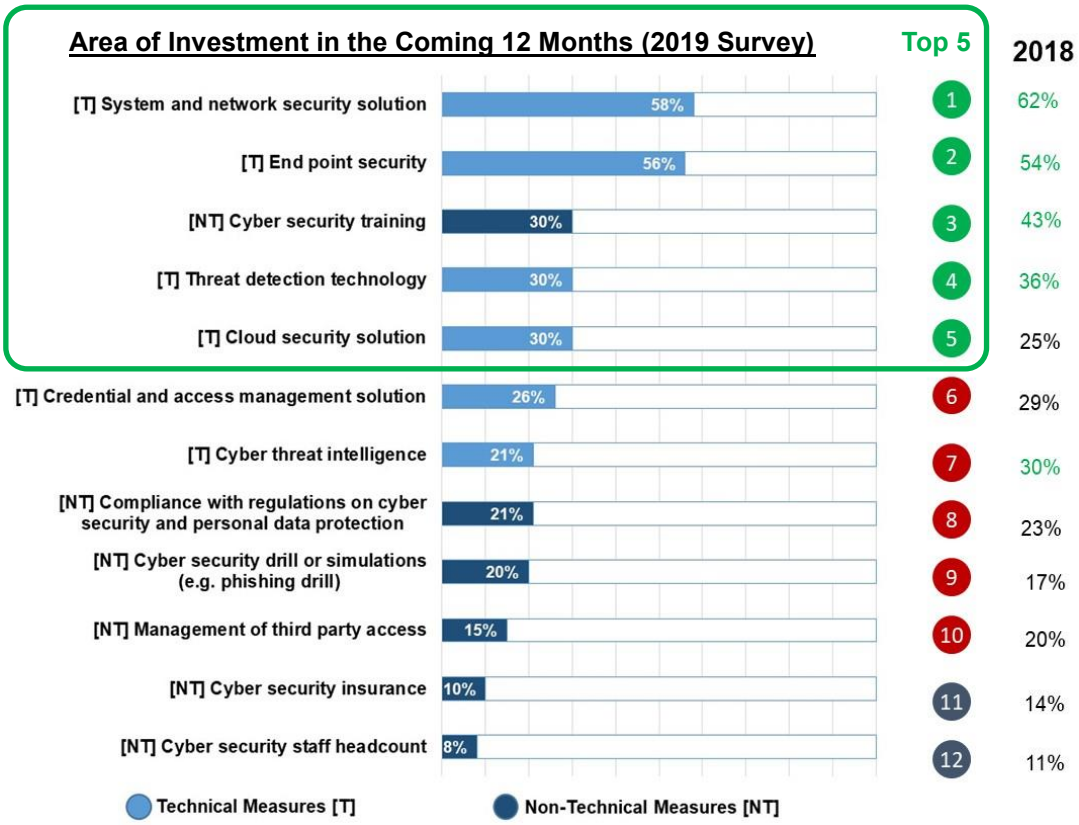
The investment areas can be classified into technical and non-technical measures as below:

Technical Measures:

- End point security
- System and network security solution
- Cloud security solution
- Credential and access management solution
- Threat detection technology
- Cyber threat intelligence

Non-Technical Measures:

- Cyber security insurance
- Cyber security staff headcount
- Cyber security training
- Cyber security drill or simulations (e.g. phishing drill)
- Management of third party access
- Compliance with regulations on cyber security and personal data protection
- Others



Among all investment areas, the “System and network security solution” (58%) and “End point security” (56 %) are the top two popular ones which are the common IT infrastructure of enterprises regardless of the sector and size. While the non-technical measure, “Cyber security training” (30%) remained in the third place for investment in 2019 and as the top non-technical measure, despite its percentage has dropped significantly (43% in the previous year).

The 4th popular area for investment in the coming 12 months was “Threat detection technology” that we expected it will rise in the future years together with the 6th one “Credential and assess management solutions” and 7th “Cyber threat intelligence” which are the newer technologies.

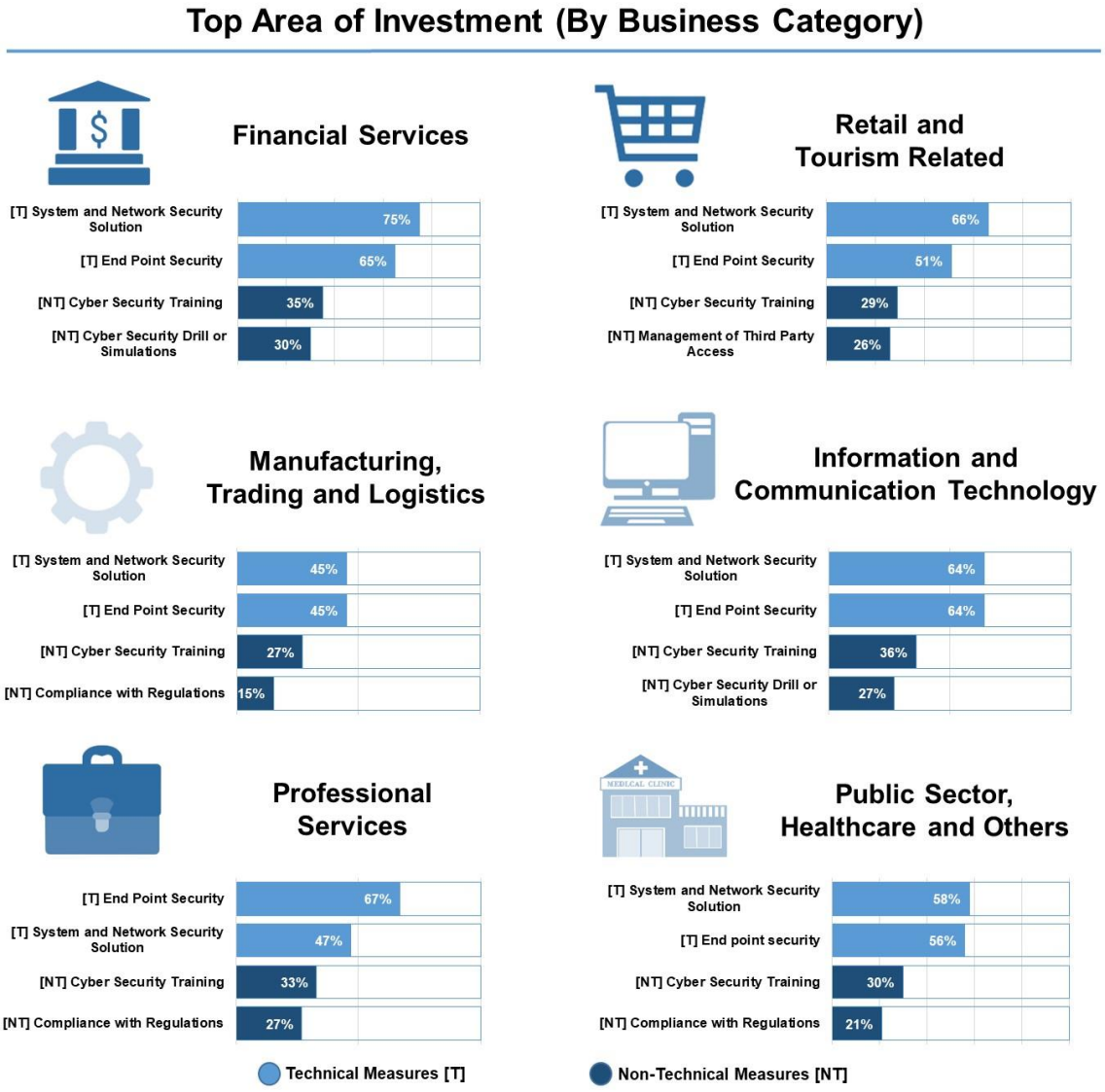
30% of respondents would invest in “Cloud security” which climbed from 7th in 2018 to 5th in 2019. It reflected that cloud technology was becoming more mature and more widely adopted.

It was worth to note that “Management of third party access” has dropped to 10th from 9th this year.

For non-technical measures, the “Cyber security insurance” (10%) and “Cyber security staff headcount” (8%) remained as the least popular ones in 2019. It is believed that “Cyber security insurance” was still a fresh new concept to many enterprises in Hong Kong and worthwhile to track its growth in future

surveys. Although the job market for cyber security professionals was hot owing to the growing cyber security threats, enterprises are seen not putting “Cyber security staff headcount” to a higher priority perhaps due to the cost concern and difficulties in finding the right candidate to suit short-term needs.

In terms of the business categories, the top two areas of investment in technical measures and non-technical measures are presented as below:



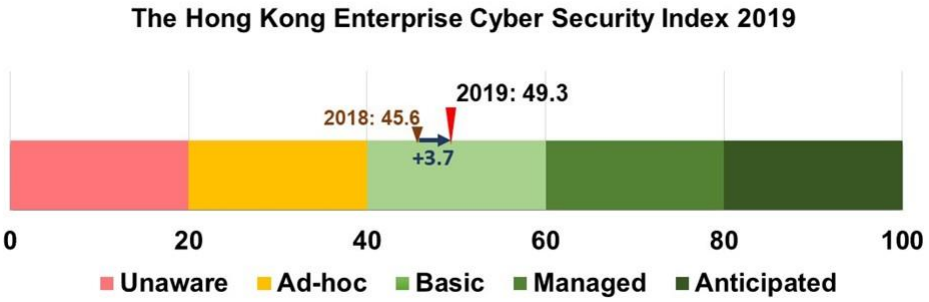
4 Conclusion & Recommendations

4.1 Key Findings

The Hong Kong Cyber Security Readiness Index

(1) The SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI) indicated the overall level of security maturity among Hong Kong Enterprises which remained at "Basic" this year.

The SSH-HKECSRI in the 2019 survey has increased from 45.6 to 49.3 and was same as last year's "Basic" level.



(2) "Financial services" was still the best performing business category, remained in the "Managed" level with a score of 66.0.

All other business categories were at the "Basic" level, in the range of 44-56.

.

(3) "Large Enterprises" ranked higher than SMEs.

The Cyber Security Readiness Index for Large Enterprises alone was promoted from "Basic" level (58.3 in 2018) to "Managed" level (67.3), while SMEs remained at the "Basic" level (45.6). This means that larger enterprises generally adopted more comprehensive cyber security measures than smaller ones.

(4) The majority of enterprises scored high in "data backup management" which is widely used to mitigate ransomware and extortion attacks that hinge on the availability of data.

Indicators	
1. Policy & Assessment	**48.5**
1.1 Security Risk Assessment	45.6
1.2 Security Policy and Practice	51.5
2. Technology Controls	**55.7**
2.1 Cyber Threats Detection	46.3
2.2 Patch Management	67.2
2.3 Security Hardening	76.9
3. Process Control	**63.4**
3.1 Privileged Access Management	57.5
3.2 Data Backup Management	**86.4**
3.3 Third Party Risk Management	23.3
4. Human Awareness	**29.5**
4.1 Cyber Security Awareness Education	29.5

(5) "Privileged access management" is crucial in mitigating exposure to advanced persistent threats (APT), internal and external incidents. It had the score of 57.5.

(6) "Third Party Risk Management" recorded the lowest score (23.3) which is alarming.

This result had to be interpreted together with other points in this section namely,

- Point #10 on the ignorance of Privileged Access Management for Third Party.
- Point #15 on the low priority of "Management of third party access" in investment.

While the score of privileged access management was 57.5 as in point #5 that respondents understood its importance, only 37% respondents could tell what security measures were adopted for privileged access management for third party from point #10 and "Management of third party security access" was of low priority (10th) in future investment from point #15.

Cyber Security Environments

(7) Nearly all (94%) of the respondents regarded IT systems and data as highly important. The most common responses were: important (11%), very important (29%) and extremely important (54%).

(8) More respondents (41%) encountered external attacks in 2019 than that in 2018 (26%). Internal incidents also raised to 11% 2019 from 3% in 2018 while incidents caused by external partners raised to 8% 2019 from 3% in 2018.

(9) The top three external attacks in the past 12 months were Phishing (77%), Ransomware (42%), and Other Malware Attack including Botnet (22%).
It was worth to note that "Phishing" raised significantly from 49% in 2018.

Assess Management – Internal and Third Party

(10) Privileged Access Management for Third Party was largely ignored
Among the 35% of respondents who had third party IT services, more than a half (56%) allowed the service provider access to their systems or data in their enterprise network and 43% allowed the service provider access to their systems or data on the cloud. **However, only 37% of respondents could tell what kind of management measures of privileged access were adopted for third party**.

(11) The majority of the respondents were using basic solutions in privileged access management. Advanced solutions ("Real-time monitoring or session recording", "Use SSH keys or multi-factor authentication" and "Via credentialess software") had a low adoption rate for both internal staff (25%-45%) and third party (14%-39%).

(12) Shared accounts with Privileged Access were not properly managed. Over 55% of the respondents had not adopted measures to manage these accounts.

Cyber Security Investment Plan in the Coming 12 Months

(13) 40% of all respondents planned to enhance cyber security in the coming 12 months.
The top three business categories in cyber security investment were "Financial services" (61%), "Public sector, Healthcare, NGO and others" (47%) and "Professional Services" (43%).

(14) Technology solutions occupied four of the top five investment areas. "Cyber security training" being the only non-technology solution ranked the third.

The four technology solutions were "System and network solution", "End-point security", "Threat detection technology" and "Cloud security solution" which climbed from 7th in 2018 to 5th in 2019, reflecting the maturity and popularity of the use of cloud technology.

"Cyber security training" was less popular in 2019. The drop might be due to the lack of prominent cyber attacks in the past 12 months that made cyber security awareness education an urgent need.

(15) "Management of third party access" ranked 10th out of 12 investment areas which the respondents would invest in the coming one year.

4.2 Recommendations

(1) Enterprises putting more efforts in cyber security

Enterprises should enhance their cyber security readiness to reach the "Managed" and "Anticipated" level, especially for larger enterprises.

To get the most significant improvement, efforts could be directed towards weaker areas, such as "Third Party Risk Management", "Cyber Security Awareness Training", "Security Risk Assessment" and "Cyber Threat Detection".

(2) Manage Third Party Risks

"Supply Chain Attack" was one of the five potential cyber security trends in 2019[2], where cyber criminals try to exploit the supply chain through third-party suppliers who usually have some level of access to their customer's network. Thus, enterprises should pay more attention to risks posed by third parties. For example, a significant number of financial institutions co-operates with fintech partners whose security standards might be lower than those of the financial institutions; supply chain partners are connected via network interfaces to exchange production data and logistics data in the manufacturing and logistics sectors, that the network interfaces and application programming interfaces are the potential attack surfaces for attackers.

As more and more cyber attacks attempt to exploit the weakest part of the supply chain, enterprises are advised to enhance their supply chain security management. The Guideline

[2] HKPC Urges Enterprises to Adopt "Security by Design" to Sharpen IT Security in 2019 https://www.hkcert.org/my_url/en/articles/19012201

"Understanding and Tackling Supply Chain Attacks"[3] detailing the nature of supply chain attacks and providing steps to tackle the risks has been published, below a brief:

- Include third party risks in security risk assessment, estimate risks and the flow of information with partners
- Put in place security policy and contract terms to control outsourcing partners
- Require partners to include security protection in their processes
- Segregate networks with partners and set up proper access control
- Involve partners in enterprise awareness education when necessary

(3) Embrace Cyber Threat Detection

As a new thinking for cyber security, we should compromise and figure out how to detect the compromise as early as possible. Traditional preventions (e.g. firewall and antivirus) are necessary but not sufficient. Instead, the defense-in-depth approach embracing detection strategies to discover threats within the enterprise infrastructure and acquiring threat intelligence outside the enterprise are both essential measures for ramping up the threat responsiveness of enterprises.

(4) Raise Cyber Security Awareness via Education

Cyber security awareness education is usually in low priority until there is a huge media exposure of prominent cyber attacks. Top attacks in 2019 included phishing, ransomware and CEO scams leveraged on human vulnerability. For example, a staff accidentally opened an attachment which included ransomware would cause the data on the enterprise server to be encrypted and become inaccessible.

It is advised to move up cyber security awareness education as an important part of the enterprise security strategy as follows:

- Provide training to all general staff and newcomers.
- Conduct regular cyber drill exercises, monitor performance and address the weakest areas.
- Obtain senior management's open commitment to reinforce a culture of security.

(5) Raise awareness of Access Management

More awareness education and technical seminars should be provided on access management and advanced solutions. When enterprises deploy more IT applications, especially in the cloud and through outsourcing, data becomes more exposed to third party risks. Assessing the role of credentials management should be an integral part of these projects.

- End of Report -

[3] https://www.hkcert.org/my_url/en/guideline/18041201

About HKPC

The Hong Kong Productivity Council (HKPC) is a multi-disciplinary organisation established by statute in 1967, to promote productivity excellence through integrated advanced technologies and innovative service offerings to support Hong Kong enterprises. HKPC is the champion and expert in facilitating Hong Kong's reindustrialisation empowered by Industry 4.0 and Enterprise 4.0 – focusing on R&D, IoT, big data analytics, AI and Robotics technology development, digital manufacturing, etc., to help enterprises and industries upgrade their business performance, lower operating costs, increase productivity and enhance competitiveness.

HKPC is a trusted partner with all-rounded innovative solutions for Hong Kong industries and enterprises, enabling them to achieve resources and productivity utilisation, effectiveness and cost reduction, and enhanced competitiveness in both local and international marketplaces.

In addition, HKPC partners and collaborates with local industries and enterprises to develop applied technology solutions for value creation. It also benefits a variety of sectors both locally and internationally through product innovation and technology transfer, with commercialisation of multiple market-driven patents and technologies, bringing enormous opportunities abound for licensing and transferring technology.
For more information, please visit www.hkpc.org.

About HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) is operated by HKPC, It is the centre for coordination of computer security incident response for local enterprises and Internet Users. Its missions are to facilitate information disseminating, provide advices on preventive measures against security threats and to promote information security awareness. HKCERT collaborates with local bodies to collect and disseminate information and coordinate response actions. HKCERT is also a member of the Forum of Incident Response and Security Teams (FIRST) and the Asia Pacific Computer Emergency Response Teams (APCERT).
For more information, please visit https://www.hkcert.org.

About SSH.COM

SSH.COM helps organisations access, secure and control their digital core – their critical data, applications and services. The company has 3,000 customers around the world, including 40 % of Fortune 500 companies, many of the world's largest financial institutions, and major organisations in all verticals. The company helps customers thrive in the cloud era with solutions that offer secure access with zero inertia, zero friction and zero credentials risk. SSH.COM sells online; through offices in North America, Europe and Asia; and through a global network of certified partners. The company's shares (SSH1V) are quoted on the Nasdaq Helsinki. For more information, visit www.ssh.com.

License

Disclaimer

SSH-
HKECSRI
2019

Published by Hong Kong Productivity Council

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong

Tel	(852) 2788 5678
Fax	(852) 2788 5900
Website	www.hkpc.org
Email	hkpcenq@hkpc.org