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

HKCERT

Sponsored by SSH.COM

HKECSRI 2018

A study report conducted independently by the Hong Kong Productivity Council (HKPC) Reseach Team and the framework of the index was developed with the support of Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT).

SSH Hong Kong Enterprise Cyber Security Readiness Index 2018 Survey

Sponsored by SSH.COM

Content

1. Introduction

1.1 Background

Information Technology (IT) is already an essential and crucial element in our daily lives. Both individuals and business parties are inter-connected through the network of the “cyber world”. However, similarly to the real world, the cyber world is exposed to various security threats that can cause immense impact and damage.

In Hong Kong, the Government of the Hong Kong Special Administrative Region issued its first Hong Kong Smart City Blueprint 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 in every industry and in the daily lives of citizens, more intensive network communications, and the use of big data, will provide opportunities for both good guys and attackers. We need to keep track of the status of cyber security readiness and ensure it can keep up with technological change.

1.2 SSH Hong Kong Enterprise Cyber Security Readiness Index

In view of the above background, the Hong Kong Productivity Council Research Team (HKPC), with the support of the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), developed a comprehensive framework to construct the Hong Kong Enterprise Cyber Security Readiness Index (HKECSRI) to keep track of the status of local cyber security awareness and readiness in business sectors to raise public awareness, to facilitate policy formulation and to support preventive measures to tackle cyber threats.

In 2018 the first survey applying this framework was conducted by HKPC with the sponsorship of SSH Communications Security (SSH.COM). The index is named the **SSH Hong Kong Enterprise Cyber Security Readiness Index** (the “Index”) to reflect this collaboration. The methodology of the **SSH Hong Kong Enterprise Cyber Security Readiness Index Survey 2018 (**the **“**Survey”), the design of questionnaire and the execution of the interview were decided and conducted by HKPC independently.

1.3 Special Topic

Besides the Index, the Survey also picks one special topic each year for in-depth study. For 2018, the chosen special topic was “Credentials Management”.

Credentials are defined as the information used to authenticate a user or device to access network services, which is essential to control access to sensitive data.

Credential Management is the solution or service that helps enterprises to manage the **creation, storage and revocation** of credentials, as **users** (staff/partners/customers) come and go or change role, and as **business processes** evolve. It is a key success factor in Identity, Authentication and Access Management (IAAM).

In 2017, Hackers obtained login credentials to access data on Uber’s Amazon Web Services. 57 million of Uber customers were leaked. It is clear that a proper management of credentials and privileged access is crucial to the security of critical services. In the cloud computing era, the amount of credentials and the involvement of third parties in IAAM grow exponentially. Credentials are expected to be one of the most important topics to be managed in the cyber environment.

1.4 Structure of Report

This report sets out our 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

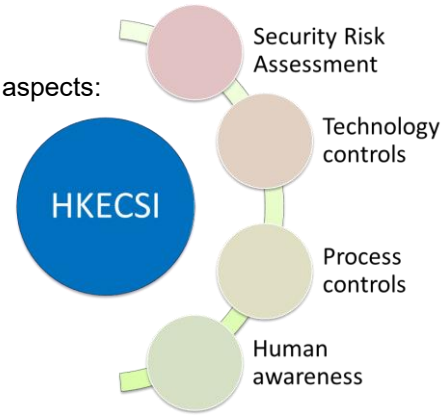
2.1 Framework of the SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI)

The SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI) is constructed by assessing the comprehensiveness of security measures of the respondents. Comprehensiveness is assessed in four key areas: policy and compliance, process, technology and human awareness. Questions in the four key areas are devised by information security professionals according to cyber security development. The options given to respondents are classified in scores based on comprehensiveness level.

Components of SSH-HKECSRI

The SSH-HKECSRI is composed of sub-indices from four aspects:

- Security Risk Assessment
- Technology Controls
- Process Controls
- Human Awareness



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

The index has a range of 0 to 100. The index score is mapped to a level.

Index range	Level
0 - 20	Unaware
21 - 40	Ad-hoc
41 - 60	Basic
61 – 80	Managed
> 80	Anticipated

2.2 Sample Distribution

Data is collected by telephone interview with no less than 350 Enterprises, with at least 50 of them being Large Enterprises[1] in each year. 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 accordingly 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.

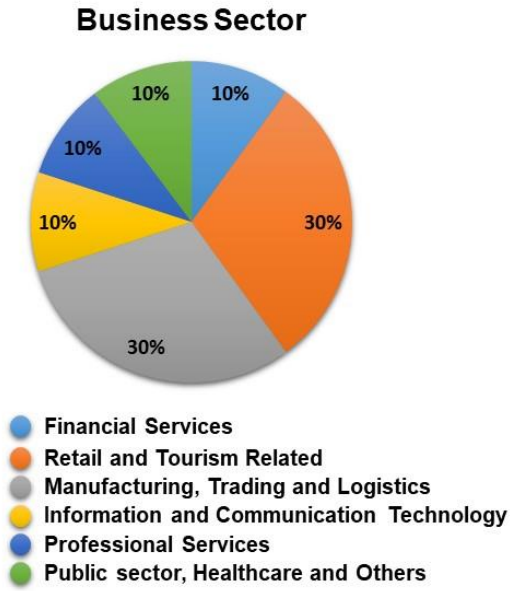
Category	Coverage
1. Financial Services	Banking/ Securities/ Insurance/ Other financial services
2. Retail and Tourism related	Retail/ Food & Beverage/ Accommodation/ Travel Services
3. Manufacturing, Trading and Logistics	Manufacturing/ Import & export/ Wholesales/ Logistics
4. Information and Communication 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 the figure, at least 10% of responses are collected for each business category, with 30% from both “Retail and Tourism Related” and “Manufacturing, Trading and Logistics”, with the consideration of the numbers of establishments in those categories.

Among the 350 respondents, 300 of them were Small and Medium Enterprises (SMEs) and 50 of them were Large Enterprises.



SMEs
Sample Size: 300

Large Enterprises
Sample Size: 50

	Size of Company (Number of Staff)						
	1-5	**6-20**	**21-50**	**51-100**	**101-200**	**201-500**	**>500**
Financial Services	0%	31%	54%	3%	6%	3%	3%
Retail and Tourism related	22%	28%	36%	4%	5%	5%	1%
Manufacturing, Trading and Logistics	12%	36%	32%	11%	5%	1%	2%
Information and Communication Technology	14%	46%	26%	6%	3%	3%	3%
Professional Services	15%	29%	41%	0%	15%	0%	0%
Public sector, Healthcare and Others	11%	25%	50%	3%	6%	0%	6%
All Business Categories	**14%**	**32%**	**38%**	**6%**	**6%**	**2%**	**2%**

3. Findings

This chapter presents the survey findings and data analysis for the study and is divided into four sub-sections. The topics covered are as follows:

1. Cyber Security Environment
2. SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI)
3. Special Topic - Credentials Management
4. Investment Plans for Cyber Security

350 respondents were successfully interviewed in this study, including 300 SMEs and 50 Large Enterprises.

3.1 Cyber Security Environment

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

- Views on the Importance of IT System & Data
- Type of Data Stored
- Cyber Attacks Experienced in the Past 12 Months
- Perceived Impact of Cyber Attacks
- Confidence in the Recovery of Key Services in 24 Hours

3.1.1. Views on the Importance of IT System & Data

The summarized view of respondents on the importance in business sectors is calculated from the average score obtained (on a 0 – 4 marks scale) based upon their perception of importance, with 0 representing “not that important” and 4 representing “extremely important”.

All respondents treated IT system and data as an important matter, with 97% of them rating “Important” or above, with a majority (59%) stating IT system and data as being extremely important.

	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)
All Business Categories	1%	2%	14%	25%	59%	**3.4**

The average score for all business categories is 3.4. In the view of business categories, “Financial Services” has the highest awareness with an average score of 3.7. “Manufacturing, Trading and Logistics” and “Public sector, Healthcare and Others” are relatively lower in awareness with an average score of 3.2 and 3.3 respectively.

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%	0%	9%	9%	83%	3.7
Retail and Tourism related	1%	0%	12%	31%	55%	3.4
Manufacturing, Trading and Logistics	1%	4%	20%	26%	50%	3.2
Information and Communication Technology	0%	3%	6%	17%	74%	3.6
Professional Services	0%	0%	15%	26%	59%	3.4
Public sector, Healthcare and Others	0%	6%	14%	23%	57%	3.3

It is also noted that Large Enterprises (3.7) in general regard IT system and data more important than SMEs (3.3).

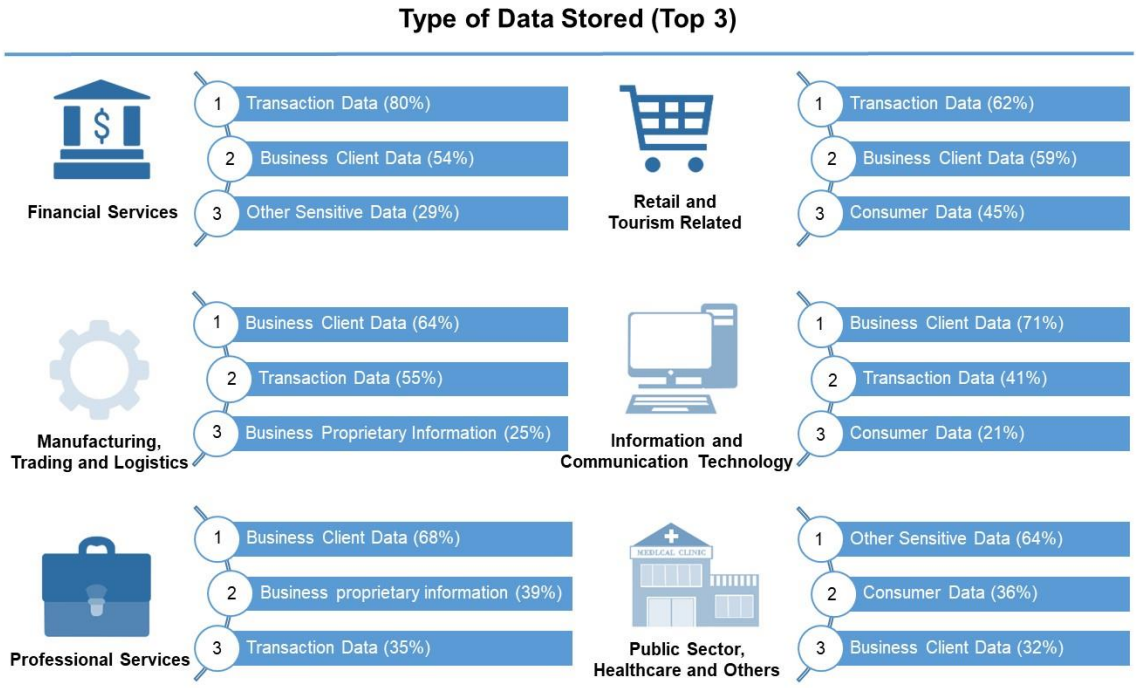
Company Size	Average score (0 – 4 marks)
SME	3.3
Large Enterprises	3.7

3.1.2. Type of Data Stored

Various types of data are involved in daily business to support operations. The types of data include:

- 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.)

In different business categories, the major types of data stored were different. A majority of “Financial Services” and “Retail and Tourism Related” stored “Transaction Data”. “Public Sector, Healthcare and Others” mainly stored “Other Sensitive Data”, like patient data/ membership data. The other three categories, namely “Manufacturing, Trading and Logistics”, “Information and Communication Technology” and “Professional Services” focused on “Business Client Data”.



3.1.3. Cyber Attacks Experienced in the Past 12 Months

3.1.3.1 External and Internal Attacks Experienced

We asked the respondents if they encountered external attacks, internal incidents, and incidents caused by external parties. External attack was the most common type (26%) while internal incidents (3%) and incidents caused by external partners (3%) were comparatively lower.

The respondents compared the occurrence of cyber security incidents in their company in the past 12 months with the previous year. The majority of the respondents considered they had a similar level of cyber attacks in the past 12 months as with the previous year. External attacks seemed to be more serious than the previous year, as 28% of respondents rated the occurrence of cyber attacks in the past 12 months as “More Serious” or “Far More Serious”.

	Encountered incidence	Occurrence of Cyber Security Incidents in past 12 months when compared with the previous year			
		Less Serious	Similar	More Serious	Far More Serious
External Attacks	26%	10%	61%	24%	4%
Internal Incidents	3%	18%	73%	9%	0%
Incidents caused by External Partners	3%	10%	90%	0%	0%

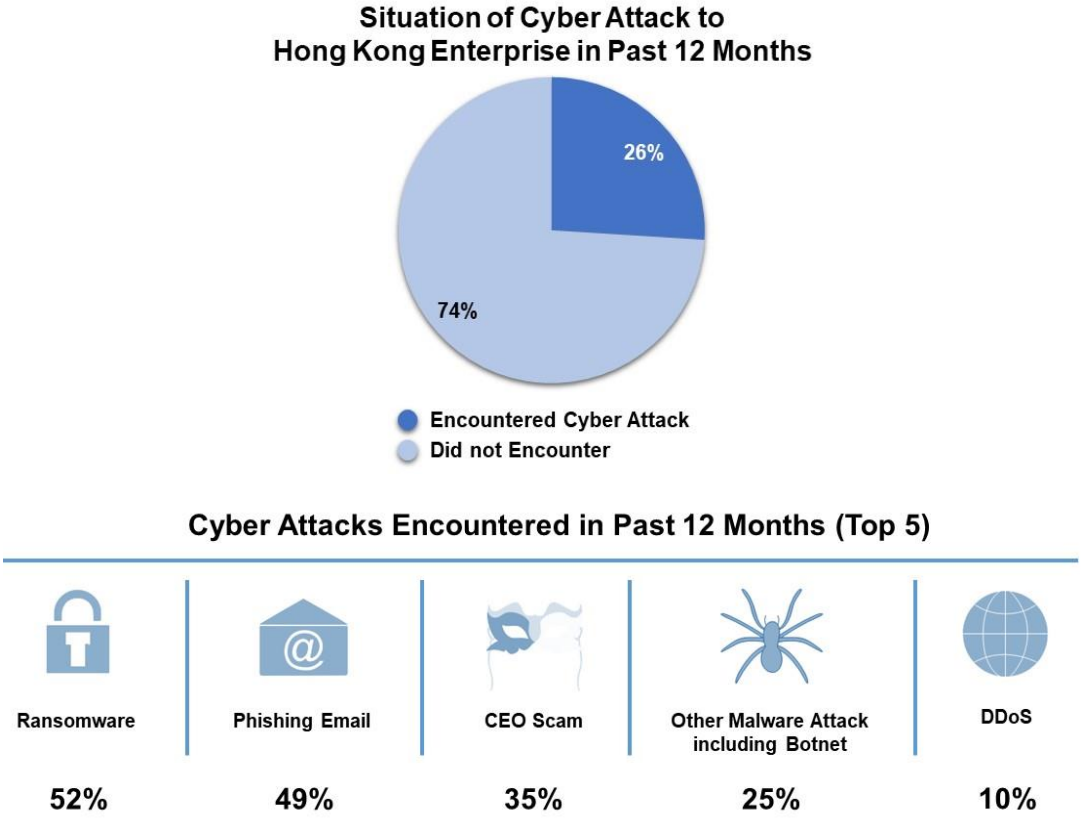
3.1.3.2 Form of Cyber Attacks Experienced

Around one-fourth of the respondents (26%) encountered cyber attacks in past 12 months. Cyber attacks can be classified by various criteria, including:

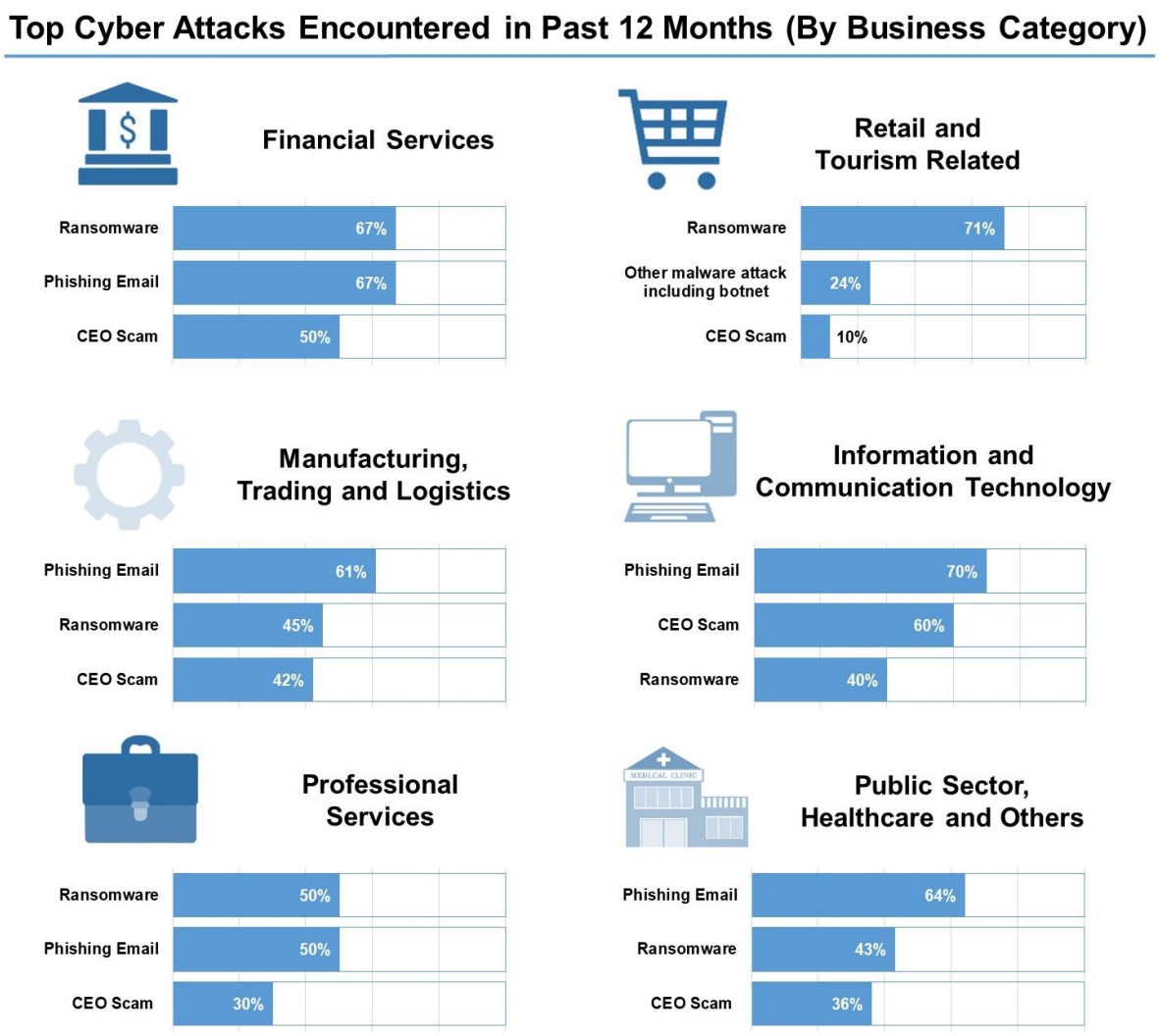
- Ransomware
- Other malware attack, including botnet
- Data/ credential leakage or theft
- Espionage
- CEO scam
- Phishing email
- DDoS (Distributed Denial of Service)
- Web server & app attacks

- Attack on other services like POS (Point of Sale) / remote access / CCTV (Closed-circuit television)
- Hacking targeting corporate service accounts
- Others

The most common form of attack encountered was “Ransomware” (52%), followed by “Phishing Email” (49%), “CEO scam” (35%), “Other malware attack” (25%) and “DDoS” (10%)



In terms of business category, “Ransomware” was more popular in “Financial Services”, “Retail and Tourism Related” and “Professional Services”, while “Phishing Email” was more popular in “Manufacturing, Trading and Logistics”, “Information and Communication Technology”, and “Public sector, Healthcare and Others”.



3.1.4 Perceived Impact of Cyber Attacks

The respondents also rated the impact of cyber security incidents in terms of severity (0: Very Low, 1: Low, 2: Medium, 3: High, and 4: Very High), using the following eight categories.

1. Service disruption
2. Breach of customer data
3. Damage to intellectual properties
4. Damage to data or system
5. Damage to reputation
6. Financial loss
7. Physical damage or human injury
8. Compliancy/ Legal responsibility associated

The composite impact score was then calculated by the average of the 8 aspects. The top three impact areas of each business sector are **bolded** for easier reference. In general, "Service Disruption", "Breach of customer data" and "Damage to data or system" were ranked high. In some specific industries, namely "Manufacturing, Trading and Logistics" and "Information and Communication Technology", the importance of reputation is emphasized, while in "Professional Services", concerns are mainly around financial losses.

	Perceived Impact of Cyber Attacks Average Rating (0-4)						
Sectors	**FS**	**RT**	**MTL**	**ICT**	**PS**	**PHO**	**All**
Service disruption	**3.29**	**3.01**	**2.98**	2.80	**3.16**	**3.19**	3.04
Breach of customer data	**3.24**	**2.94**	2.92	**3.20**	**3.21**	**3.19**	3.04
Damage to data or system	**3.14**	**2.87**	**3.05**	**3.20**	3.03	**3.06**	3.02
Damage to reputation	3.03	2.84	**3.01**	**3.17**	3.13	3.00	2.99
Financial loss	3.06	2.78	2.93	2.97	**3.24**	2.24	2.86
Compliancy/ Legal responsibility associated	3.03	2.43	2.77	2.86	2.73	2.80	2.70
Damage to intellectual properties	2.68	2.79	2.59	2.63	2.72	2.56	2.67
Physical damage or human injury	2.28	2.24	2.38	2.35	2.00	2.09	2.26
Impact Score (Average)	2.97	2.74	2.83	2.90	2.90	2.77	2.82

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

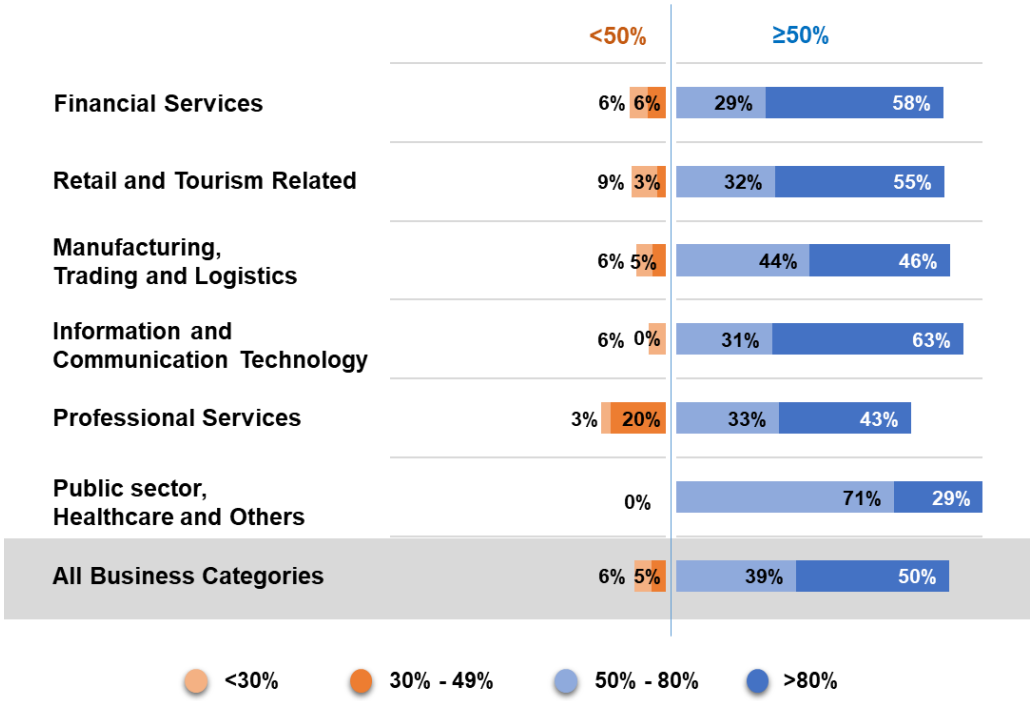
ICT: Information and Communication Technology **PS:** Professional Services **PHO:** Public sector, Healthcare and Others

All: All Business Categories

3.1.5 Confidence in the Recovery of Key Services in 24 Hours

The respondents were asked what percentage of key services they can recover in 24 hours when a security incident occurs.

Around 89% of the respondents felt confident that they could recover 50% or more of their key services within 24 hours. A large proportion of them (50%) believed they are able to recover over 80% of the services, especially in the business categories of "Information and Communication Technology" and "Financial Services". On the other hand, approximately 9% in "Retail and Tourism Related" felt they would be struggling to resume 30% of key services to their customers in 24 hours.


<50%
≥50%
Financial Services
6%
6%
29%
58%
Retail and Tourism Related
9%
3%
32%
55%
Manufacturing,
Trading and Logistics
6%
5%
44%
46%
Information and
Communication Technology
6%
0%
31%
63%
Professional Services
3%
20%
33%
43%
Public sector,
Healthcare and Others
0%
71%
29%
All Business Categories
6%
5%
39%
50%
<30%
30% - 49%
50% - 80%
>80%

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

3.2.1 SSH-HKECSRI definition

The index is calculated by assessing the maturity of current security measures adopted, in four aspects: security risk assessment, technology controls, process controls and human awareness. The index is in the range of 0 to 100. The higher the number, the more mature the security measures adopted.

Index (0 – 100)	Level	Description
0 – 20	Unaware	Management not aware of cyber security investment necessary for business strategy. This level is characterized by lack of security risk assessment to understand vulnerabilities and the impact on the organization, and lack of policies and controls to secure the business.
20.1 – 40	Ad-hoc	Organization starts to be conscious about cyber security investment. This level is characterized by inconsistent, reactive and ad-hoc measures in response to attacks. Some security controls are applied but not in a managed manner (planned, documented and duplicable process.)
40.1 – 60	Basic	Organization has built awareness to protect the business' investment against cyber attacks and ensure continuity. This level is characterized by the existence of some form of cyber security function, and the implementation of technology controls but without central management and fine-grain access control. Security awareness education is provided for limited staff only.
60.1 – 80	Managed	Organization is aware enough to manage in a planned and controlled manner. This level is characterized by the existence of an organized 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, mandatory and monitored access control. User awareness education programme is provided to all general staff.

> 80	Anticipated	Organization is aware of keeping abreast of emerging cyber security threats and compliance requirements. This level is characterized by the full support of the Board of Directors for the cyber security function, more proactiveness than the Managed level to achieve higher readiness, and use of benchmarking to measure success. A comprehensive security function is established within the organization and it is communicated externally frequently. Organization is aware of the global threat landscape and the security advancement outside the organization and keeps abreast of any risks related to business or technological changes.

3.2.2 Components of SSH-HKECSRI 2018

The SSH-HKECSRI measures the comprehensiveness of security measures in the following aspects:

1. Security Risk Assessment
2. Technology Controls
3. Process Controls
4. Human Awareness

Indicators are chosen for the four aspects. In 2018, the indicators are:

Four Aspects	**Indicators of each Aspect** Score (1 – 100)	**Sub-index Score for each Aspect**
Security Risk Assessment	- Security Risk Assessment	1 – 100
Technology controls	- Threat detection technology	1 – 100
Process controls	- 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**

For each indicator, the expected activities are mapped to levels 0 to 4 of comprehensiveness, with level 4 being the most comprehensive. Each level is assigned a score as follows:

Level 0: 0

Level 1: 25

Level 2: 50

Level 3: 75

Level 4: 100

For each indicator, the sub-index of each aspect is calculated by the average of scores of all the indicators of that aspect.

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. 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	
2. 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		
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

3.2.3 SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI) for 2018

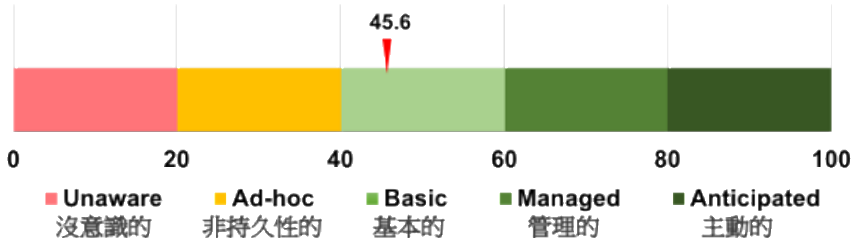
The index measures overall cyber security capability in terms of composite security measures.

Overall SSH-HKECSRI = Average of Sub-Indices

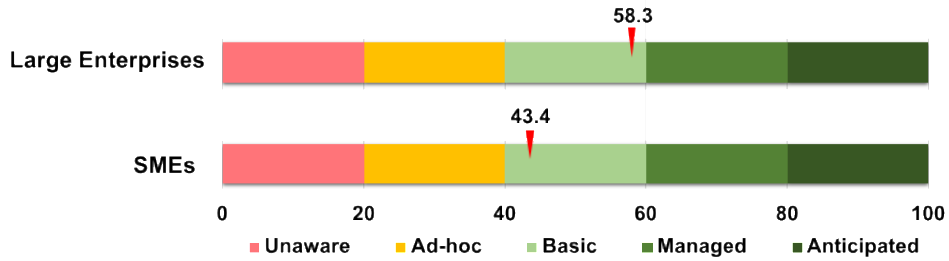
The overall sub-indices are reordered below. The SSH-HKECSRI was then calculated by the average of the 4 sub-indices assuming all indicators are of equal weight.

Indicators	Sub-index Score
Security Risk Assessment	49.4
Technology controls - Threat detection technology	36.9
Process controls - Data backup management (87.8) - Privileged access management (64.3) - Third party risk management (19.8)	57.3
Human awareness - Cyber security awareness education	38.8
SSH-HKECSRI = Average of sub-index scores	**45.6**

The **SSH Hong Kong Enterprise Cyber Security Readiness Index 2018** (SSH-HKECSRI 2018) is reported as **45.6** which is mapped to "**Basic**" **level**.



When considering the size of the company, Large Enterprises are in the upper "Basic" level at 58.3 while SMEs are in the lower "Basic" level at 43.4.



The scores for each indicator for different Business Categories are calculated in the following table in each cell. The bottom row shows the sub-index for each Business Category. The top two measures of each Business Category are highlighted in green color.

	Average Rating (0-100)						
Indicator	FS	RT	MTL	ICT	PS	PHO	All
1. Security Risk Assessment	64.8	50.5	40.3	60.3	58.8	39.0	49.4
2. Technology Controls - Cyber Threats Detection	52.8	26.8	39.3	37.3	46.3	34.8	36.9
3. Process Control	71.2	54.8	51.9	60.7	62.8	58.8	57.3
3.1 Privileged Access Management	73.5	65.0	58.0	66.3	68.5	65.5	64.1
3.2 Data Backup Management	97.8	86.5	85.3	89.3	92.5	84.0	87.8
3.3 Third Party Risk Management	42.3	13.0	12.3	26.5	27.3	27.0	19.9
4. Human Awareness - Cyber Security Awareness Education	53.3	33.3	36.5	48.5	30.3	49.3	38.8
Sub-index of business category	**60.5**	**41.3**	**41.9**	**51.6**	**49.5**	**45.5**	**45.6**

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

Security risk assessment and process control were the most popular measures adopted across business categories. It is worth noting that the indicators in Process Controls vary a lot. While data backup management and privileged access management had excellent adoption across business categories, third party risk management was not impressive.

Cyber threat detection has become more and more important in recent years but only the Financial service category has a score above 50 which means most companies are still using preventive measures rather than threat intelligence-based measures. The human is the last line of defense, and

cyber security awareness is the key success factor for security. Only the Financial service category has a score above 50. Most companies are comparatively putting fewer resources in this area.

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

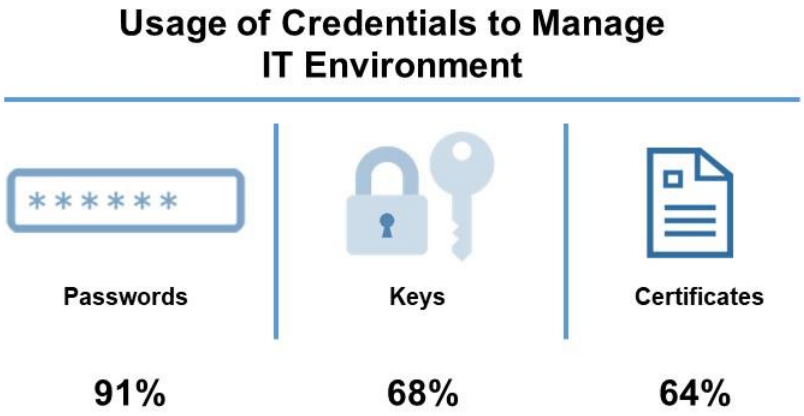
	Category Sub-index	
Financial Services	60.5	Managed
Information and Communication Technology	51.6	Basic
Professional Services	49.5	Basic
Public sector, Healthcare and Others	45.5	Basic
Manufacturing, Trading and Logistics	41.9	Basic
Retail and Tourism related	41.3	Basic

3.3 Special Topic - Credentials Management

In addition to the standard SSH-HKECSRI topics, the Survey also includes one special topic per year. For 2018, the special topic selected was “Credentials Management”.

3.3.1 Usage of Credentials

From the survey, the most commonly used were Passwords (91%), followed by Keys (68%) and Certificates (64%)



3.3.2 Management of Credentials

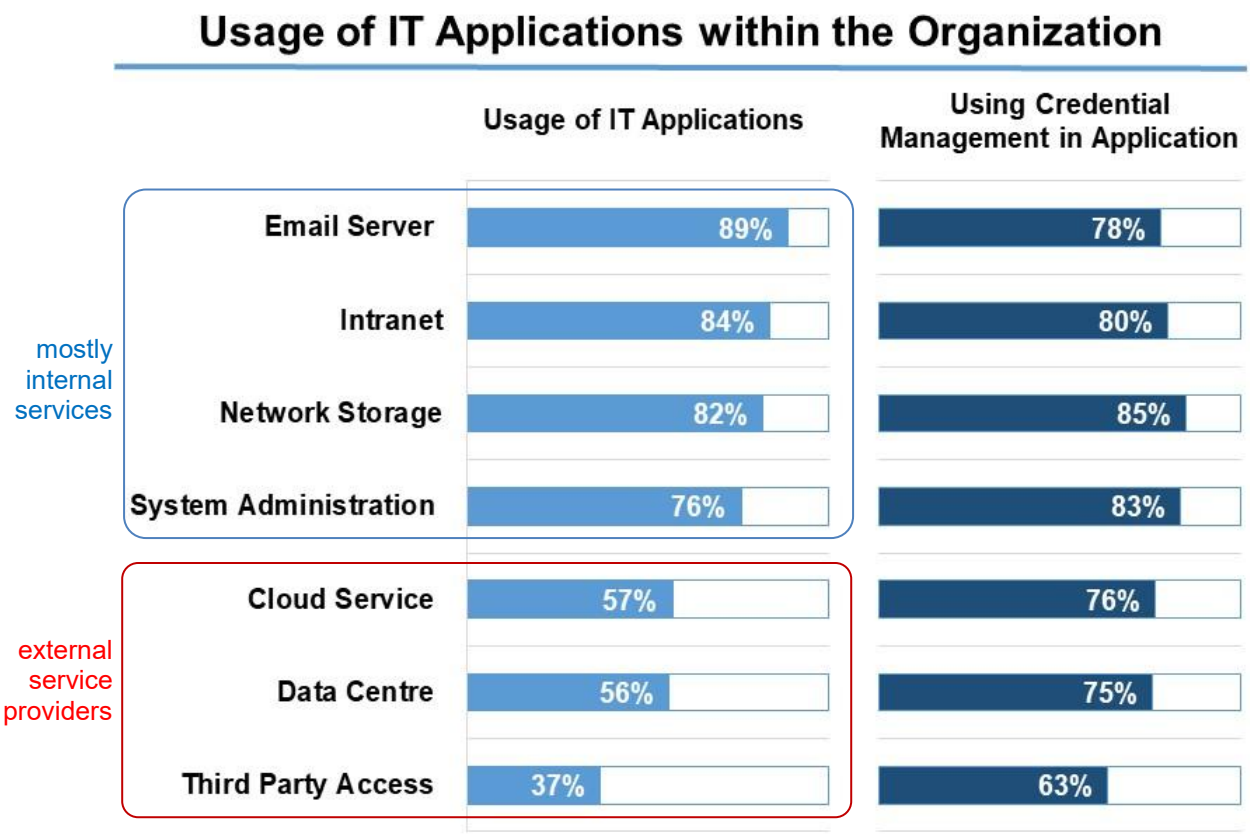
The top IT applications used were “Email Server” (89%), followed by “Intranet” (84%) and “Network Storage” (82%). Each of them had a usage of over 80%.

Usage of credentials management was the highest in “Network Storage” (85%) and “System Administration” (83%), while the corresponding numbers for “Email server” and “Intranet” were around 80%. These are mostly internal systems or services in the enterprises, although some enterprises are migrating email, intranet and network storage services to cloud-based platforms.

Over a half of the respondents were using external services, including cloud services (57%) and data centre services (56%). The adoption of credentials management was approximately 75%, slightly lower than that of internal services.

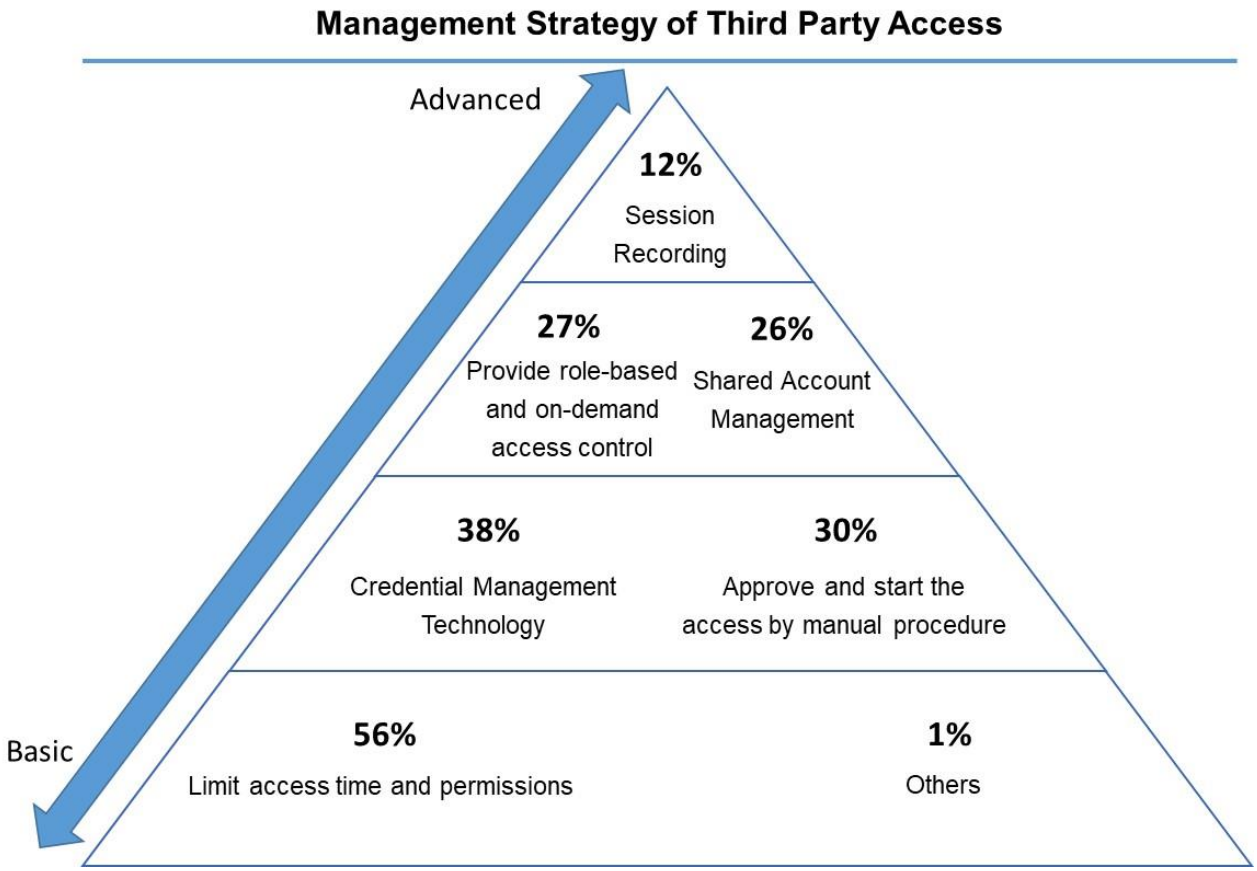
Approximately 37% of enterprises used “Third Party Access”, among which only 63% were “using

credentials management", the lowest in all IT applications.



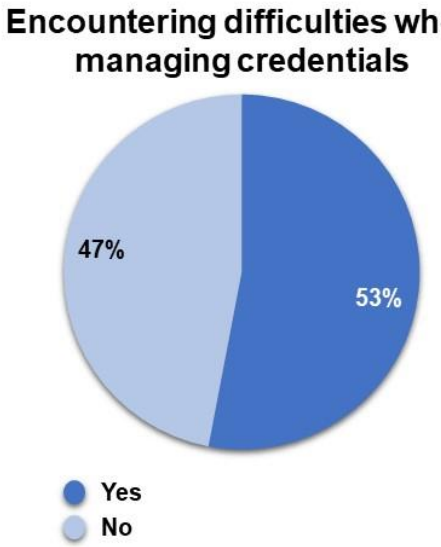
Credentials Management in Third Party Access

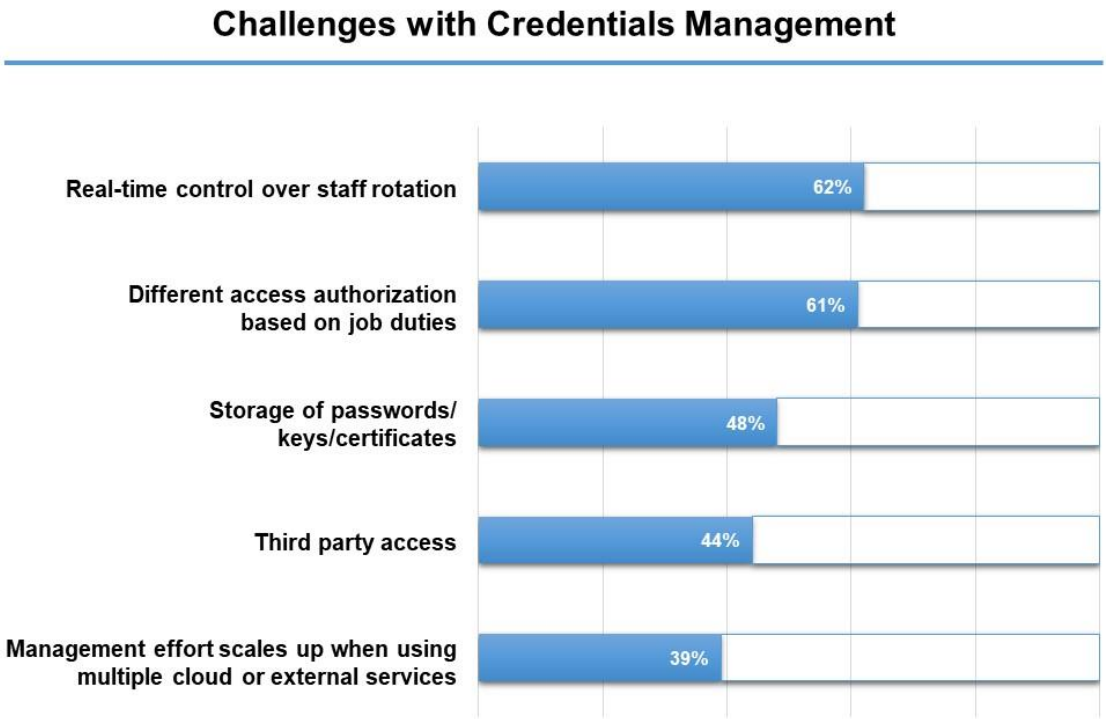
Those who had third party access with credentials management, answered a follow-up question on their management strategy. Most of the respondents were still using a basic solution – “Limit access time and permissions” (56%). Advanced solutions like “Provide role-based and on-demand access control” (27%), “Shared account management” (26%) and “Session recording” (12%) were not being widely adopted.



3.3.3 Difficulties with Credentials Management

Over half of the respondents (53%) encountered some type of difficulties when managing credentials. Among the difficulties encountered, “Real-time control over staff rotation” (62%) and “Different access levels based on job duties” (61%) were the areas with most challenges. **Therefore, responsive and detailed access control were major issues in credentials management**.





Other challenges involved “Storage of credentials” (48%) and “Third party access” (44%). Some respondents (39%) foresee that management effort scales up when using multiple cloud or external services.

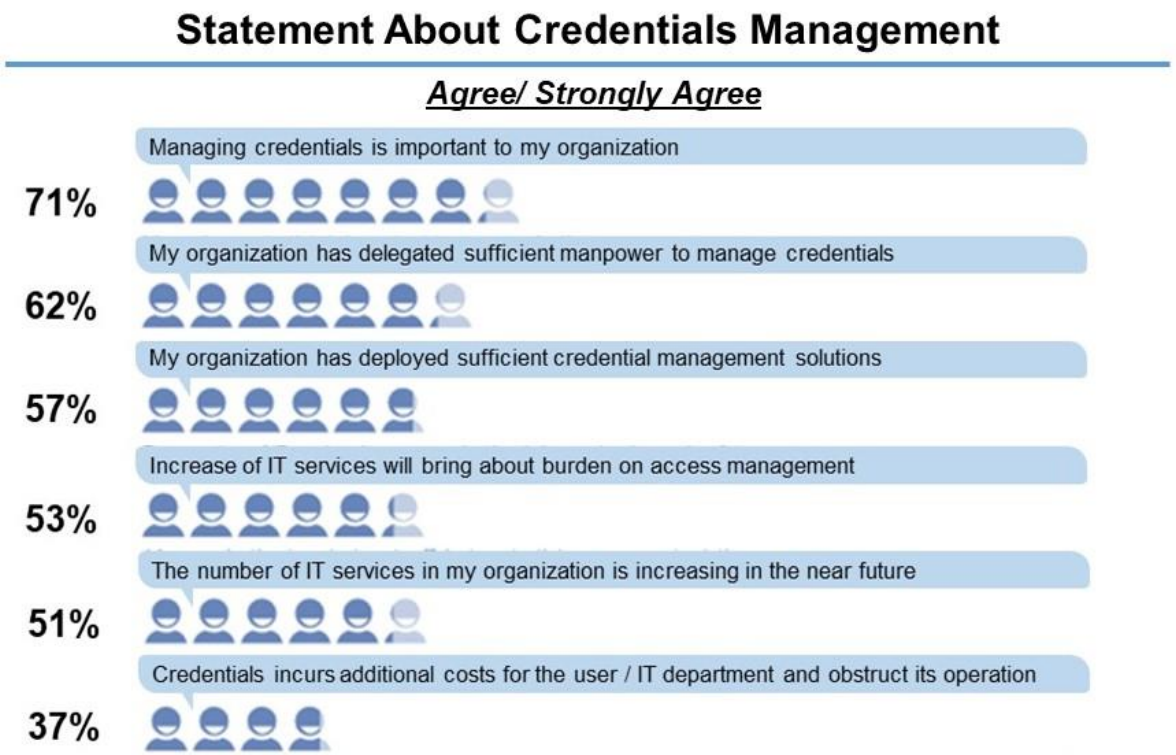
3.3.4 Views on Credentials Management

The views on credentials management were gauged. Most respondents were positive towards credentials management. Over 70% of respondents regarded managing credentials as important and 63% of them did not see that credentials management would incur additional costs or slow down

operations.

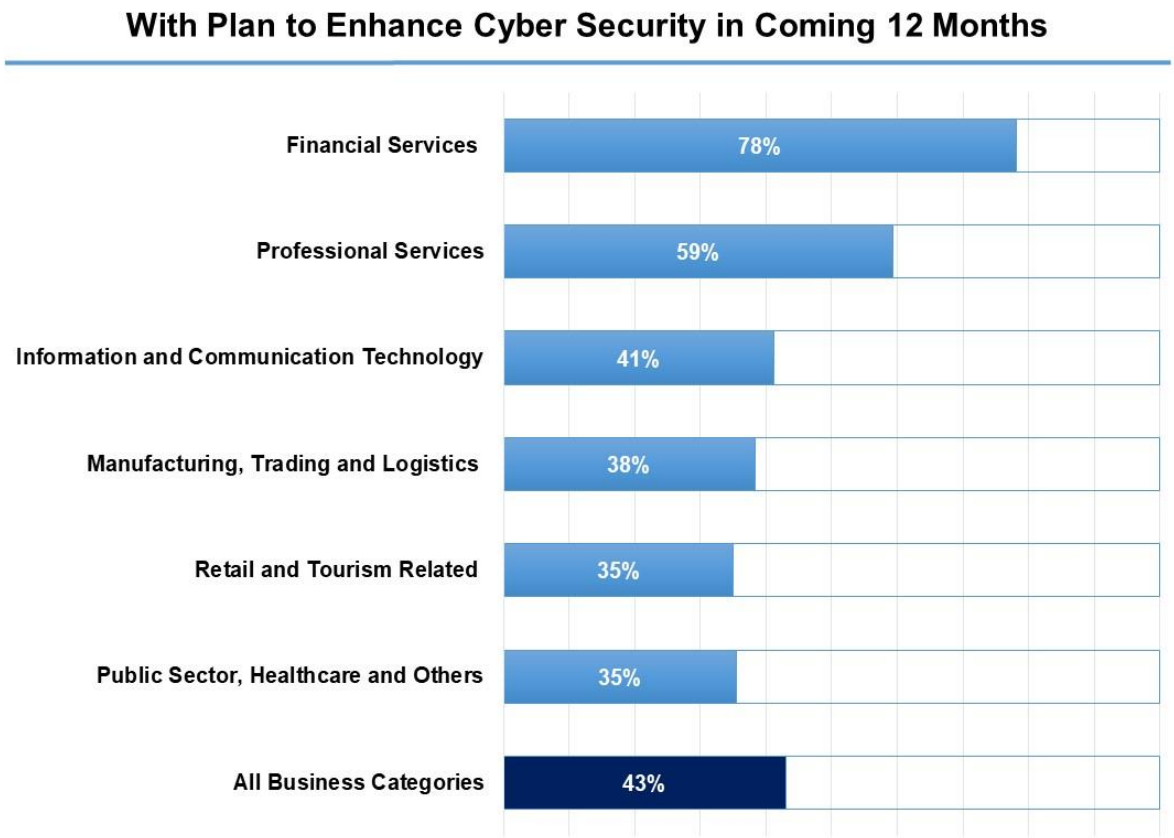
Over a half of the respondents deemed current investment in credentials management as sufficient in terms of manpower (63%) and credentials management solutions (57%). Yet, some of them saw there were areas to improve in terms of manpower (38%) and technology solution (43%) respectively.

Over half of the respondents foresaw that their companies would adopt more IT services in the near future (51%) and this increase would increase the time and effort needed for access management (53%).



3.4 Investment Plans for Cyber Security

Around 43% of the respondents were planning to enhance cyber security in the coming 12 months. In terms of business category, “Financial Services” (78%) was the most active category, while “Retail and Tourism Related” (35%) and “Public Sector, Healthcare and Others” (35%) were less active.



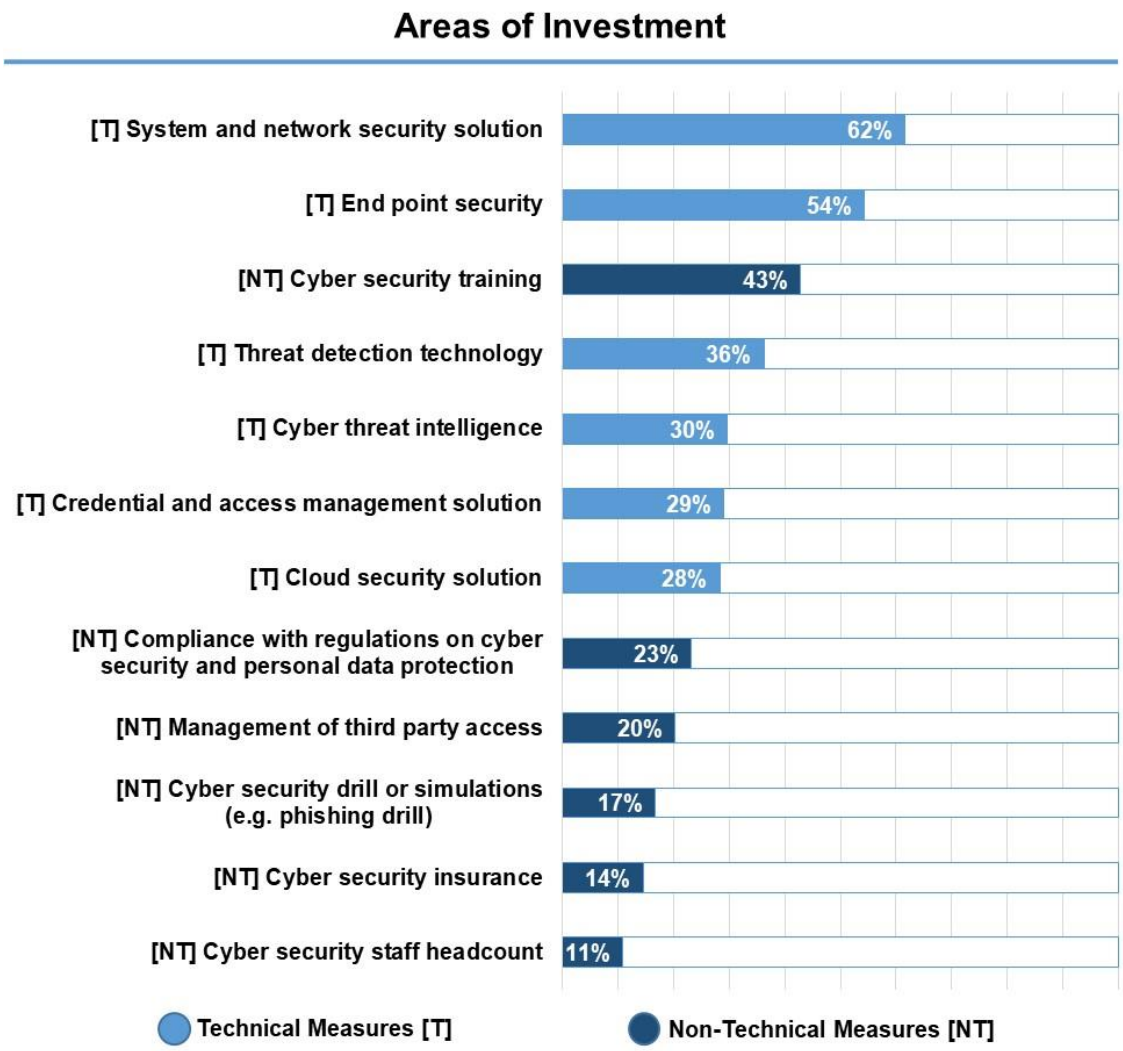
The investment area can be classified into Technical Measures and Non-Technical Measures, including:

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



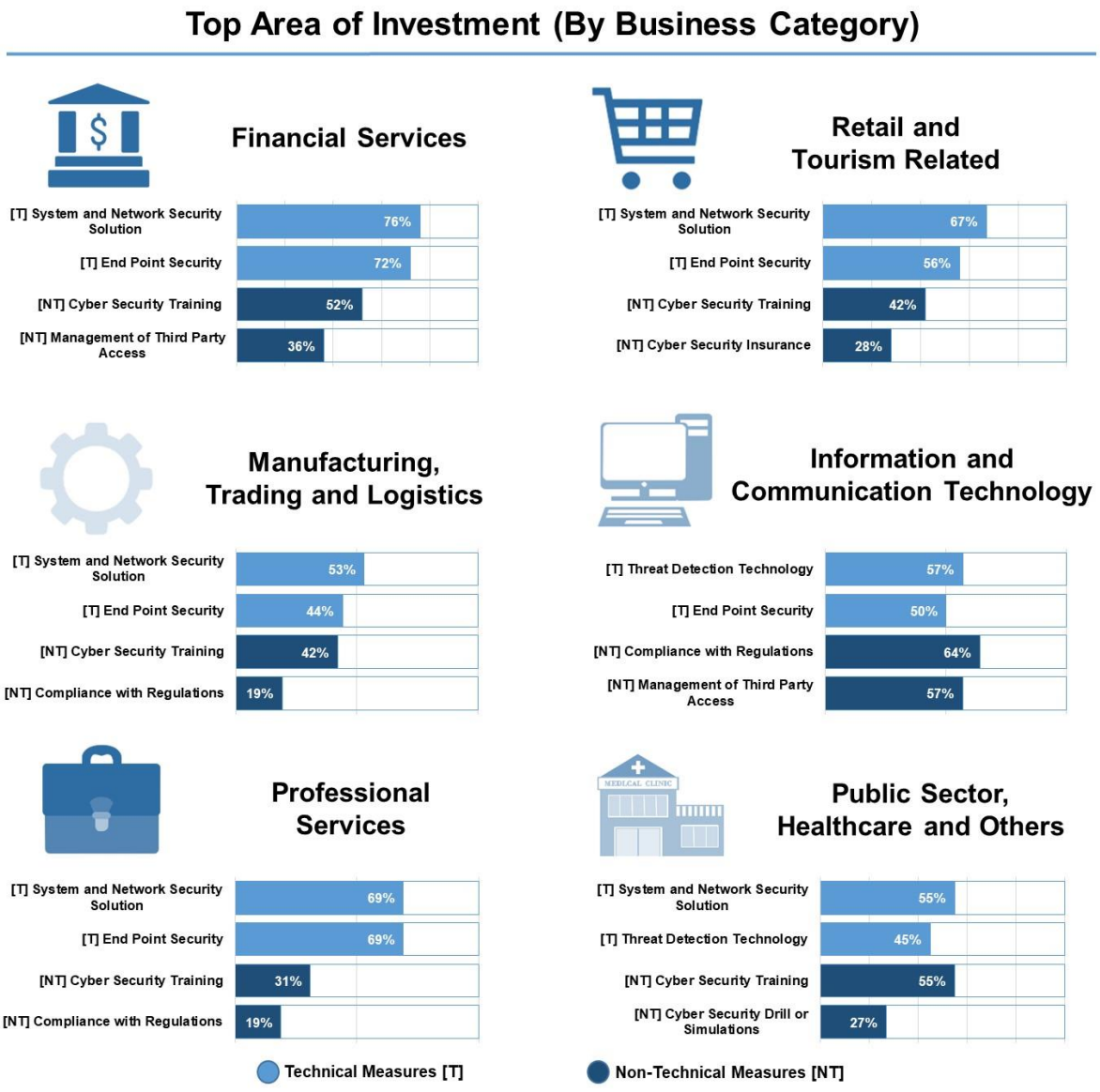
"System and network security solution" (62%) and "End point security" (54%) are the most popular investment areas. They are the common IT infrastructure of enterprises of any sector and any size.

It should be noted that "Cyber security training" (43%) came in the third place, and it is also the top non-technical measure for investment. Compared with the past 12 months, enterprises seemed to plan to invest more resources in cyber security awareness training in the coming 12 months, probably due to the prominence of cyber attacks, such as WannaCry ransomware in 2017.

Threat detection technology (43%) and cyber threat intelligence (36%) are newer popular technologies that have climbed up to the top 5. Closely following are another two new technologies: credentials management (29%) and cloud security (28%). These were expected to grow in popularity when more enterprises adopt cloud computing. GDPR comes into effect in 2018, so compliance with regulation (23%) was expected to rise further up in the coming years.

For non-technical measures, Cyber security insurance" (14%) and "Cyber security staff headcount" (11%) were the least popular. "Cyber security insurance" was still a fresh new concept to many enterprises in Hong Kong. It would be worthwhile to track its growth in future surveys. With growing cyber security threats, the job market for cyber security professionals was hot. However, enterprises might not put "Cyber security staff headcount" at a higher priority due to cost concern and difficulty in finding the right candidate to suit short-term need. Perhaps we would need to track the investment in managed security services for a more complete picture in future surveys.

For each business category, the top two areas of investment in technical measures and non-technical measures were presented as below:



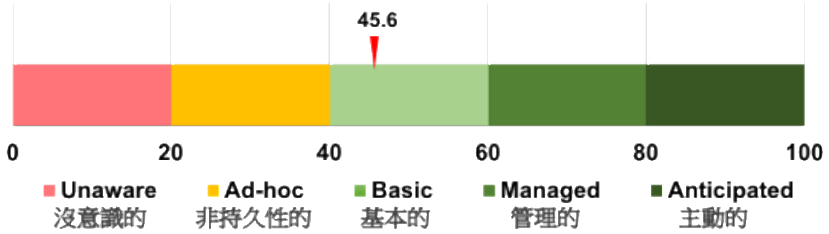
4 Conclusion & Recommendations

4.1 Key Findings

The Hong Kong Cyber Security Readiness Index

(1) The SSH Hong Kong Enterprise Cyber Security Readiness Index (SSH-HKECSRI) indicated that the overall level of security maturity among Hong Kong Enterprises is "Basic".

The SSH-HKECSRI in 2018 survey was 45.6 (equivalent to the "Basic" level) for all business categories.



The breakdown of results per business category is as follows:

(2) "Financial services" was the best performing business category, reaching the "Managed" level with a score of 60.5.

All other business categories were at the "Basic" level, in the range of 41 - 52.

.

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

In terms of company size, the Cyber Security Readiness Index for Large Enterprises alone was 58.3 ("Basic" level) and that of SMEs was 43.4 ("Basic" level). This means that larger enterprises generally adopted more comprehensive cyber security measures.

(4) The majority of enterprises scored high in "data backup management" which can help mitigate ransomware and extortion attacks that target data.

Indicators	Average score
1. Security Risk Assessment	49.5
2. Cyber Threats Detection	36.8
3.1 Data Backup Management	87.8
3.2 Privileged Access Management	64.3
3.3 Third Party Risk Management	19.8
4. Cyber Security Awareness Education	38.8

(5) "Privileged access management" is crucial in mitigating exposure to advanced persistent threats (APT) and to internal and partner incidents. It had the second best index at 64.3.

(6) "Third Party Risk Management" received the lowest score, which is an alarming result. Many cyber attacks attempt to exploit the weakest part of the supply chain (See HKCERT Guideline "Understanding and Tackling Supply Chain Attack".[2]) A further cause for concern is that this topic was also prioritized very low in terms of investment (position 9).

Cyber Security Environments

(7) Nearly all (97%) of the respondents regarded IT systems and data as highly important. The most common responses were: important (14%), very important (25%) and extremely important (59%).

(8) The perceived impact of cyber attacks was regarded as "High" (rating 4 out of 5) in all business categories.

(9) The top 3 forms of cyber attack in the past 12 months were ransomware (52%), phishing email (49%), CEO scam (35%).

In the past 12 months, 26% of respondents had encountered external attacks. Other types of attacks were insider incidents (3%) and incidents caused by external partners (3%).

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

Credentials Management

(10) Most respondents were positive towards credentials management. 70% rated it as important and 63% did not see it as incurring additional costs or slowing down operations.

(11) Adoption of credentials management in internal IT applications was high (over 80%) and that of external services was a bit lower (around 75%). Third party access ranked the lowest (63%).

(12) Over a half of the respondents regarded the current investment in manpower (62%) and technology solutions (57%) as sufficient.

(13)The majority of the respondents were using basic technology solutions in third party access management. Advanced solutions had a low adoption rate: session recording (12%), role-based and on-demand access control (27%).

(14) Over 60% of the respondents found the lack of responsive management and detailed control the biggest hurdles in credentials management.

Cyber Security Investment Plan

(15) 43% of respondents had a plan to enhance cyber security in the next 12 months. Business categories with a high Enterprise Cyber Security Readiness Index were willing to spend the most.

These were “Financial services” (78%), Professional services (58%) and ICT (41%).

(16) In terms of investment areas, technology solutions occupied four of the top five. “Cyber security awareness training” is the only non-technology solution (position 3).

The others in the top five were “System and network solution”, “End-point security”, “Threat detection technologies” and “Cyber threat intelligence”. The latter two are more recent technologies that have been adopted more in the last few years.

“Credentials management” and “Cloud security” followed closely in positions 6 and 7. They were expected to move further up in ranking as cloud adoption becomes more commonplace. The next one was “Compliance with regulation” which was expected to move higher in forthcoming years when GDPR is active.

4.2 Recommendations

(1) HKPC recommended enterprises put more effort into cyber security to move the maturity level up to the "Managed" or "Anticipated" level.

Enterprises should enhance their cyber security readiness to meet at least "Basic" Level. However they should target at the "Managed" and "Anticipated" level in the long run, especially for larger enterprises.

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

(2) Manage Third Party Risks

HKCERT named "Supply Chain Attack" as one of the five Potential Cyber Security Trends in the outlook for 2018[3]. Supply Chain Attack is where cyber criminals try to exploit the supply chain through third-party suppliers, as they usually have some level of access to their customer's network. Enterprises should pay more attention to risks posed by third parties. For example, a significant number of financial institutions are in co-operation with fintech partners whose security standards might be lower than those of the financial institutions. In the manufacturing and logistics sector, supply chain partners are connected via network interfaces to exchange production data and logistics data. Network interfaces and application programming interfaces are potential attack surfaces for attackers.

HKCERT published the Guideline "Understanding and Tackling Supply Chain Attacks" in April 2018 and detailed the nature of supply chain attacks and provided steps to tackle the risks:

- Include third party risks in security risk assessments, 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

Prevention strategy (e.g. firewall and antivirus) alone is no longer a sufficient form of defense. Enterprises should adopt the defense in depth approach and embrace detection strategies. Detecting threats occurring within the enterprise infrastructure and acquiring threat intelligence about developments outside the enterprise are both essential measures for ramping up the threat responsiveness of enterprises.

[3] HKPC Warns of More Financially-Motivated Cyber Attacks in 2018
https://www.hkcert.org/my_url/en/articles/18011801

Furthermore, sharing threat intelligence among peers in the same business sector can help cyber security resilience.

(4) Raise Cyber Security Awareness

People are the last line of defense and yet is often a neglected aspect of security. Some security incidents occurred because of human vulnerability, for example, a staff member accidentally opening an attachment that included ransomware, causing the data on the enterprise server to be encrypted and become inaccessible. Another example is a user being tricked to give out their WhatsApp authentication code and losing control of his WhatsApp account.

It is advised to increase cyber security awareness education as part of the enterprise security strategy as follows:

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

(5) Raise Awareness of Credentials Management

More awareness education and technical seminars should be provided on credentials 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 -

About HKPC

The Hong Kong Productivity Council (HKPC) is a multi-disciplinary organization established by statute in 1967. HKPC's mission is to promote productivity excellence through the provision of integrated support across the value chain of Hong Kong firms, to achieve a more effective utilization of resources, to enhance the value-added content of products and services, and to increase international competitiveness. HKPC conducts independent Study on cyber security and privacy to enable public and private organizations to have a better understanding on the trends in cyber threats and best practices to enhance their reputation and competitiveness in the global market.

For more information, please visit http://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 organizations 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 organizations 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
2018

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