香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Hong Kong Enterprise Cyber Security Readiness Index and Privacy Awareness Survey 2023

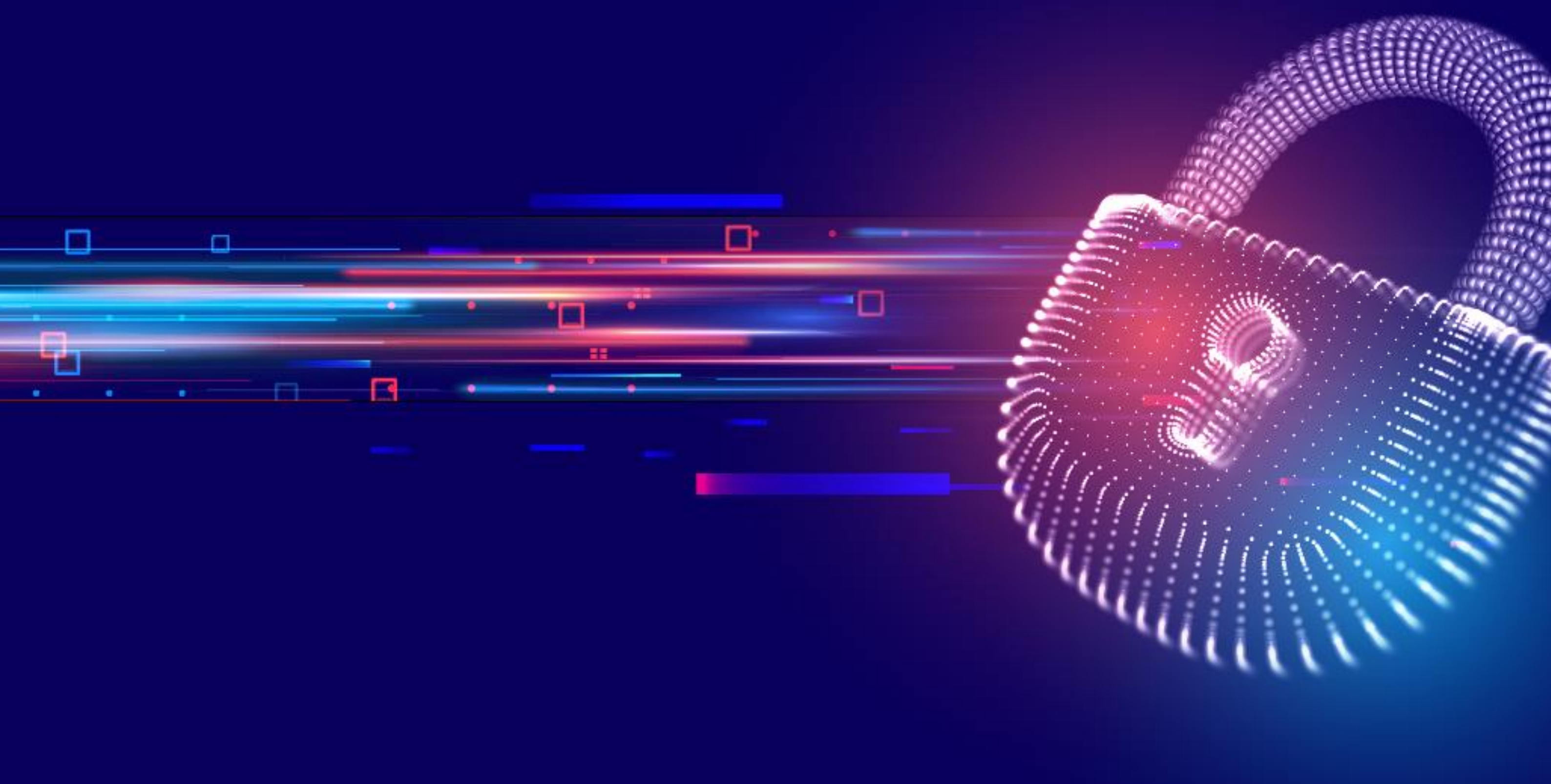


Table of Content

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 interconnected through the network of the "cyber world". However, like the real world, the cyber world is exposed to various security threats that can cause immense impacts and damages.

The HKSAR Government issued the first Smart City Blueprint for Hong Kong in December 2017, aiming to enhance the effectiveness of city management and improve people's quality of life as well as Hong Kong's attractiveness and sustainability by making use of innovation and technology. It involves the promotion of digital transformation across all industries and the daily lives of all citizens, more intensive network communications and the use of big data, providing opportunities for both general users and attackers. Hence, efforts must be made to regularly monitor the status of cyber security readiness and ensure it can keep up with technological change.

1.2 Hong Kong Enterprise Cyber Security Readiness Index and Privacy Awareness Survey

In view of the above background, the Hong Kong Productivity Council (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 (the Index), 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 in tackling cyber threats.

In 2023, Hong Kong Productivity Council Cyber Security (HKPC Cyber Security), commissioned by the Office of the Privacy Commissioner for Personal Data (PCPD), conducted the sixth round of the survey using this framework and the Privacy Awareness Survey as the thematic survey of 2023. The name of the survey – **Hong Kong Enterprise Cyber Security Readiness Index and Privacy Awareness Survey** – reflects this collaboration. The methodology of the survey, the design of the questionnaire and the execution of the interviews were decided and conducted by HKPC Cyber Security independently.

1.3 Thematic Survey of the Year: Privacy Awareness

As mentioned above, the special topic chosen for in-depth understanding in 2023 was privacy awareness among enterprises. Relevant questions of the thematic survey were designed by HKPC Cyber Security in consultation with PCPD.

Personal data is defined as information that relates to a living individual and from which it is practicable for the identity of the individual to be directly or indirectly ascertained. It must also exist in a form in which access to or processing of the data is practicable. Meanwhile, personal data privacy is the protection of personal data during the entire data life cycle, including collection, use, retention, and deletion.

Personal data privacy has become increasingly important nowadays. On the one hand, there is an expansion in the use of personal data for multi-various purposes, from making purchases to accessing credit reports to training artificial intelligence (AI) systems, etc. Enterprises are collecting and analysing more personal data for better understanding of their customers so as to provide more personalised services to their customers, and more parties in the same enterprise are involved in the usage and analysis of personal data. On the other hand, the advancement of technologies such as generative AI, blockchain, cloud computing, etc. and the surge of cyber security attacks increase the complexity of personal data privacy protection.

To foster a business environment where businesses value the importance of privacy and data protection and respect for individuals' privacy in this technological era, the survey seeks to assess the awareness and current practices of privacy and data protection among enterprises, their perceived level of difficulty in complying with data protection laws, and the challenges that they may encounter when putting privacy protection into practice.

1.4 Structure of Report

This report sets out our approach and methodology in conducting the Index survey, before providing the survey findings and presenting the results of data analysis.

After this introductory chapter, the rest of this report is structured as follows:

- Chapter 2 describes the methodology of the survey in details;
- Chapter 3 presents the findings of the survey; and
- Chapter 4 lays out the conclusions and recommendations based on the findings illustrated in Chapter 3.

2. Methodology

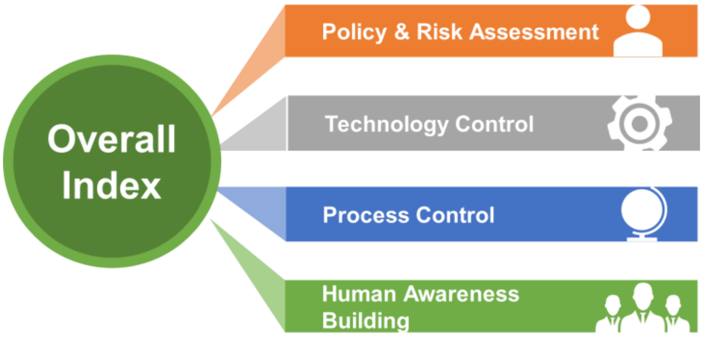
2.1 Framework of the Index

The Index is constructed by assessing the comprehensiveness of the security measures of the surveyed enterprises in four key areas: Policy and Risk Assessment, Technology Control, Process Control and Human Awareness Building. Questions in the four key areas are devised by information security professionals according to cyber security development. The options given to surveyed enterprises are classified into scores based on their level of comprehensiveness.

Components of the Index

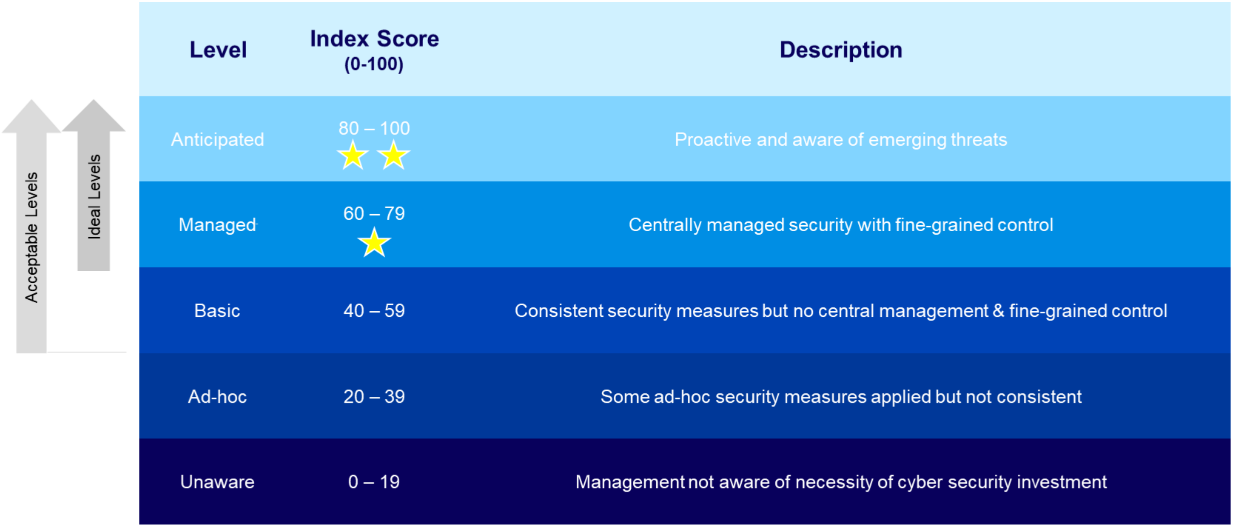
The Index is composed of sub-indices from four aspects:

- Policy & Risk Assessment
- Technology Control
- Process Control
- Human Awareness Building



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

The Index is calculated by assessing the comprehensiveness of current security measures adopted in four aspects: Policy and Risk Assessment, Technology Control, Process Control and Human Awareness Building. In the range of 0 to 100, the higher the Index, the better the resistance to and survivability of cyber security risks.


Acceptable Levels
Ideal Levels

Level	Index Score (0-100)	Description
Anticipated	80 – 100 ★★	Proactive and aware of emerging threats
Managed	60 – 79 ★	Centrally managed security with fine-grained control
Basic	40 – 59	Consistent security measures but no central management & fine-grained control
Ad-hoc	20 – 39	Some ad-hoc security measures applied but not consistent
Unaware	0 – 19	Management not aware of necessity of cyber security investment

Higher Readiness Index = Better Resistance and Survivability

2.2 Sample Distribution

Conducted in September 2023, the survey collected the data through telephone interviews with no less than 350 enterprises, with at least 50 of them being Corporates[1]. The sample was randomly selected from publicly available directories and the business registry database maintained by the Census and Statistics Department.

To ensure that the view of every targeted industry can be captured and represented in the survey while considering the actual proportion to the total number of establishments in Hong Kong, quota sampling was adopted to cover six key business 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 Communications Technology;
5. Professional Services; and
6. Non-governmental Organisation (NGOs), Schools and Others

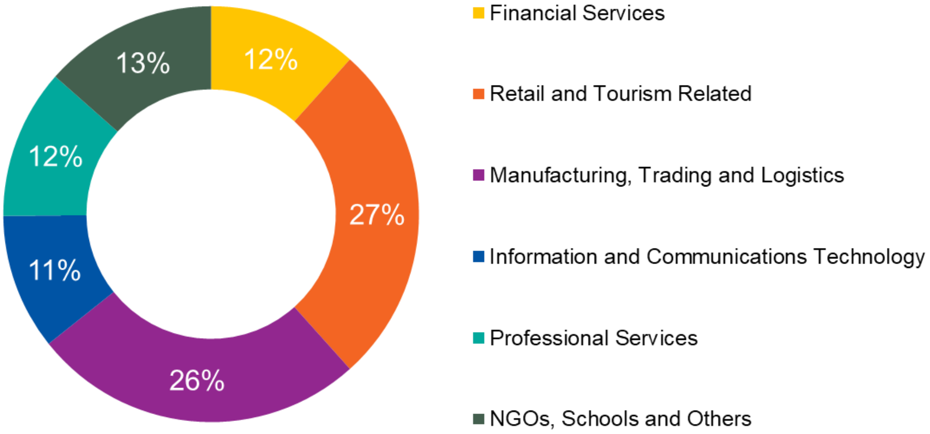
[1] Corporates refer to "Manufacturing establishments with 100 or more employees; or non-manufacturing establishments with 50 or more employees". https://www.success.tid.gov.hk/english/aboutus/sme/service_detail_6863.html

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 Communications Technology	Information and Communications Technology
5. Professional Services	Legal / Accounting / Auditing / Company Secretary / Consultancy, etc.
6. NGOs, Schools and Others	NGOs, Schools, Healthcare and Others

2.3 Profile of Surveyed Enterprises

The survey successfully gauged the views of management-level or IT-responsible officers from 378 enterprises in Hong Kong. As shown in the below figure, at least 11% of responses were collected for each business category, with 27% engaging in “Retail and Tourism related” businesses and 26% being “Manufacturing, Trading and Logistics” enterprises, considering the larger numbers of establishments in these categories.



Among these 378 surveyed enterprises, 309 of them were Small-and-Medium Enterprises (SMEs) and 69 of them were Corporates.

309
SMEs

69
Corporates

The breakdown of sample by business category and company size is summarised in the table below:

	SMEs		**Corporates**		**Total**	
	n	**%**	**n**	**%**	**n**	**%**
Financial Services	36	12%	8	12%	44	12%
Retail and Tourism related	86	28%	15	22%	101	27%
Manufacturing, Trading and Logistics	81	26%	17	25%	98	26%
Information and Communications Technology	35	11%	5	7%	40	11%
Professional Services	36	12%	8	12%	44	12%
NGO, Schools and Others	35	11%	16	23%	51	13%
All Business Categories	**309**	**100%**	**69**	**100%**	**378**	**100%**

3. Survey Findings

This chapter presents the key findings from the survey and is divided into four sub-sections. The topics covered are as follows:

1. Cyber Security Environment
2. The Index
3. Cyber Security Investment Plans and Challenges
4. Thematic Survey of the Year: Privacy Awareness

The survey successfully collected the opinions from 378 enterprises – 309 SMEs and 69 Corporates through telephone interview.

3.1 Cyber Security Environment

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

- Views on the Importance of Information Technology (IT) Systems & Data
- Level of Confidence towards the Cyber Security Level
- Types of Data Stored
- Cyber Security Attacks Experienced in the Past 12 Months

3.1.1 Views on the Importance of IT Systems & Data

The summarised view of surveyed enterprises on the importance of IT systems and data in business sectors is calculated based on the average score of their perceived importance (on a scale of 1 to 5), with 1 representing "not that important" and 5 representing "extremely important".

All Business Categories	Not that important (1 mark)	Somewhat important (2 marks)	Important (3 marks)	Very important (4 marks)	Extremely important (5 marks)	Average score (1 – 5 marks)
2023	3%	6%	19%	29%	42%	**4.0**
2022	4%	8%	22%	29%	36%	**3.9**
2021	1%	4%	20%	27%	48%	**4.1**

Overall speaking, surveyed enterprises continue to treat IT systems and data as a "very important" matter, with the average score for all business categories being 4.0.

Similar finding is also observed from the detailed breakdown of the results over the past 3 years. In 2023, 9 out of 10 surveyed enterprises (91%) consider IT systems and data "important" or above. It is also good to see that 42% consider IT systems and data "extremely important", though it is still 6 percentage points behind 2021.

By company size, Corporates consider IT systems and data more important than SMEs, with average scores of 4.6 and 3.9 respectively.

Company Size	Average score (1 – 5 marks)
SMEs	3.9
Corporates	4.6

Looking into the results by business categories, *Information and Communications Technology* enterprises continue to have the highest perceived importance of IT systems and data with an average score of 4.5, followed by enterprises in *Manufacturing, Trading and Logistics* (4.2), *Financial Services* (4.0) and *Retail and Tourism* (3.9). *NGOs, Schools and Others* and *Professional Services* enterprises have the lowest perceived importance score of 3.8, with only around one-third considering IT systems and data "extremely important".

Business Category	Not that important (1 mark)	Somewhat important (2 marks)	Important (3 marks)	Very important (4 marks)	Extremely important (5 marks)	Average score (1 – 5 marks)
Information and Communications Technology	3%	3%	10%	18%	68%	**4.5**
Manufacturing, Trading and Logistics	2%	3%	18%	35%	42%	**4.2**
Financial Services	2%	9%	18%	23%	48%	**4.0**
Retail and Tourism related	4%	8%	20%	30%	39%	**3.9**
NGOs, Schools and Others	4%	8%	24%	33%	31%	**3.8**
Professional Services	5%	7%	27%	30%	32%	**3.8**

3.1.2 Level of Confidence towards the Cyber Security Level

Surveyed enterprises were also asked to rate their level of confidence towards their current cyber security level on a scale of 1 to 5, with "1" being "totally unconfident" and "5" being "extremely confident". The results are summarised in the table below.

All Business Categories	Totally unconfident (1 mark)	Unconfident (2 marks)	Neutral (3 marks)	Confident (4 marks)	Extremely confident (5 marks)	Average score (1 – 5 marks)
2023	3%	5%	31%	46%	15%	**3.7**
2022	1%	3%	30%	48%	18%	**3.8**

In general, surveyed enterprises are less confident about their level of cyber security relative to last year, with an average score of 3.7 reported. In particular, the proportion of enterprises being "unconfident" or "totally unconfident" (8%) doubled compared with last year.

Consistently, Corporates (4.0) are more confident towards their cyber security level than SMEs (3.6).

Company Size	Average score (1 – 5 marks)
SMEs	3.6
Corporates	4.0

Similar as previous finding, *Information and Communications Technology* enterprises rank top with an average score of 4.1, with over 8 in 10 of them are "confident" and "extremely confident". This is followed by enterprises in *Financial Services* (3.9), *Manufacturing, Trading and Logistics* (3.7) and *Professional Services* (3.6), with 73%, 64% and 63% being "confident" or "extremely confident" in their cyber security level respectively. On the other hand, *NGOs, Schools and Others* and *Retail and Tourism* enterprises are less confident compared with other business categories, both with an average score of 3.5. In particular, 14% of enterprises in *Retail and Tourism* enterprises are "unconfident" or "totally unconfident" in their cyber security level, the highest among all business categories.

Business Category	Totally unconfident	Unconfident	Neutral	Confident	Extremely confident	Average score
	(1 mark)	(2 marks)	(3 marks)	(4 marks)	(5 marks)	(1 – 5 marks)
Information and Communications Technology	--	5%	13%	50%	33%	**4.1**
Financial Services	--	2%	25%	57%	16%	**3.9**
Manufacturing, Trading and Logistics	3%	3%	30%	52%	12%	**3.7**
Professional Services	--	7%	39%	54%	9%	**3.6**
NGOs, Schools and Others	6%	2%	35%	53%	4%	**3.5**
Retail and Tourism related	6%	8%	36%	32%	19%	**3.5**
Overall	**3%**	**5%**	**31%**	**46%**	**15%**	**3.7**

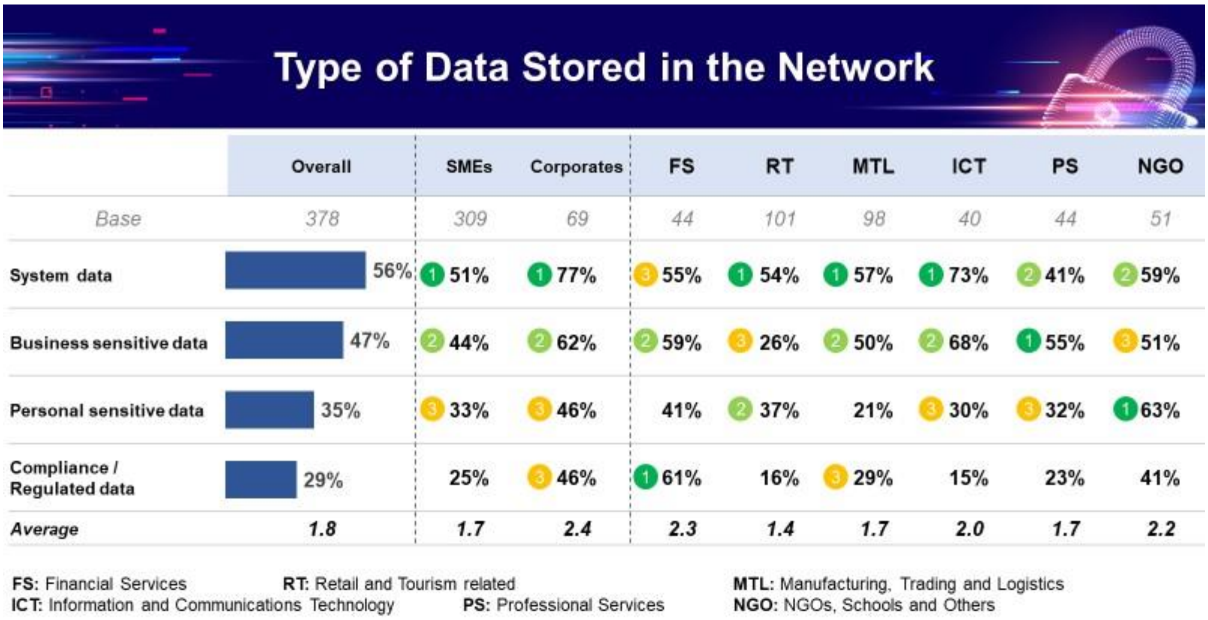
Note: "--" denotes 0%

3.1.3 Types of Data Stored

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

- Personal sensitive data (e.g. credit card number, contact details)
- Business sensitive data (e.g. contract details, credits, intellectual properties)
- System data (e.g. control data, system log, system configuration, access records)
- Compliance / Regulated data (e.g. General Data Protection Regulation, Personal Data (Privacy) Ordinance, Securities and Futures Ordinance)
- Other sensitive data (e.g. working documents, teaching materials)

Surveyed enterprises store 1.8 types of data on average, and Corporates store more types of data (2.4) than SMEs (1.7). It is also found that *Retail and Tourism* (1.4), *Professional Services* (1.7), and *Manufacturing, Trading and Logistics* (1.7) enterprises store less types of data compared with enterprises in other business categories.



Type of Data Stored in the Network

	Overall	SMEs	Corporates	FS	RT	MTL	ICT	PS	NGO
Base	*378*	*309*	*69*	*44*	*101*	*98*	*40*	*44*	*51*
System data	56%	① 51%	① 77%	③ 55%	① 54%	① 57%	① 73%	② 41%	② 59%
Business sensitive data	47%	② 44%	② 62%	② 59%	③ 26%	② 50%	② 68%	① 55%	③ 51%
Personal sensitive data	35%	③ 33%	③ 46%	41%	② 37%	21%	③ 30%	③ 32%	① 63%
Compliance / Regulated data	29%	25%	③ 46%	① 61%	16%	③ 29%	15%	23%	41%
Average	*1.8*	*1.7*	*2.4*	*2.3*	*1.4*	*1.7*	*2.0*	*1.7*	*2.2*

FS: Financial Services **RT:** Retail and Tourism related **MTL:** Manufacturing, Trading and Logistics
ICT: Information and Communications Technology **PS:** Professional Services **NGO:** NGOs, Schools and Others

In terms of the types of data stored, “System data” (56%) ranks top, followed by “Business sensitive data” (47%) and “Personal sensitive data” (35%). It is also found that significantly more Corporates (46%) store “Compliance / regulated data” than SMEs (25%).

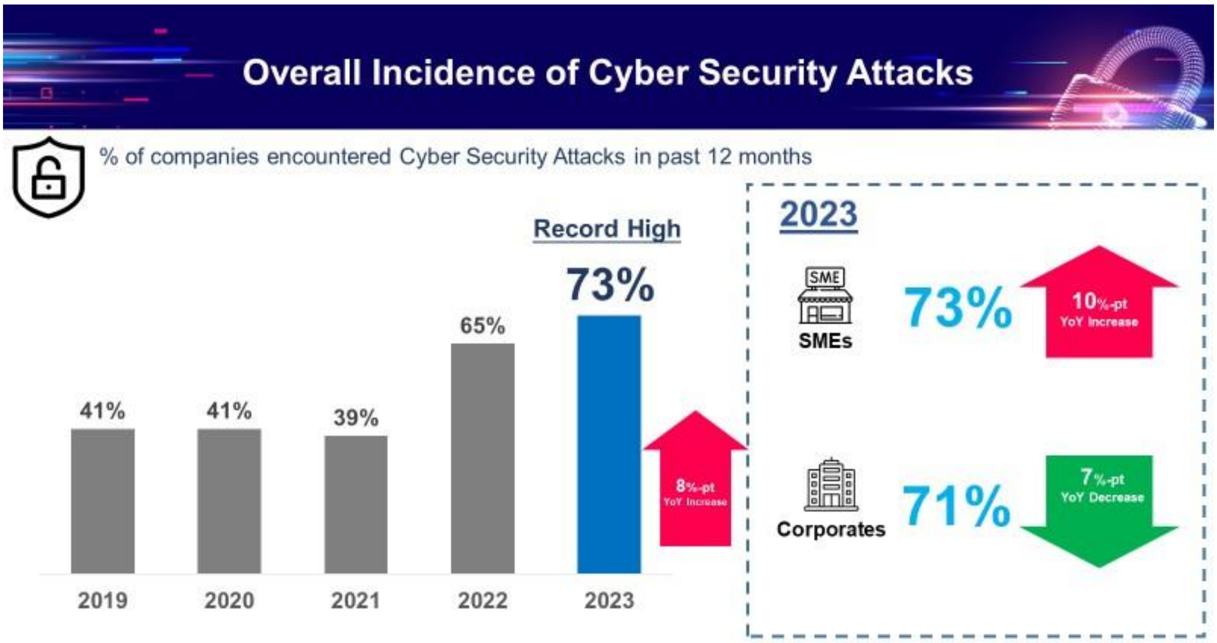
In different business categories, the types of data being stored slightly differ. In particular, “Compliance / Regulated data” is more commonly stored among *Financial Services* enterprises (61%), while more *NGOs, Schools and Others* (63%) and *Financial Services* enterprises (41%) store “Personal sensitive data”. On the other hand, less than half of the *Professional Services* enterprises (41%) keep “System data”, much lower compared with other business categories (ranging from 54% to 73%).

3.1.4 Cyber Security Attacks Experienced in the Past 12 Months

3.1.4.1 Incidence of Cyber Security Attacks in Past 12 Months

73% of the surveyed enterprises have experienced at least one type of cyber security attack in the past 12 months, regardless of whether such attacks caused financial losses to the enterprise(s) concerned or not. Compared with 2022, the incidence rate uplifted significantly by 8 percentage points to its record high.

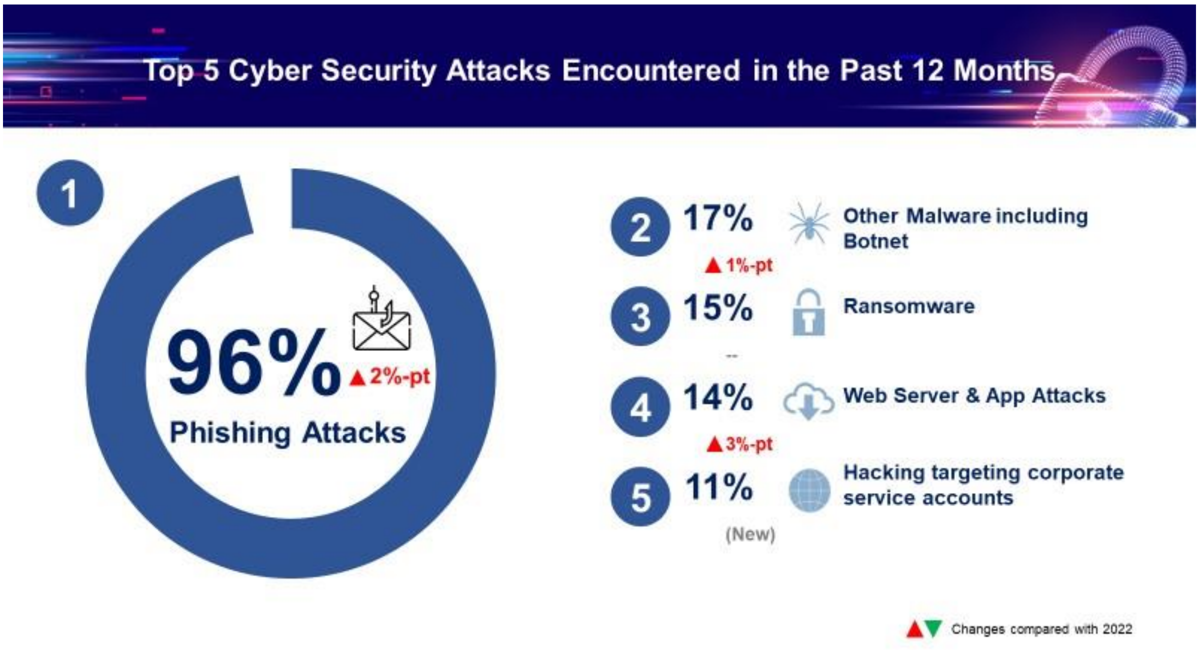
The increased incidence of cyber security attacks is mainly from SMEs (73%, +10 percentage points). On the other hand, such incidence is down by 7 percentage points among Corporates (71%).



Cyber security attacks can be caused by external attacks, internal attacks, or attacks caused by external partners (e.g. outsourced IT / business partners). The following types of cyber security attacks were covered in this year's survey:

- Ransomware
- Other malware attacks, including botnet
- Data / credential leakage or theft
- Phishing attacks:
  - Email phishing, including spear phishing
  - Vishing (Voice phishing)
  - Smishing (SMS phishing), including SMS and instant messaging apps such as WhatsApp, Telegram or Discord, etc.
  - Angler phishing, e.g. Facebook, Instagram or LinkedIn
  - Phishing using AI or Generative AI, e.g. Deepfake, speech synthesis or fake Chatbot
- Phishing attacks (continued):
  - Quishing, phishing using QR Code
  - Online advertisement counterfeiting other organisations
  - Other phishing attacks
- Web server and App attacks
- Attack on other services like POS (Point of Sale) / remote access / CCTV (Closed-circuit television) / Internet of Things (IoT)
- Hacking targeting corporate service accounts, e.g. email accounts, social media accounts, online banking accounts or other online service accounts
- Attacks targeting Web3.0, such as theft of crypto assets, attacking smart contract or enterprise blockchain
- Insider threat

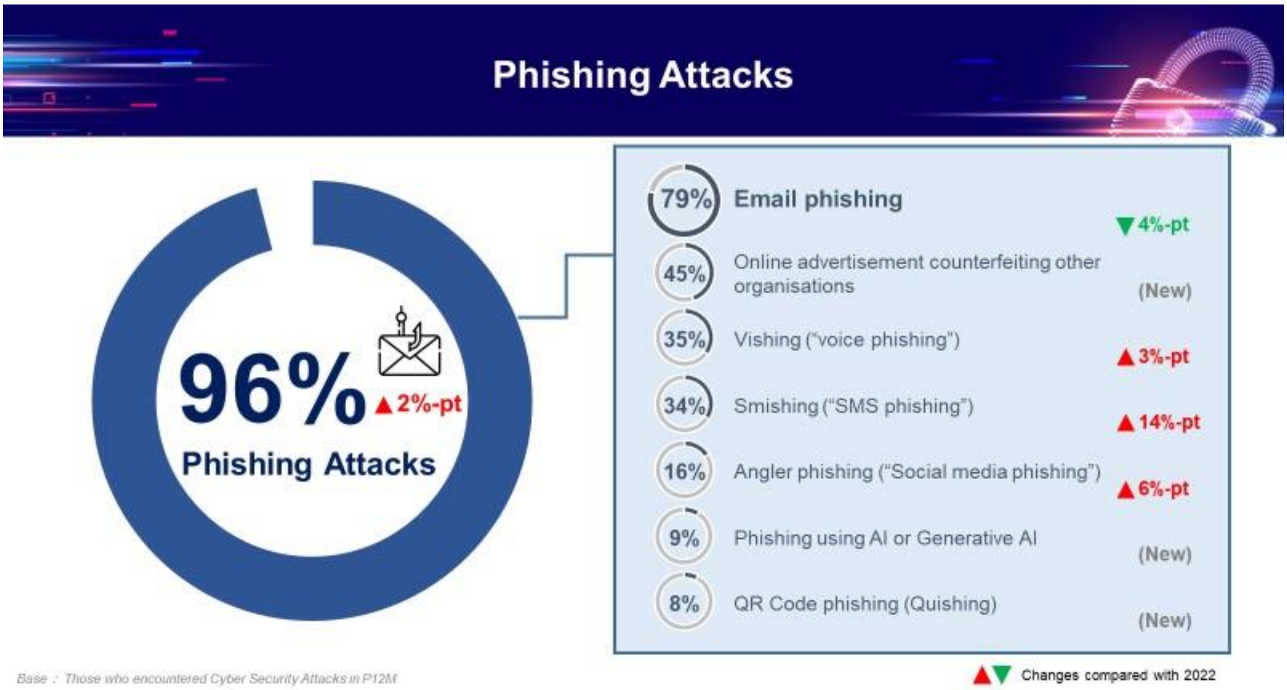
“Phishing attacks” continue to be the most common type of cyber security attacks encountered by the surveyed enterprises in the past 12 months, experienced by nearly all (96%) of the enterprises during the reference period. In addition to “phishing attacks”, other common forms of cyber security attacks are similar to last year’s, which include “other malware attacks including Botnet” (17%), “ransomware” (15%), “web server and app attacks” (14%) and “hacking targeting corporate service accounts” (11%).



Top 5 Cyber Security Attacks Encountered in the Past 12 Months

▲▼ Changes compared with 2022

Looking into the development of phishing attacks this year, “Email phishing” (79%) continues to be the most common type of phishing attacks, followed by “Online advertisement counterfeiting other organisations” (45%), “Vishing” (35%) and “Smishing” (34%) and “Angler phishing” (16%), where increased incidence is observed for the latter three types of phishing attacks. Meanwhile, emerging phishing attacks such as “Phishing using AI or Generative AI” (9%) and “Quishing (QR Code phishing)” (8%) are also reported by enterprises sustaining phishing attacks in the past 12 months.



Phishing Attacks

96% ▲2%-pt Phishing Attacks

79%	Email phishing	▼4%-pt
45%	Online advertisement counterfeiting other organisations	(New)
35%	Vishing (“voice phishing”)	▲3%-pt
34%	Smishing (“SMS phishing”)	▲14%-pt
16%	Angler phishing (“Social media phishing”)	▲6%-pt
9%	Phishing using AI or Generative AI	(New)
8%	QR Code phishing (Quishing)	(New)

Base : Those who encountered Cyber Security Attacks in P12M

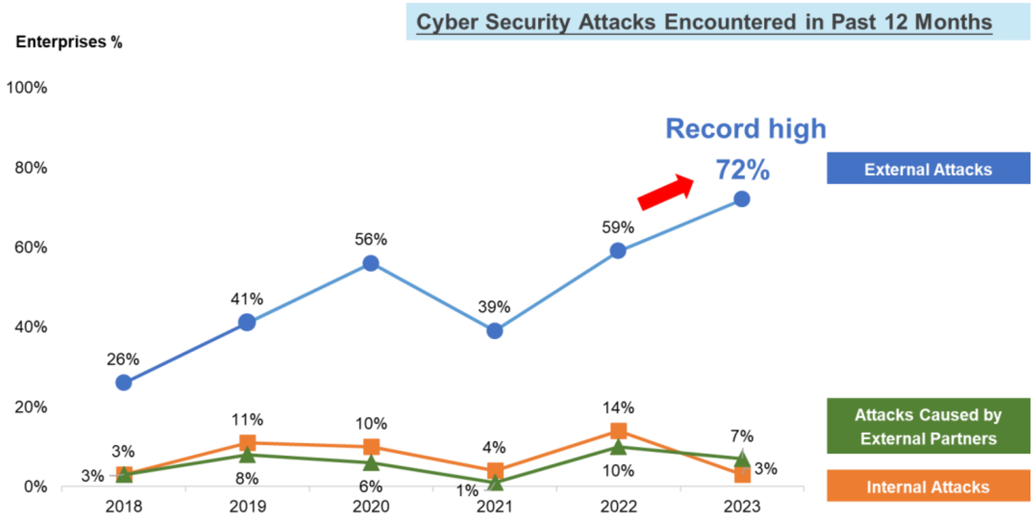
▲▼ Changes compared with 2022

3.1.4.2 External and Internal Attacks Experienced

Surveyed enterprises encountering any cyber security attacks over the past 12 months were also asked whether each of the cyber security attacks they have encountered were external attacks, internal attacks, and / or attacks caused by external parties.

External attack continues to be the most common type of cyber security attacks encountered by enterprises, with over seven out of ten surveyed enterprises had such encounter over the past 12 months. Compared with last year, such incidence surged by another 13 percentage points, reaching a record high of 72%.

Occurrence of internal attacks and attacks caused by external partners were significantly lower than external attacks, where 3% and 7% of the surveyed enterprises encountered each type of these cyber security attacks respectively. Although the incidence of internal attacks returns to its previous low level, occurrence of attacks caused by external partners remains relatively high when looking at the trend over the years.


Cyber Security Attacks Encountered in Past 12 Months

3.2 Hong Kong Enterprise Cyber Security Readiness Index (the Index)

3.2.1 Indicators of the Index

The Index measures the comprehensiveness of security measures in four aspects, each of which forms a sub-index:

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

Indicators chosen for the sub-indices in 2023 are listed in the table below:

Sub-index	**Indicators of each Sub-index** Score (0 – 100)	Sub-index Score
Policy & Risk Assessment	- Security Risk Assessment - Security Policy and Practice	0 – 100
Technology Control	- Cyber Threats Protection - Patch Management - Security Hardening	0 – 100
Process Control	- Data Backup Management - Privilege Access Management	0 – 100
Human Awareness Building	- Cyber Security Awareness Education	0 – 100
Overall Index	**Average of sub-indices**	**0 – 100**

For each indicator, the expected activities are mapped to Level 0 to Level 4 based on comprehensiveness in adoption, with level 4 being the most comprehensive. Each level has an assigned score as follows:

Level 0:	0
Level 1:	25
Level 2:	50
Level 3:	75
Level 4:	100

Each sub-index score is calculated by averaging the scores of all indicators inside; and the Level of each indicator is estimated based on the surveyed enterprise's claimed response to the respective questions on the adoption of various types of cyber security measures in the past 12 months. A summary of cyber security measures measured in the questionnaire is summarised in the table below:

Cyber 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 the following: * Review critical IT systems regularly * Invite external assessor to review IT systems	
1.2 Security Policy and Practice	None	Security policy / guideline document is in place	Staff needs to acknowledge it	+1 for each of the following: * Have a security policy / guideline to classify data according to sensitivity * Have a security / guideline on the responsibility of security attack response * Review or update on security policy / guideline	
2.1 Cyber Threats Protection	None		+1 for each of the following, max. 4 marks: * Application Firewall * IDS / IPS * Two-factor/Multi-factor Authentication * Cloud Security Technology * Backup and Recovery solution * Endpoint Detection & Response (EDR) * Has consolidated system event logs of multiple systems * Vulnerability scanning and fixing * Acquired threat intelligence * Network Access configuration * Security control monitoring solution * Penetration Test (PT) * Zero Trust Architecture (ZTA) * Passwordless authentication * Managed Security Service (MSS) * Data loss prevention (DLP) * Other relevant ones		
2.2 Patch Management	None	Occasionally when some people told to do	It is done regularly	+1 for each of the following: * Have a central patch management * Implement any automatic testing and patching system	
2.3 Security Hardening	None	Covering part of the systems only	All systems covered	+1 for each of the following: * Turn on logging / alert for errors for systems * Do regular scanning to detect system vulnerabilities	
3.1 Privileged Access Management	None	Yes	Also with privileged access management system deployed	+1 for each of the following: * Record accesses in log file * Review access log when needed (+2) Review access log regularly	

Cyber security measures adopted in the past 12 months					
Comprehensiveness Levels	**0**	**1**	**2**	**3**	**4**
Marks allocated (0 – 100)	**0**	**25**	**50**	**75**	**100**
3.2 Data Backup Management	None	Yes, but not regularly	Yes, regularly	+1 for each of the following: * Keep offline / offsite copy * Conduct recovery drill exercise * Use any cloud backup or automatic replication	
4. Cyber Security Awareness Education	None	Only for new-comers	Also for general staff	Cyber security drill exercise	C-level management openly involved

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

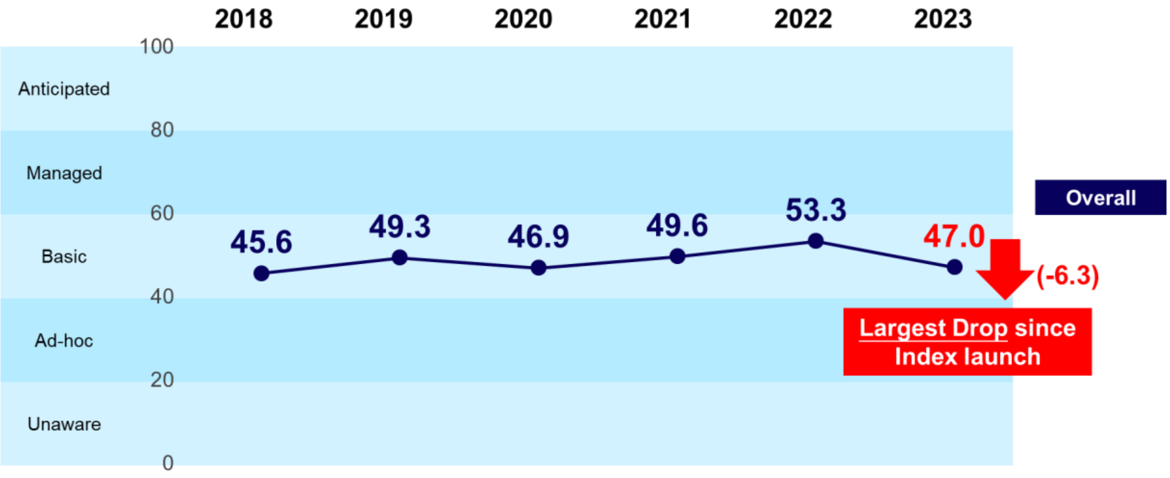
Overall Index = Average of Sub-Indices

An enterprise's level of cyber security readiness can be understood by its overall index score, and the following table details the description of each level:

Level	Index Score	Description
Unaware	0-19	Management not aware of necessity of cyber security investment
Ad-hoc	20-39	Some ad-hoc security measures applied but not consistent
Basic	40-59	Consistent security measures but no central management and fine-grained control
Managed	60-79	Centrally managed security with fine-grained control
Anticipated	80-100	Proactive and aware of emerging threats

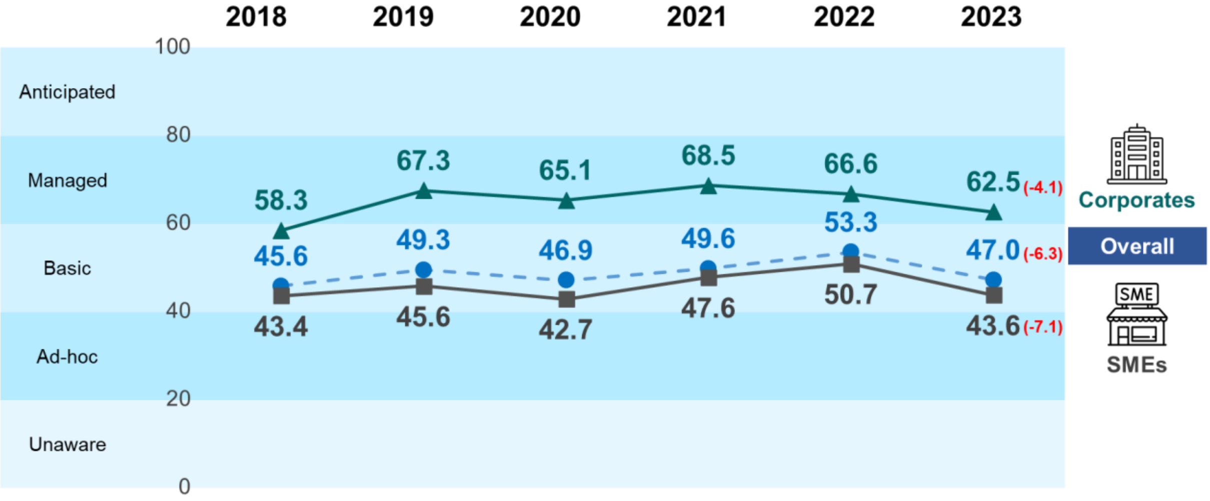
It is recommended that an enterprise should at least attain "Basic" level of cyber security readiness (40 points or above) for resistance and survivability in case of cyber security attacks.

3.2.2 Overall Index



The overall index drops by 6.3 points in 2023 to 47.0 points, the largest drop since the launch of the index in 2018.

The chart below shows the overall index development by company size:



Looking at the index development by company size, both SMEs (43.6 points) and Corporates (62.5 points) suffer a drop in index, with SMEs' index falling at a larger magnitude (-7.1 points). Although the index for Corporates weakens by another 4.1 points this year, it still sustains the "Managed" level of cyber security readiness.

Overall index development by different business categories is illustrated in the table below:

	2018 Index	2019 Index	2020 Index	2021 Index	2022 Index	2023		YoY Change
						Index	Level	
Financial Services	60.5	66.0	62.9	62.9	65.7	**64.9**	**Managed**	**-0.8**
Information and Communications Technology	51.6	55.8	50.2	52.2	61.1	**63.3**	**Managed**	**+2.2**
Manufacturing, Trading and Logistics	41.9	45.8	45.7	49.1	57.5	**48.6**	**Basic**	**-8.9**
NGOs, Schools and Others	45.5	51.8	51.9	52.3	47.1	**45.9**	**Basic**	**-1.2**
Professional Services	49.5	48.0	42.9	49.0	48.4	**43.5**	**Basic**	**-4.9**
Retail and Tourism related	41.3	44.0	40.9	42.0	45.8	**33.3**	**Ad-hoc**	**-12.5**
Overall (All Business Categories)	**45.6**	**49.3**	**46.9**	**49.6**	**53.3**	**47.0**	**Basic**	**-6.3**

Regarding the index development by business category, except *Information and Communications Technology* which further picks up by another 2.2 points, all business categories suffer declines at different magnitudes compared with 2022.

In particular, *Financial Services* (64.9 points) continues to be the business category with the highest index despite a mild decrease of 0.8 points, followed by *Information and Communications Technology* (63.3 points) which is the only business category with increase in index registered. Both sustain the "Managed" cyber security readiness level, meaning that the cyber security is centrally managed with fine-grained control.

Manufacturing, Trading and Logistics (48.6 points), *NGOs, Schools and Others* (45.9 points), and *Professional Services* (43.5 points) remain in the "Basic" cyber security readiness level. On the other hand, *Retail and Tourism* continues to be the business category with the lowest index among all business categories. This year, it suffers the largest drop of 12.5 points to 33.3 points and becomes categorised as "Ad hoc" level of cyber security readiness.

3.2.3 Sub-indices

The table below shows the development trend of the sub-indices.

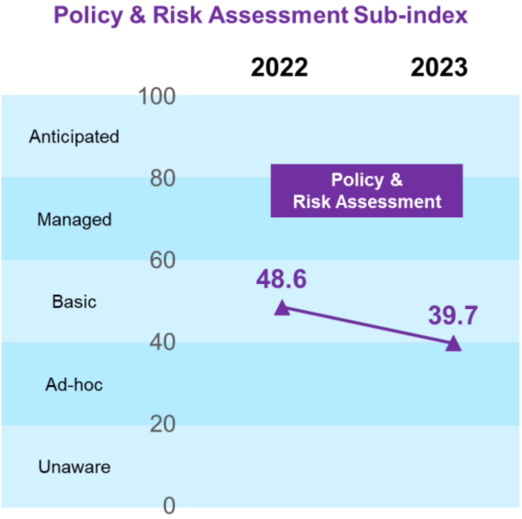
Component of Index	2018	2019	2020	2021	2022	2023	YoY Change
Policy & Risk Assessment	49.4	48.5	46.1	45.5	48.6	39.7	**-8.9**
Technology Control	36.9	55.7	60.1	66.7	66.3	55.1	**-11.2**
Process Control	57.3	63.4	54.3	58.7	73.1	68.1	**-5.0**
Human Awareness Building	38.8	29.5	26.9	27.6	25.1	25.2	**+0.1**
Overall = average of sub-index scores	**45.6**	**49.3**	**46.9**	**49.6**	**53.3**	**47.0**	**-6.3**

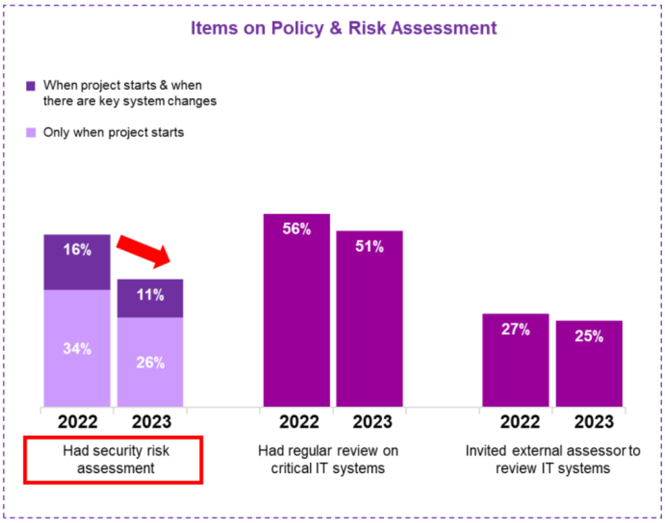
From the results, three out of four sub-indices namely “Technology Control” (-11.2 points), “Policy & Risk Assessment” (-8.9 points) and “Process Control” (-5.0 points) drop simultaneously, with the former two declining at a higher magnitude. It is also worth noting that this is the first time “Policy & Risk Assessment” (39.7 points) falls to “Ad-hoc” level.

In addition, “Human Awareness Building” continues to be an area which warrants enterprises’ attention, as this is the only sub-index which stays low at the lower “Ad hoc” level.

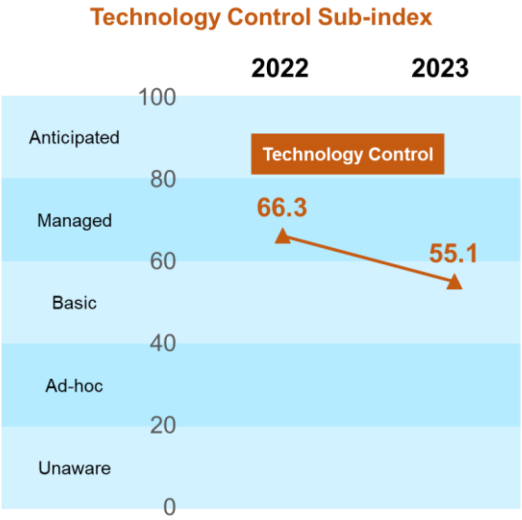
On the other hand, “Process Control” maintains at “Managed” level at 68.1 points.

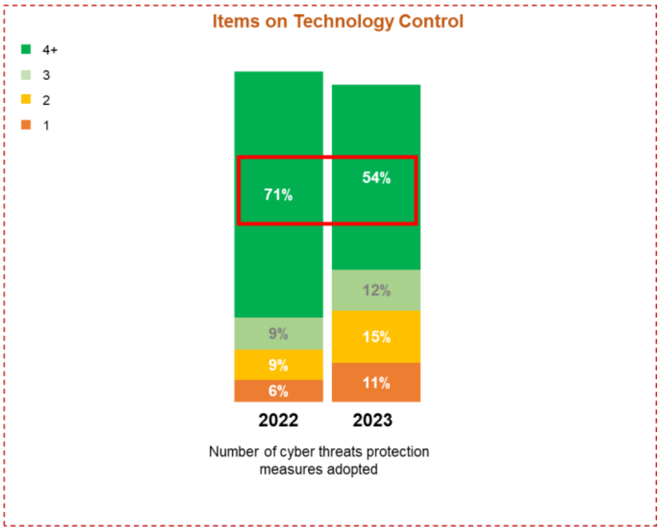
Looking into the development of the components within “Policy & Risk Assessment” sub-index, it is found that the adoption of all relevant measures weakens this year, particularly for “conducting security risk assessment in past 12 months”, with only 37% of surveyed enterprises claiming to have adopted such measure, a drop of 13 percentage points compared with past year. It is also found that only one in four (25%) enterprises invite external assessor to review their IT systems.



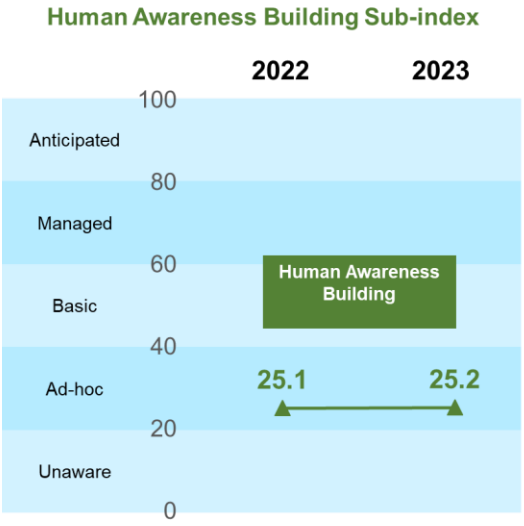


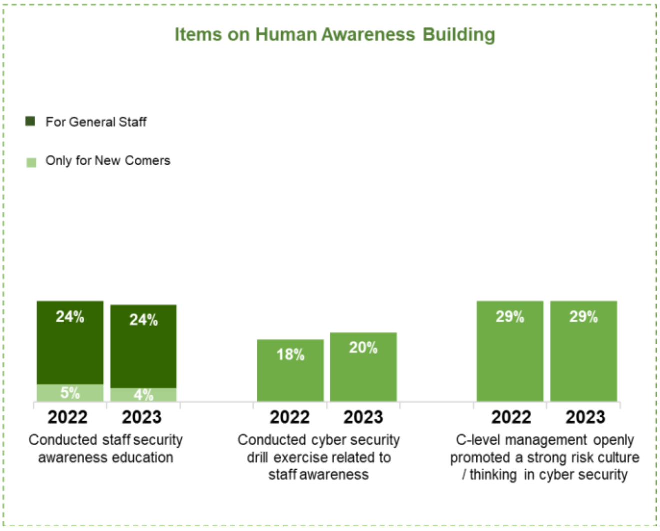
On the other hand, the drop in “Technology Control” sub-index is mainly due to fewer enterprises having patch management, as well as the reduced adoption of cyber threat protection measures, such as application firewall, IDS / IPS, two-factor / multi-factor authentication, etc. In particular, the proportion of enterprises utilising four or more measures drops drastically from 71% last year to 54% this year, while those adopting one to three measures / solutions surges by 14 percentage points.





On the other hand, the adoption of various measures under “Human Awareness Building” sub-index has no improvements compared with last year.





A summary of sub-index scores by company size can be found in the table. The bottom row of the table shows the sub-indices for SME and Corporates.

	Average Rating (0-100)		
Indicator	Corporates	SMEs	All
1. Policy & Risk Assessment	58.2	35.6	39.7
2. Technology Control	70.8	51.6	55.1
3. Process Control	79.9	65.5	68.1
4. Human Awareness Building	41.3	21.6	25.2
Sub-index of SMEs / Corporates	62.5	43.6	47.0

Overall speaking, Corporates have across the board higher sub-index scores than SMEs. However, their “Human Awareness Building” sub-index (41.3) is only slightly above “Ad hoc” level, indicating that there is no consistent measure in such area. For SMEs, on top of “Human Awareness Building” (21.6) which is approximating the “Unaware” level, “Policy & Risk Assessment” (35.6) should also be further enhanced – within which “Security risk assessment” is an area that SMEs can consider starting with.

The sub-index performance by business categories is summarised in the table below. Again, the bottom row of the table shows the sub-index for each business category.

Indicator	Average Rating (0-100)						All
	FS	RT	MTL	ICT	PS	NGO	
1. Policy & Risk Assessment	59.1	25.1	40.1	57.8	36.6	39.7	39.7
2. Technology Control	68.0	42.7	57.7	73.8	50.9	52.1	55.1
3. Process Control	83.2	52.8	74.1	79.1	64.2	68.4	68.1
4. Human Awareness Building	49.4	12.6	22.4	42.5	22.2	23.5	25.2
Sub-index of business category	64.9	33.3	48.6	63.3	43.5	45.9	47.0

FS: Financial Services **RT:** Retail and Tourism related **MTL:** Manufacturing, Trading and Logistics
ICT: Information and Communications Technology **PS:** Professional Services **NGO:** NGOs, Schools and Others
All: All Business Categories

In general, *Financial Services* and *Information and Communications Technology* enterprises have better sub-index performance across the board, while *Retail and Tourism related* enterprises consistently have the lowest scores across all sub-indices.

In terms of sub-index, "Process Control" and "Technology Control" are the two controls most adopted across business categories. Looking at "Process Control", all business categories have attained "Managed" level or above, except *Retail and Tourism* which stays at high "Basic" level with scores being deducted from "Patch management".

"Policy and Risk Assessment" is one area which can be further enhanced, especially for *Retail and Tourism* (25.1), *Professional Services* (36.6) and *NGOs, Schools and Others* (39.7) enterprises, where these three business categories could have better performance in "Security risk assessment". On top of the adoption of "Security risk assessment", *Retail and Tourism related* enterprises will also need to improve the adoption of "Security policy and practice".

Human is the last line of defence, and cyber security awareness is the key success factor for the line of human defence. "Human Awareness Building" sub-index, however, is low across different business categories except *Financial Services* (49.4) and *Information and Communications Technology* (42.5) enterprises which are at "Basic" level. In particular, *Retail and Tourism related* (12.6) enterprises are only at "Unaware" level, indicating the management is not aware of the necessity of such measures or cultivating the cyber security culture. All remaining business categories are only at the lower "Ad-hoc" level, ranging from 22.2 to 23.5.

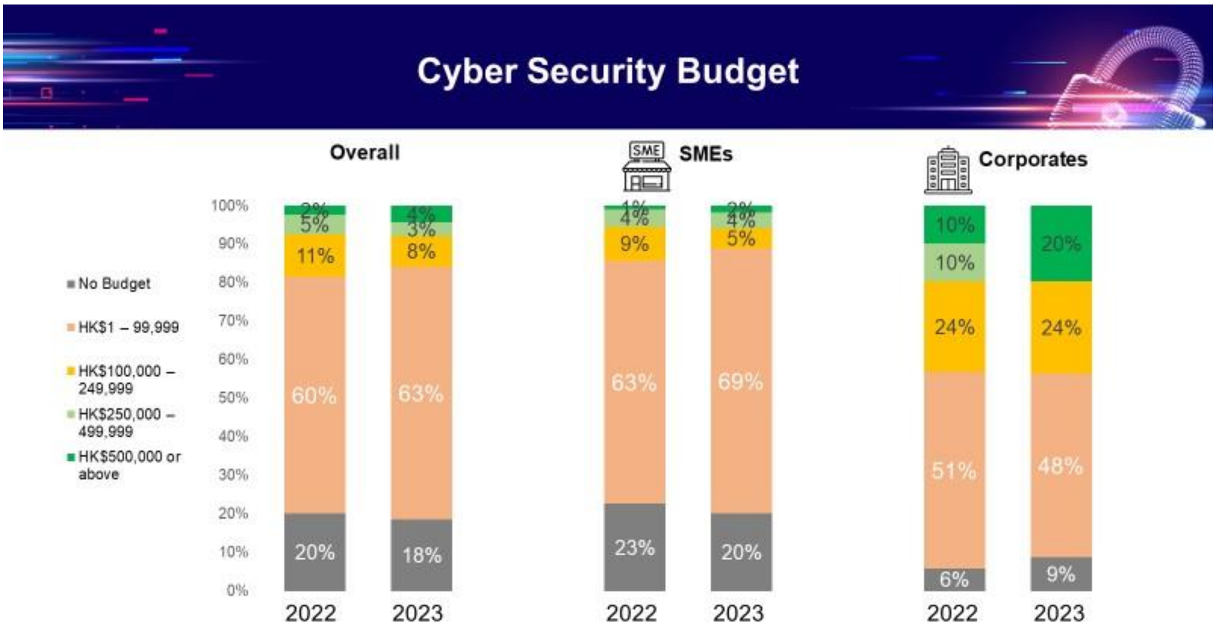
3.3 Cyber Security Investment Plans and Challenges

3.3.1 Cyber Security Budget

Compared with last year, surveyed enterprises are more willing to invest in cyber security, and the majority of them are spending less than HK$ 100,000 in the past 12 months.

Looking at the results by company size:

- More SMEs are spending HK$1 – 99,999 in the past 12 months (+6 percentage points) compared with last year, but the proportion of those invested HK$100,000 or above has slightly decreased.
- Although there is a slight increase in Corporates having no cyber security budget in the past 12 months, the proportion of Corporates spending HK$500,000 or above on cyber security in the past 12 months doubled this year.

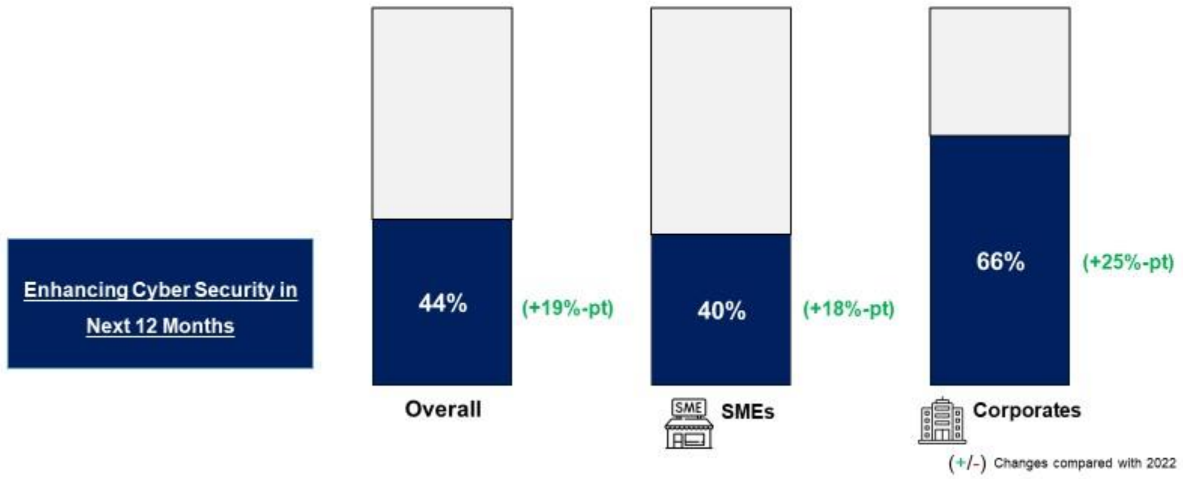


Cyber Security Budget

3.3.2 Enhancement Plans for Cyber Security

44% of surveyed enterprises have plans to enhance cyber security in the next 12 months, a surge of 19 percentage points compared with the results last year. While more SMEs (+18 percentage points) and Corporates (+25 percentage points) have plans to enhance their cyber security level, Corporates (66%) show higher eagerness in enhancing their cyber security level.

Plans to Enhance Cyber Security in Next 12 Months



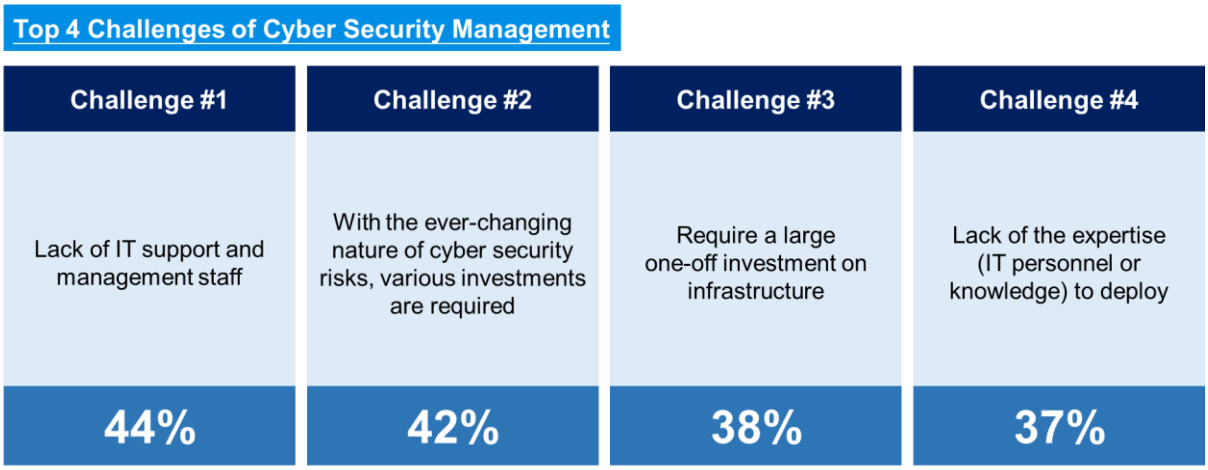
In terms of business categories, two in three enterprises in *Information and Communications Technology* have plans to enhance their cyber security level in the next 12 months, while enterprises in *Financial Services* (57%) and *NGOs, Schools and Others* (51%) are also more active compared with other business categories. Although *Retail and Tourism* is the business category with the lowest Index this year, only one in three of them have plans to enhance cyber security.

	FS	RT	MTL	ICT	PS	NGO	All
Planning to Enhance Cyber Security in Next 12 Months	57%	33%	38%	67%	44%	51%	44%
Not Enhancing Cyber Security in Next 12 Months	43%	67%	62%	33%	56%	49%	56%

FS: Financial Services **RT:** Retail and Tourism related **MTL:** Manufacturing, Trading and Logistics
ICT: Information and Communications Technology **PS:** Professional Services **NGO:** NGOs, Schools and Others
All: All Business Categories

3.3.3 Challenges of Cyber Security Management

The top four challenges of cyber security management remain the same over years, which are mainly related to personnel and investment. In particular, "lack of IT support and management staff" (44%) remains the top challenge facing enterprises, followed closely by "various investments are required due to the ever-changing nature of cyber security" (42%), "large one-off investment on infrastructure required" (38%) and "lack of expertise (IT personnel or knowledge) to deploy" (37%).



Top 4 Challenges of Cyber Security Management

Challenge #1	Challenge #2	Challenge #3	Challenge #4
Lack of IT support and management staff	With the ever-changing nature of cyber security risks, various investments are required	Require a large one-off investment on infrastructure	Lack of the expertise (IT personnel or knowledge) to deploy
44%	42%	38%	37%

3.4 Thematic Survey of the Year: Privacy Awareness

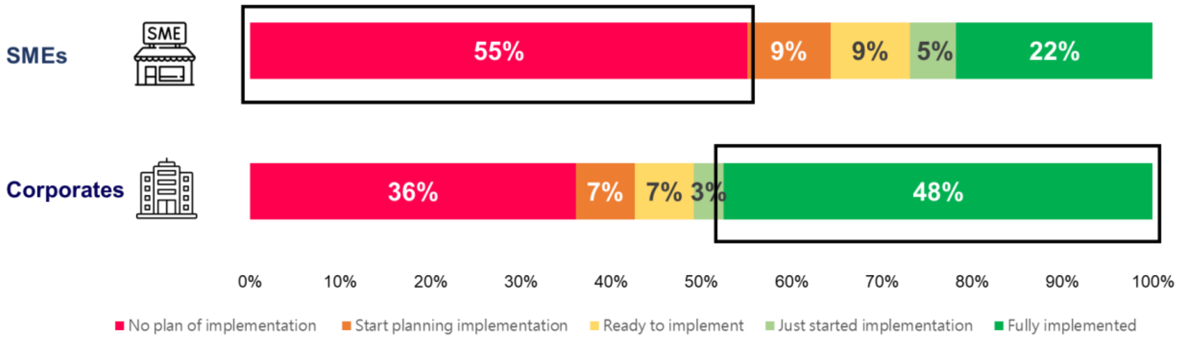
The thematic survey in this year looks into enterprises' awareness of privacy, which covers their current practices in data protection measures, their awareness of privacy risks involved in the use of emerging technologies and whether they have internal guidelines in response to these risks, their perception towards the difficulty in complying with the Personal Data (Privacy) Ordinance (PDPO), as well as their perception towards the level of privacy protection in Hong Kong. The thematic survey also gauged enterprises' awareness of the work of the Office of the Privacy Commissioner for Personal Data (PCPD) and their level of support towards various proposed amendments to the PDPO.

3.4.1 Current Practices in Data Protection Measures

3.4.1.1 Level of Implementation of Personal Data Privacy Management Programme (PMP)

The PCPD has advocated since 2014 that enterprises should develop their own PMP with the rising public expectations for privacy protection. In particular, enterprises should embrace personal data protection as part of their corporate governance responsibilities and apply them as a business imperative throughout the enterprises, starting from the board room. A PMP usually consists of three components namely 1) organisation commitment; 2) programme control; and 3) on-going assessment and revision.

Enterprises were asked about the stage of implementation of PMP in their organisation. From the results of the survey, adoption of PMP is more common among Corporates, with close to half (48%) of them having "fully implemented" their own PMP, and another 10% of them having "just started implementation" or "being ready to implement". However, the implementation level is opposite among SMEs, with 55% having "no plan of implementation".



Looking into the results by business categories, more enterprises from *Information and Communications Technology* (43%) and *Financial Services* (40%) have "fully implemented" PMP, while 61% of enterprises from *Retail and Tourism* and *Manufacturing, Trading and Logistics* have no plan of implementing PMP.

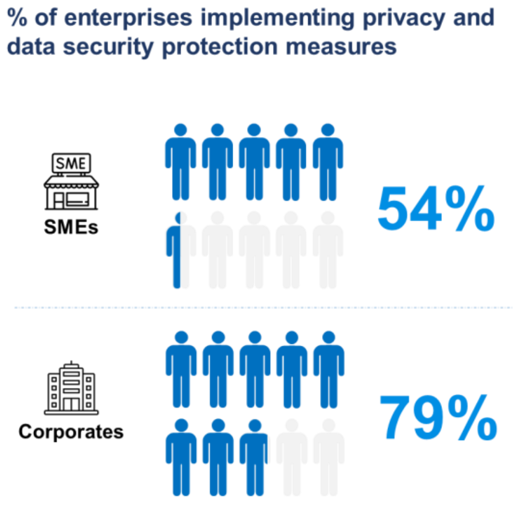
	FS	RT	MTL	ICT	PS	NGO	All
No plan of implementation	**33%**	**61%**	**61%**	**40%**	**55%**	**40%**	**52%**
Start planning implementation	**10%**	**7%**	**5%**	**5%**	**15%**	**15%**	**9%**
Ready to implement	**8%**	**12%**	**8%**	**10%**	**5%**	**6%**	**8%**
Just started implementation	**10%**	**4%**	**4%**	**3%**	**0%**	**8%**	**5%**
Fully implemented	**40%**	**16%**	**22%**	**43%**	**25%**	**31%**	**26%**

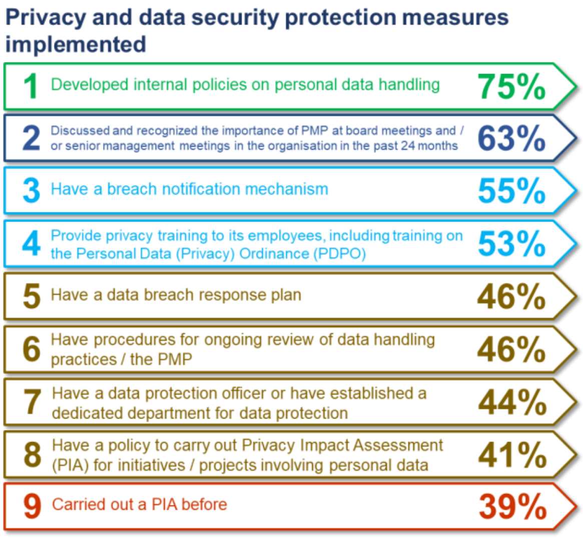
FS: Financial Services **RT:** Retail and Tourism related **MTL:** Manufacturing, Trading and Logistics
ICT: Information and Communications Technology **PS:** Professional Services **NGO:** NGOs, Schools and Others
All: All Business Categories

3.4.1.2 Implementation of Privacy and Data Security Protection Measures

Similar to the results of PMP implementation, implementation of various privacy and data security protection measures is significantly higher among Corporates, with close to 80% of them having implemented at least one of the privacy and data security protection measures. Meanwhile, around half of the surveyed SMEs have implemented at least one of the measures.

Of the privacy and data security protection measures implemented by these enterprises, "having developed internal policies on personal data handling" (75%) is most commonly implemented, followed by "having discussed and recognised the importance of PMP at board meetings and / or senior management meetings in the organisation in the past 24 months" (63%), "having a breach notification mechanism" (55%) and "providing privacy training to its employees" (53%). On the contrary, only 39% have "carried out a Privacy Impact Assessment before".


% of enterprises implementing privacy and data security protection measures


Privacy and data security protection measures implemented

In terms of the implementation of privacy and data security protection measures among different business categories, *Financial Services* (82%), *Information and Communications Technology* (73%) and *NGOs, Schools and Others* (70%) enterprises show higher implementation rate. Although *Retail and Tourism* ranks third in business categories collecting personal sensitive data (37%), it has the lowest implementation rate in terms of privacy and data security protection measures (42%).

	FS	RT	MTL	ICT	PS	NGO	All
Implementing Privacy and Data Security Protection Measures	**82%**	**42%**	**54%**	**73%**	**58%**	**70%**	**59%**
Not Implementing Privacy and Data Security Protection Measures	**18%**	**58%**	**46%**	**28%**	**42%**	**30%**	**41%**

FS: Financial Services **RT:** Retail and Tourism related **MTL:** Manufacturing, Trading and Logistics
ICT: Information and Communications Technology **PS:** Professional Services **NGO:** NGOs, Schools and Others

All: All Business Categories

3.4.2 Privacy Risks in Using Emerging Technologies

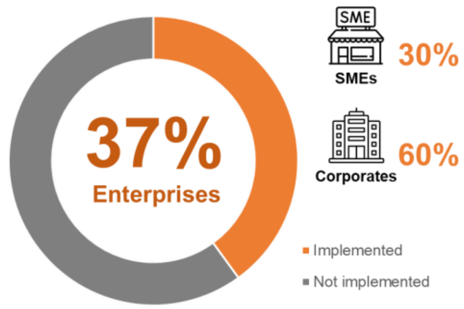
3.4.2.1 Usage of Emerging Technologies

The thematic survey this year also gauged enterprises' usage of the following emerging technologies in their daily operation, their perceived level of privacy risks in using these technologies, and whether they have developed internal guidelines in addressing the risks associated with privacy:

- Generative AI (for text, audio, image, video, code, etc.) such as ChatGPT;
- Data analytics and work process automation;
- Internet of Things (IoT);
- Blockchain related technology;
- Cloud computing; and
- Cookies and other online trackers

In general, using new technologies in daily operation is not very common among surveyed enterprises. An overall 37% of enterprises use at least one of the above technologies in their operations, with the percentage of enterprises claiming to have "implemented" each of these technologies ranging from 5% to 22%. Technologies considered more mature, namely "cloud computing" (22%), "data analytics and work process automation" (19%) and "cookies and other online trackers" (18%) are more commonly implemented.

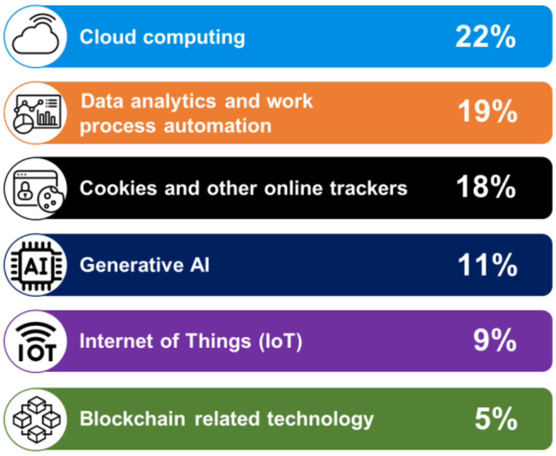
It is also found that Corporates (60%) have higher rate of implementing these emerging technologies compared to SMEs (30%).



Implemented any *emerging technologies in operations

*Note: The emerging technologies covered in the survey include: (i) Generative AI, (ii) data analytics and work process automation, (iii) Internet of Things (IoT), (iv) blockchain related technology, (v) cookies and other online trackers, and (vi) cloud computing

% of Enterprises Implementing Respective Emerging Technologies in Operations:



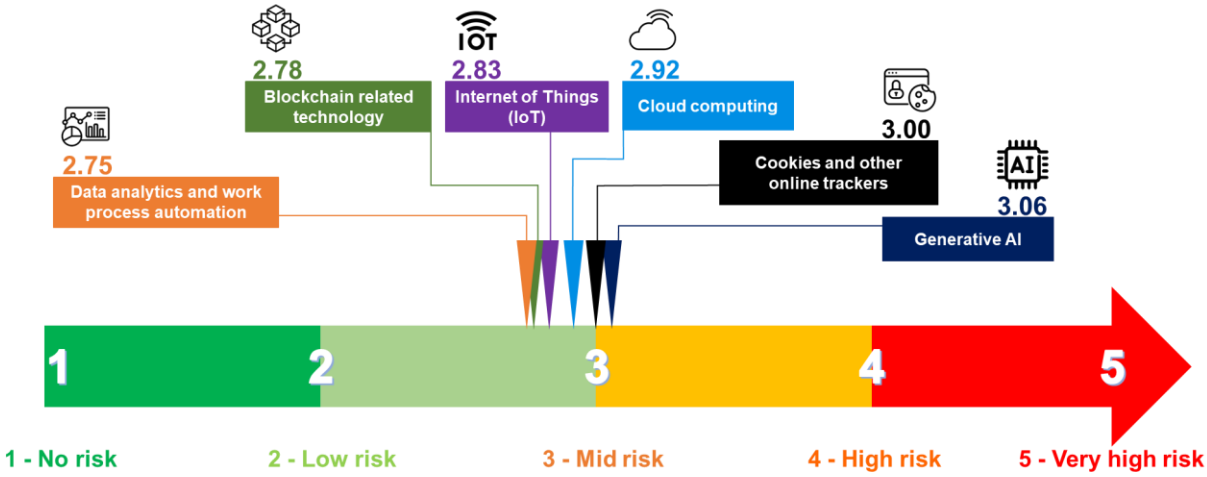
The following table shows the further breakdown between Corporates and SMEs in respect of each emerging technology:

	SMEs	Corporates	All
Cloud computing	**18%**	**42%**	**22%**
Data analytics and work process automation	**15%**	**40%**	**19%**
Cookies and other online trackers	**14%**	**37%**	**18%**
Generative AI	**9%**	**22%**	**11%**
Internet of Things (IoT)	**6%**	**23%**	**9%**
Blockchain related technologies	**2%**	**18%**	**5%**

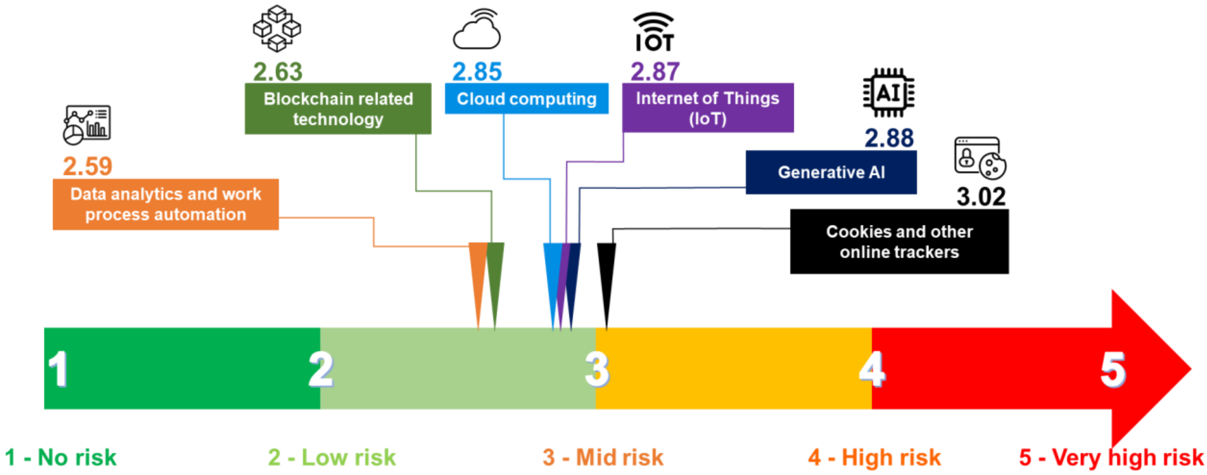
In general, Corporates have a higher rate of implementing these emerging technologies across the board, and the implementation of “cloud computing” and “data analytics and work process automation” reaches 40%. On the other hand, technologies which are considered more mature, namely “cloud computing”, “data analytics and work process automation” and “cookies and other online trackers” are more commonly implemented by both SMEs and Corporates.

3.4.2.2 Perceived Level of Risk to Privacy when Using the Emerging Technologies

All enterprises, regardless of whether they are currently using respective emerging technologies, are aware of the risk to privacy associated with such usage. On a scale of 1 (“No risk”) to 5 (“Very high risk”), enterprises’ perceived risk of using these technologies ranges from 2.75 to 3.06 (i.e. between “Low risk” and “Mid risk”). In particular, they consider “Generative AI” (3.06) and “Cookies and other online trackers” (3.00) having the highest level of privacy risk involved, at “Mid Risk” level. This is followed by “Cloud computing” (2.92), “IoT” (2.83) and “Blockchain related technology” (2.78).



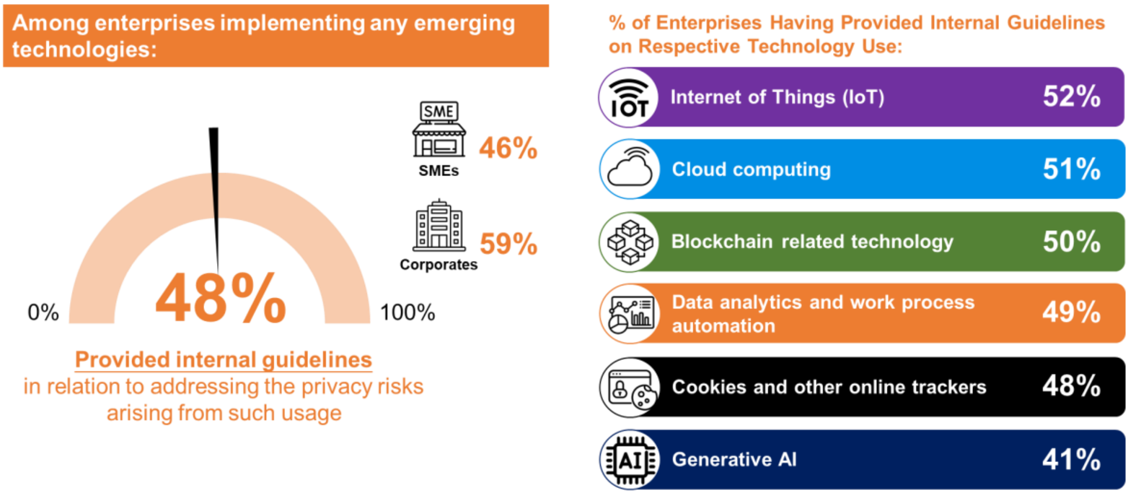
Among enterprises using respective emerging technologies, they are also aware of the privacy risk associated with their usage. Their perceived risk of using these technologies ranges from 2.59 to 3.02 (i.e. between "Low risk" and "Mid risk"). Instead of "Generative AI" being considered as having the highest risk at overall level, "Cookies and other online trackers" (3.02) rank first in terms of the perceived privacy risk involved in usage. "Generative AI" (2.88) ranks second, and is followed by "IoT" (2.87) and "Cloud computing" (2.85).



Note: Due to small sample bases, no sub-group comparison between Corporates and SMEs is available

3.4.2.3 Availability of Internal Guidelines in Response to the Risk Associated with the Use of Emerging Technologies

Although enterprises using respective emerging technologies are aware of the privacy risk associated with such usage as outlined in the previous section, for majority of these technologies, overall only about half (48%) of the enterprises using these emerging technologies have internal guidelines available for using respective technologies in response to the privacy risks associated. Notably, the level of implementation of internal guidelines by enterprises using Generative AI (41%) is the lowest.

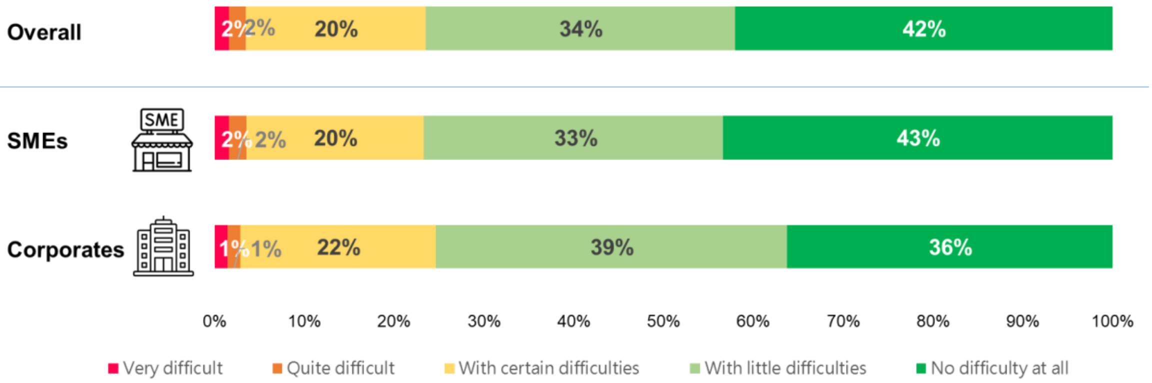


Note: Due to small sample bases, no sub-group comparison between Corporates and SMEs are available

3.4.3 Perception towards Privacy Protection in Hong Kong

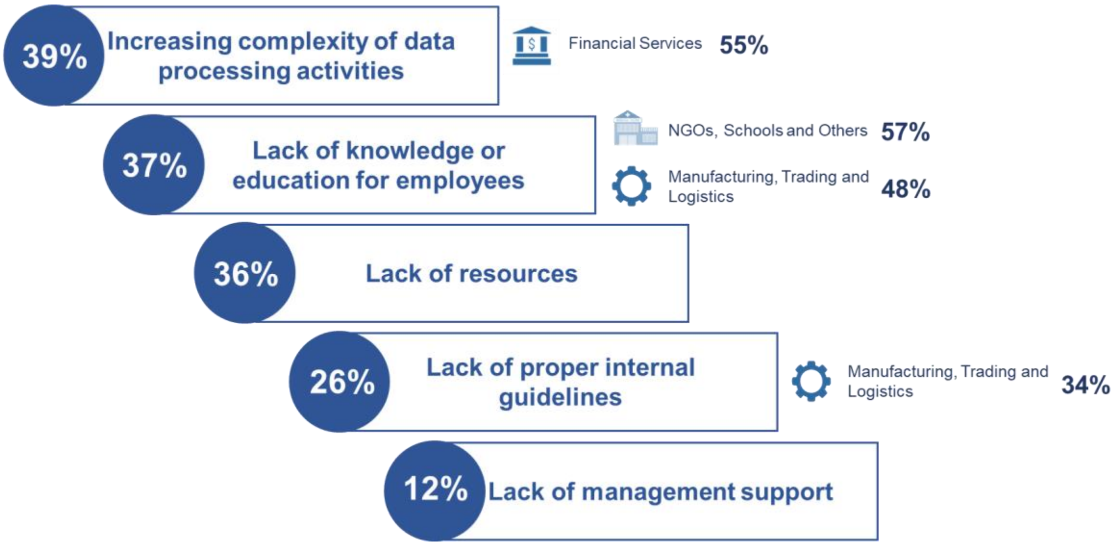
3.4.3.1 Perceived Level of Difficulty to Comply with the PDPO

Majority of the surveyed enterprises are confident in complying with the PDPO, with 42% consider having "no difficulty", and 34% consider having "little difficulties". On the other hand, only 4% of the surveyed enterprises consider compliance with PDPO "quite difficult" or "very difficult".



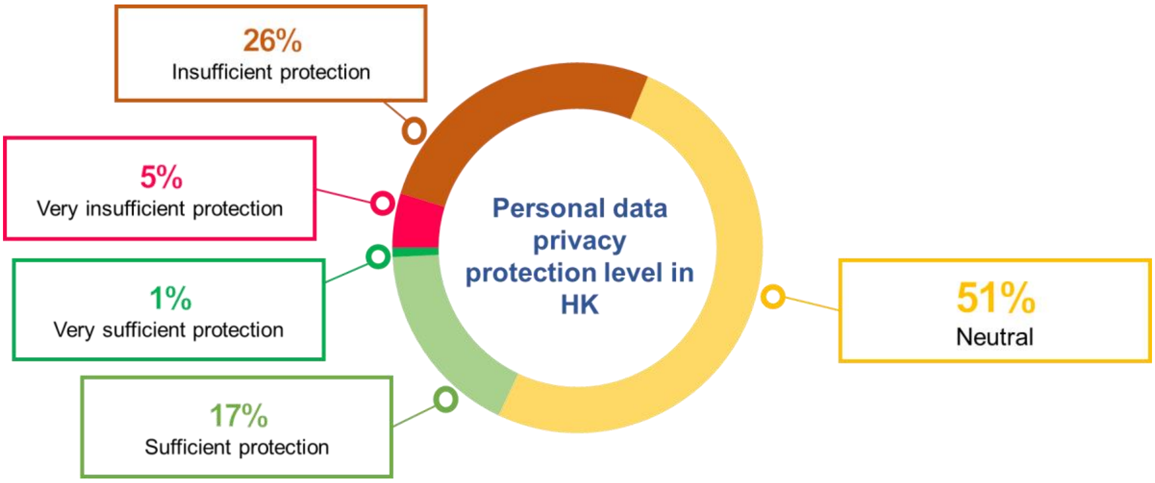
In terms of the key challenges faced by enterprises in complying with the PDPO, the top 3 challenges identified are "increasing complexity of data processing activities" (39%), "lack of knowledge or education for employees" (37%) and "lack of resources" (36%).

Looking into the results by business categories, it is found that "increasing complexity of data processing activities" is more commonly reported by *Financial Services* (55%) as a challenge, while *NGOs, Schools and Others* (57%) and enterprises in *Manufacturing, Trading and Logistics* (48%) more commonly perceive "lack of knowledge or education for employees" as a challenge, and 34% of enterprises in *Manufacturing, Trading and Logistics* consider "lack of proper internal guidelines" as a key challenge. Notably, only 12% of enterprises consider "lack of management support" a challenge for compliance.



3.4.3.2 Overall Perception on the Level of Personal Data Privacy Protection in Hong Kong

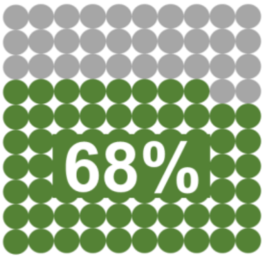
While slightly over half (51%) of the surveyed enterprises take a neutral stance, 18% of them consider the level of personal data privacy protection in Hong Kong "sufficient" or "very sufficient". On the other hand, about three in ten enterprises consider such protection "insufficient" or "very insufficient". Subgroup analysis found that the result is consistent regardless of company size and business categories.



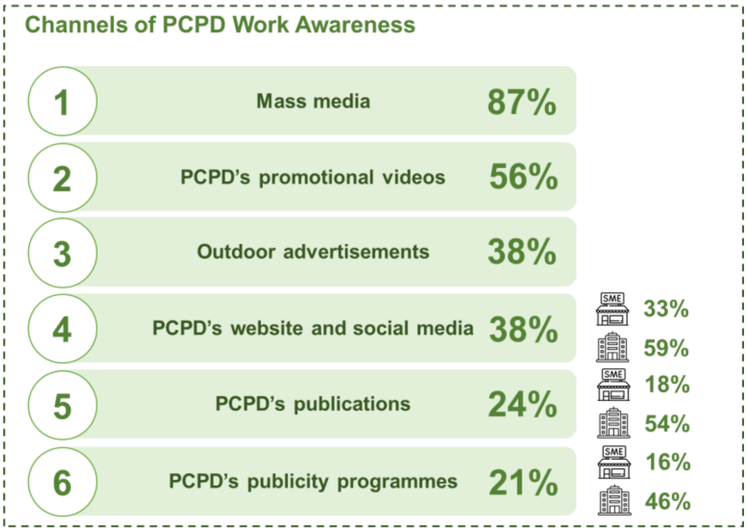
3.4.4 Awareness of the Work of PCPD

Over two-thirds (68%) of the surveyed enterprises are aware of the work of PCPD. Among these enterprises, mass media (87%) is the most common channel through which enterprises know about the work of PCPD, followed by "PCPD's promotion videos (e.g. on TV or YouTube)" (56%).

Analysis by company size also finds that significantly more Corporates than SMEs understand more about PCPD through "PCPD's website and social media" (59%, vs. 33% for SMEs), "PCPD's publications (e.g. guidance notes, pamphlets, factsheets and code of practice, etc.)" (54%, vs. 18% for SMEs) and "PCPD's publicity programmes (e.g. seminars, webinars, workshops)" (46%, vs. 16% for SMEs).



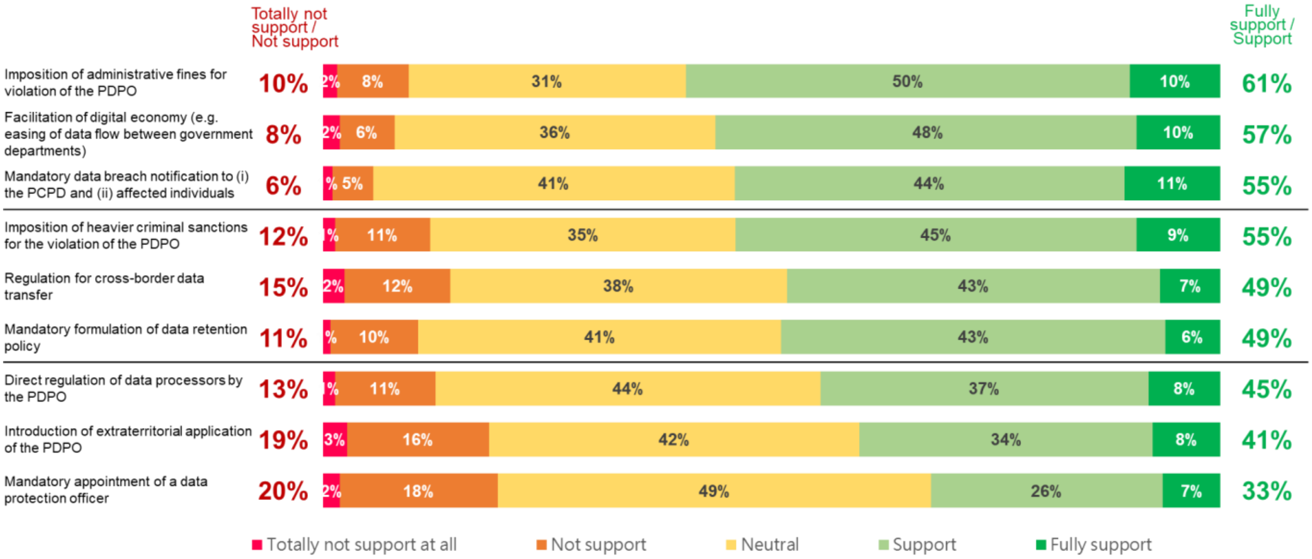
Are aware of the work of PCPD



3.4.5 Level of Support towards Various Proposed Amendments to the PDPO

Surveyed enterprises in general are supportive towards majority of the proposed amendments to the PDPO. Among the proposed amendments evaluated in the survey, “Imposition of administrative fines for violation of the PDPO” is the most supported proposed amendment, with 61% of the survey enterprises “fully support” or “support” such amendment. This is followed by “Facilitation of digital economy (e.g. easing of data flow between government departments)”, “Mandatory data breach notification to (i) the PCPD and (ii) affected individuals” and “Imposition of heavier criminal sanctions for the violation of the PDPO”, with 57%, 55% and 55% of enterprises indicating support respectively. “Mandatory appointment of a data protection officer” receives the lowest level of support, with only one-third of the enterprises stating they “fully support” or “support” the amendment.

On the other hand, it is notable that a considerable proportion (ranging from 31% to 49%) of the surveyed enterprises hold a neutral stance towards each of the proposed amendments.

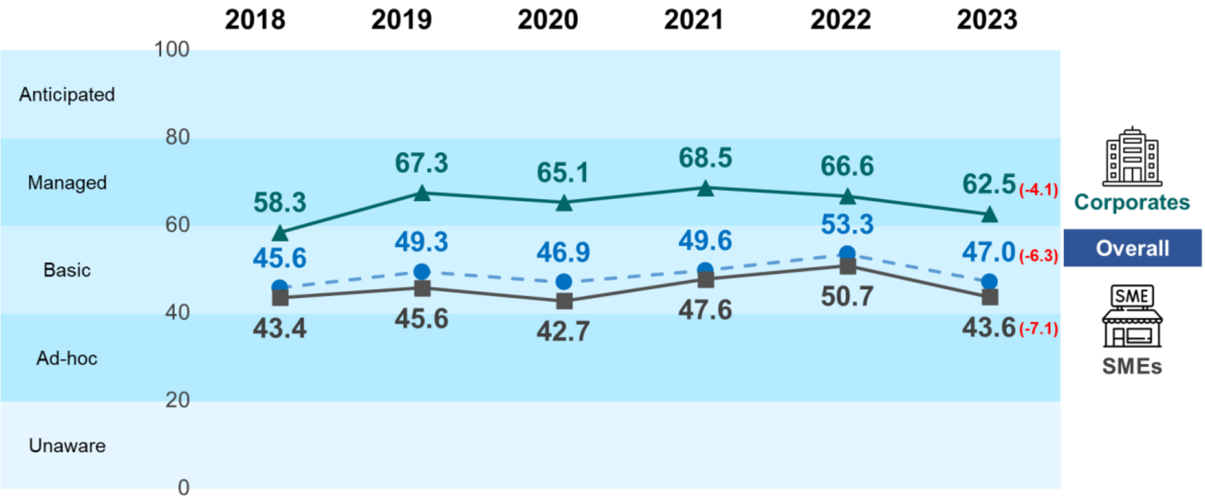


4. Summary & Recommendations

4.1 Key Findings

Hong Kong Enterprise Cyber Security Readiness Index

Overall Index drops by 6.3 points to 47.0 points, which is the largest drop since the launch of the Index in 2018. Both SMEs (43.6 points) and Corporates (62.5 points) suffer drops in index, with SMEs' index falling at a larger magnitude (-7.1 points). Although the index for Corporates further weakens by another 4.1 points this year, it still sustains the "Managed" level of cyber security readiness.



Financial Services (64.9 points) and *Information and Communications Technology* (63.3 points) sustain the "Managed" level of cyber security readiness, with the latter being the only business category with increment registered. *Manufacturing, Trading and Logistics* (48.6 points), *NGOs, Schools and Others* (45.9 points) and *Professional Services* (43.5 points) also continue staying at "Basic" level despite declines at different magnitudes. However, *Retail and Tourism* (33.3 points) suffers the largest drop of 12.5 points, falling to "Ad hoc" level of cyber security readiness.

Cyber Security Attacks Encountered in Past 12 Months

73% of the surveyed enterprises have experienced at least one type of cyber security attacks in the past 12 months, regardless whether such attacks caused financial losses to the enterprise(s) concerned or not. Compared with 2022, the incidence rate uplifted significantly by 8 percentage points to its record high. There has been a surge of 10 percentage points in the incidence of cyber security attacks among SMEs.

"Phishing attacks" continues to be the most common type of cyber security attacks, taking place on 96% of those who have encountered cyber security attacks in the past 12 months. "Email phishing" (79%) is still the most common type of phishing attacks, while "Smishing" (34%, +14%-points) and "Angler phishing" (16%, +6%-points) have become more common. In addition, emerging types of phishing attacks, namely

"Phishing using AI or Generative AI" and "QR code phishing", are also respectively reported by 9% and 8% of those enterprises having encountered cyber security attacks in the past 12 months.

Looking at the types of cyber security attacks (external attacks, internal attacks and attacks caused by external parties) encountered by the surveyed enterprises, external attacks further uplift by another 13 percentage points to a record high of 72%. Although occurrence of internal attacks returns a low level of 3%, occurrence of attacks caused by external partners remains at its relatively high level despite an improvement to 7%.

A Need for Arousing Attention on Human Awareness of Cyber Security

Although the level of cyber security has improved compared with the past, and most of the cyber security attacks can be detected and prevented, humans are still playing a vital role. "Human Awareness Building" can help prevent cyber security attacks from happening. From the results of this round of survey, there has been no significant improvement in such awareness:

1. "Human Awareness Building" sub-index remains low at 25.2 points, which is at the verge of "Ad hoc" level;
2. Phishing attacks remains prominent and the types of phishing attacks have become more diversified, but they can be avoided with proper human awareness education. In this round of survey, however, still only 28% of the surveyed enterprises have conducted staff security awareness education in the past 12 months, and only one in five enterprises have conducted cyber security drill exercise.

Implementation of PMP and Privacy and Data Security Protection Measures

The survey found that implementation of PMP and various data security protection measures is more common among Corporates:

1. Close to half (48%) of the Corporates have "fully implemented" PMP, but 55% of SMEs have "no plan of implementation"; and
2. 79% of the Corporates have implemented at least one privacy and data security protection measure, but the corresponding figure is only 54% among SMEs.

In terms of the privacy and data protection measures adopted, some of the more commonly implemented ones fall within the *Organisation Commitment* and *Programme Controls* components of PMP:

1. 75% have developed internal policies on personal data handling;
2. 63% have discussed and recognised the importance of PMP at board meetings; and / or senior management meetings in the organisation in the past 24 months
3. 55% have a breach notification mechanism; and
4. 53% have provided privacy training to its employees, including training on the PDPO.

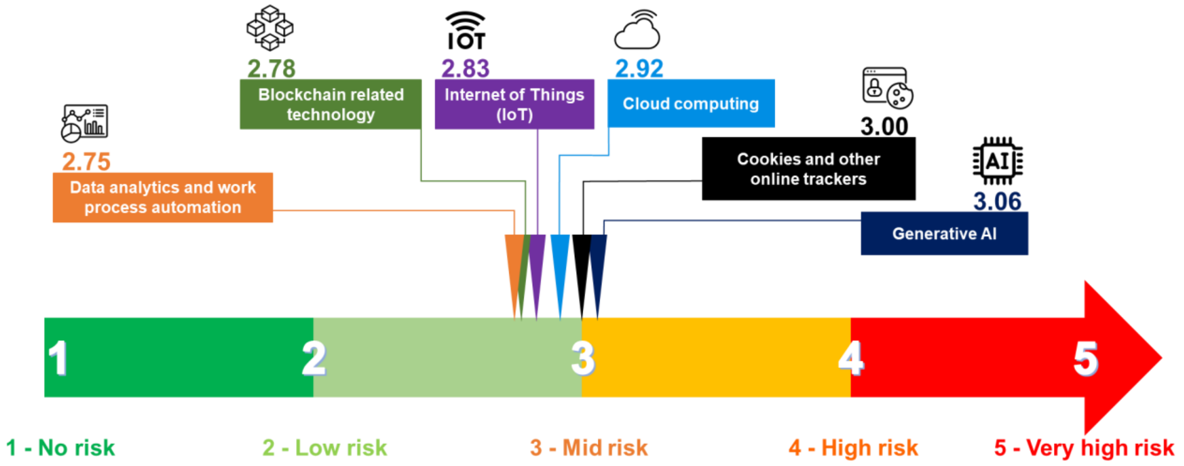
On the other hand, measures in relation to the *Ongoing Assessment and Revision* component of the PMP (for example, having procedures for ongoing review of data handling practices or the PMP) are relatively less common (46%). Other less commonly adopted PMP measures include:

1. Having a data breach response plan (46%);
2. Having a data protection officer or have established a dedicated department for data protection (44%); and
3. Having a policy to carry out Privacy Impact Assessment (PIA) for initiatives / projects involving personal data (41%) / Carried out a PIA before (39%).

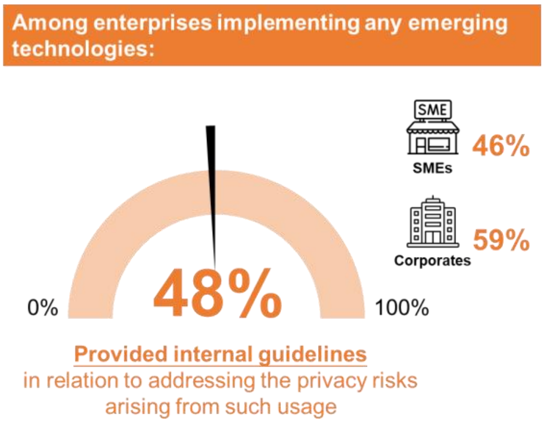
Adoption of Emerging Technologies and Perception towards the Privacy Risks of Emerging Technologies

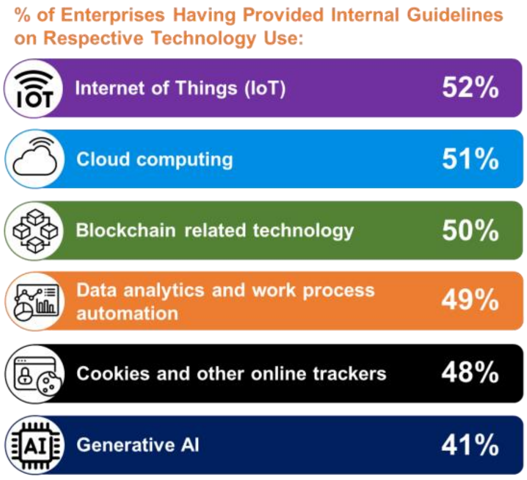
All enterprises, regardless of whether they are currently using respective emerging technologies, namely Generative AI, Data analytics and work process automation, IoT, Blockchain related technology, Cloud computing and Cookies and other online trackers, are aware of the risk to privacy associated with such usage, with their perceived risk level associated with such usage ranges from 2.75 to 3.06 (i.e. between "Low risk" and "Mid risk").

In particular, they consider "Generative AI" (3.06) and "Cookies and other online trackers" (3.00) having the highest level of privacy risk involved, followed by "Cloud computing" (2.92), "IoT" (2.83) and "Blockchain related technology" (2.78).



Although enterprises using respective emerging technologies are aware of the privacy risk associated with such usage as outlined in the previous section, overall only close to half (48%) of these enterprises have internal guidelines available for using respective technologies in response to the privacy risks associated. Availability of internal guidelines for using Generative AI is even lower, at 41%.





Perception towards Personal Data and Privacy Protection in Hong Kong

Majority of the surveyed enterprises are confident in complying with the Personal Data (Privacy) Ordinance (PDPO), with 42% consider having “no difficulty”, and 34% consider having “little difficulties”.

Regarding the overall level of personal data privacy protection in Hong Kong, while slightly over half (51%) of the surveyed enterprises take a neutral stance, 18% of them consider the level “sufficient” or “very sufficient”.

“Increasing complexity of data processing activities” (39%), “lack of knowledge or education for employees” (37%) and “lack of resources” (36%) are the top 3 perceived challenges facing enterprises in their compliance with the PDPO.

4.2 Recommendations

In response to the survey findings, the following recommendations are provided for enterprises:

(1) Move the Security Readiness Level up to the "Managed" level, and Timely Adopt Cyber Security and Data Security Measures

Amid escalation of cyber threats, more and more enterprises are digitalising their business. This trend will continue especially when more activities have become digitalised due to the pandemic. The Overall Enterprise Cyber Security Readiness Index has stayed at the "Basic Level" for several years, and the largest drop is also observed this year. Enterprises, especially smaller ones, should further enhance their cyber security readiness and move up to the "Managed" level.

To attain the most significant improvement, efforts could be directed towards addressing the weaker areas, especially "Human Awareness Building" which remains at a very low level of 25.2 points. "Policy & Risk Assessment" is the second priority area for enterprises to work on, where a drop of 8.9 points to "Ad hoc" level is observed in this round's survey due to the loosening in the conduct of "Security risk assessment". Enterprises can also review and enhance their "Patch management" and "Cyber threats protection" under "Technology Control" if resources are sufficient.

To strengthen cyber security and data security and prevent malicious attacks on their information systems, all organisations should take precautionary measures, raise their awareness of cyber security and review their data security systems, and adopt the following cyber security and data security measures timely:

- Secure computer networks: Using security devices or software such as firewalls and / or antimalware applications to protect computer networks. Software (including mobile apps and anti-malware applications) should be regularly updated to detect new viruses and emerging threats;
- Conducting vulnerability assessments and penetration tests on a regular basis, in particular for those internet facing systems;
- Implementing patch management to fix security vulnerabilities in a timely manner;
- Encrypting data in transit and storage, and effectively managing and protecting the encryption keys;
- Database management: Separating database servers from web servers by firewalls to protect the internal servers in case the web servers are compromised;
- Adopting the "least privilege" principle to grant as few access rights as possible to complete a task and assign users to appropriate roles (including restriction of the volume of data to be accessed and the duration of access); and

- Timely destructing unnecessary or expired personal data.

The PCPD issued the "Guidance Note on Data Security Measures for Information and Communications Technology" in August 2022, to provide organisations holding personal data with recommended data security measures.

(2) Raise Cyber Security Awareness via Education

Humans are always the weakness link in cyber security, yet cyber security awareness education is usually not put as a top priority until cyber attacks are reported. In this round's survey, "phishing attacks" continues to be the most common type of cyber security attacks facing enterprises, with nearly every enterprise encountering cyber security attacks in the past 12 months having such encounter. In fact, "phishing attacks" leverage on human vulnerability, for example, when a staff member accidentally opens an attachment with ransomware or clicks into a phishing link, leading to the data on the enterprise server to be encrypted and become inaccessible.

As such, it is advised to increase cyber security awareness through:

- Providing regular training to all general staff and newcomers; and encouraging them to undergo training on Cybersec Training Hub (https://cyberhub.hk/) or attend PCPD's courses;
- Conducting regular cyber security drill exercises, monitoring the performance, and addressing areas of weakness;
- Attending seminars on cyber security and subscribing to Security Advisory for updates on cyber security attacks and solutions;
- Joining Cybersec Infohub (https://www.cybersechub.hk/en/home/highlights) and PCPD's Data Protection Officer's Club (https://www.pcpd.org.hk/misc/dpoc/index.html) to exchange information and industry peers for building up collaborative defence
- Having senior management's open commitment to reinforcing a culture of security;
- Browsing HKCERT's "All-Out Anti-Phishing" Thematic Page which is a "one-stop" and easy-to-use information portal on phishing. The page also provides enterprises with ready-to-use materials to conduct phishing awareness training to their employees (https://www.hkcert.org/publications/all-out-anti-phishing)
- Browsing PCPD's "Data Security" Thematic Page, which provides "one stop" access to information concerning data security and facilitates data users' compliance with the relevant requirements under the PDPO (https://www.pcpd.org.hk/english/data_security/index.html)
- Subscribing to Managed Security Services (MSS) with extensive cyber security solutions for proactive detections and rapid responses to cyber security attacks while understanding the scale and nature of the attacks, internal controls and residue risks; and
- (For SMEs) Downloading the Incident Response Guideline for SMEs

(https://www.hkcert.org/tc/security-guideline/incident-response-guideline-for-smes) on the actions and procedures to prevent and handle cyber security attacks.

(3) Managed Security Services

The top four challenges of cyber security management continue to be talent and investment related, which include "lack of IT support and management staff" (44%), "various investments required due to the ever-changing nature of cyber security risks" (42%), "large one-off investment on infrastructure required" (38%) and "lack of expertise (IT personnel or knowledge) to deploy" (37%). Meanwhile, majority of the surveyed enterprises are spending HK99,999 or less on cyber security.

Enterprises could consider subscribing to MSS, which is an outsourcing model of security expertise addressing the above challenges of cyber security management with low set-up budget requirements and flexible pricing options, as well as the comprehensive support from cyber security experts.

(4) Establish a PMP and Adopt Data Protection Measures

To enhance data governance and ensure protection of personal data privacy, we also recommend enterprises to establish a comprehensive PMP to ensure their responsible collection, holding, processing, and use of personal data. The PCPD has issued the "Best Practice Guide on Privacy Management Programme" to provide practical advice and examples in constructing a comprehensive PMP, which includes the adoption of measures such as:

- Discussing personal data protection issues at board meetings and / or senior management meetings in the organisation;
- Developing internal policies on personal data handling;
- Developing a policy to carry out Privacy Impact Assessment (PIA) for initiatives / projects involving personal data;
- Appointing a data protection officer or a dedicated department for data protection;
- Providing privacy training to its employees, including training on the Personal Data (Privacy) Ordinance (PDPO); and
- Developing procedures for ongoing review of data handling practices / PMP.

To further safeguard their data security and cyber security, enterprises should also develop a data breach response plan and notification mechanism in guarding against cyber attacks and / or data breach incidents. Enterprises should reference the "Guidance on Data Breach Handling and Data Breach Notifications" issued by the PCPD in June 2023, which assists organisations in preparing themselves in the event a data breach occurs. Enterprises can also attend the professional workshops on PMP organised by the PDPD to understand the baseline fundamentals and components of a PMP, as well as how to maintain and improve it on an ongoing basis.

(5) Adopt Emerging Technologies Responsibly

While the adoption of emerging technologies that are considered more mature (such as cloud computing, data analytics and work process automation, as well as cookies and other online trackers) amongst enterprises, especially Corporates, is more common, but the perceived level of risk to privacy in the use of these technologies, which is generally at “Mid risk” level, is not significantly different from that of other emerging technologies. It appears that the maturity of the technology is not necessarily correlated with the perceived privacy risks level. All enterprises are encouraged to beware of the privacy risks in the adoption of emerging technologies.

With the expected increase in the usage of emerging technologies, it is imperative for enterprises to ensure their proper usage to address privacy issues. As having internal guidelines to address such privacy risks is not prevalent among the enterprises using the various emerging technologies, enterprises are urged to devise appropriate internal guidelines to address such privacy risks arising from the use of emerging technologies.

- End of Report -

About HKPC

The Hong Kong Productivity Council (HKPC) is a multi-disciplinary organisation established by statute in 1967, to promote productivity excellence through relentless drive of world-class advanced technologies and innovative service offerings to support Hong Kong enterprises. Being a key enabler of Industry 4.0 and Enterprise 4.0, HKPC strives to facilitate Hong Kong's reindustrialisation, as well as bolstering Hong Kong to be an international innovation and technology hub and a smart city. The Council offers comprehensive innovative solutions for Hong Kong industries and enterprises, enabling them to achieve resources and productivity utilisation, effectiveness and cost reduction, and enhance competitiveness in both local and overseas marketplace. The Council partners and collaborates with local industries and enterprises and world-class R&D institutes to develop applied technology solutions for value creation. It also benefits a variety of sectors through product innovation, technology transfer, and commercialisation, bringing enormous business opportunities ahead. HKPC's world-class R&D achievements have been widely recognised over the years, winning an array of local and overseas accolades.

In addition, HKPC offers SMEs and startups immediate and timely assistance in coping with the ever-changing business environment, as well as enhancing their competitive edge by providing a variety of FutureSkills trainings to upskill and nurture talents with digital capabilities and STEM competencies.

For more information, please visit HKPC's website: www.hkpc.org.

About HKPC Cyber Security

Cyber security is one of the eight major development focuses of the Hong Kong Productivity Council (HKPC). With the rapid development of information and communication technology, enterprises and individuals need to take a proactive approach to cope with various threats related to information technology security and cyber attack. HKPC Cyber Security pledges to offer enterprises comprehensive cyber security testing and advisory services, covering "Security-by-design; Compliance-by-default; and Privacy-by-default", "Design & Architecture", and "Offensive Security", etc. In addition, HKPC Cyber Security also offers training and development programmes related to cyber security to help enterprises establish a cyber security culture. The programmes cover a broad spectrum of topics, from basic cyber security concepts to advanced cyber security technologies and tools. Through raising public awareness of cyber security, HKPC Cyber Security aims to safeguard enterprises against cyber and hacking attacks while cultivating cyber security specialists, thereby enhancing the overall cyber security locally, while promoting the sustainable development of the digital economy in Hong Kong.

For more information, please visit HKPC Cyber Security's webpage: https://u.hkpc.org/HKPC-CyberSecurity.

About PCPD

The Office of the Privacy Commissioner for Personal Data (PCPD) is an independent body set up to oversee the implementation of and compliance with the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) (PDPO) in Hong Kong. The PCPD strives to ensure the protection of the privacy of individuals in relation to personal data through monitoring and supervising compliance with the PDPO, enforcing its provisions and promoting the culture of protecting and respecting personal data. Visit PCPD.org.hk for more information.

License

Disclaimer

Both HKPC and PCPD shall not have any liability, duty or obligation for or relating to the content and data contained herein, any errors, inaccuracies, omissions or delays in the content and data, or for any actions taken in reliance thereon. In no event shall HKPC and PCPD be liable for any special, incidental or consequential damages, arising out of the use of the content and data.

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