



Cyber Security



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 AI Security Survey 2024



Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024



Table of Content

1. Introduction	1
1.1 Background.....	1
1.2 Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey	1
1.3 Thematic Survey of the Year	2
1.4 Structure of Report	2
2. Methodology	3
2.1 Framework of the Index	3
2.2 Sample Distribution.....	4
2.3 Profile of Surveyed Enterprises	5
3. Survey Findings	7
3.1 Cyber Security Environment	7
3.2 Hong Kong Enterprise Cyber Security Readiness Index (the Index)	17
3.3 Cyber Security Investment Plans and Challenges	27
3.4 Thematic Survey of the Year: AI Security and Privacy Risks	30
4. Summary & Recommendations	40
4.1 Key Findings	40
4.2 Recommendations.....	44



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 damage.

The Government of the Hong Kong Special Administrative Region (HKSAR) 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. In December 2020, the HKSAR Government released the Smart City Blueprint for Hong Kong 2.0 which continues to enhance and expand existing city management measures and services. 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 AI Security Survey

In view of the above, 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 2024, Hong Kong Productivity Council Cyber Security (HKPC Cyber Security), commissioned by the Office of the Privacy Commissioner for Personal Data (PCPD), conducted the seventh round of the survey using this framework and the AI Security and Privacy Risks Survey as the thematic survey of 2024. The name of the survey – **Hong Kong Enterprise Cyber Security Readiness Index and AI Security 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: AI Security and Privacy Risks

As mentioned above, the special topic chosen for in-depth understanding in 2024 was “AI security”. Relevant questions of the thematic survey were designed by HKPC Cyber Security in consultation with the PCPD.

Artificial Intelligence (AI) refers to a range of technologies involving the use of computer programmes and machines to simulate human problem-solving capability. Examples of such applied technologies include facial recognition, voice recognition, chatbots, data analysis and automated decision-making or recommendation systems.

The adoption of AI technologies is expanding rapidly across various sectors. Enterprises are leveraging AI to enhance efficiency, gain insights, and provide innovative solutions. However, this widespread adoption also introduces new risks, such as excessive collection and improper use of personal data, adversarial attacks and ethical concerns related to AI decision-making.

Therefore, AI security has become increasingly crucial in today’s digital landscape. AI security refers to the practices and measures designed to protect AI systems from various security threats, such as cyberattacks, data breaches, and unauthorised access. This involves ensuring the integrity, confidentiality, and availability of AI systems, as well as safeguarding the data (including personal data) processed and the algorithms and the AI models used.

To foster a business environment where enterprises prioritise the security and ethical use of AI technologies, the survey seeks to assess the awareness of AI security among enterprises, including their awareness of privacy risks involved in the use of AI technologies, their current use of AI and their readiness over safe and responsible use of AI, including whether they have implemented data security measures, provided training on AI to employees and formulated internal guidelines related to the use of AI.

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 detail;
- 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:

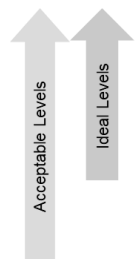
- Policy & Risk Assessment
- Technology Control
- Process Control
- Human Awareness Building



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.

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024



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 to October 2024, the survey collected the data through telephone interviews with no less than 400 enterprises, with at least 50 of them being Corporates¹. 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 Organisations (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/what_are_sme.html

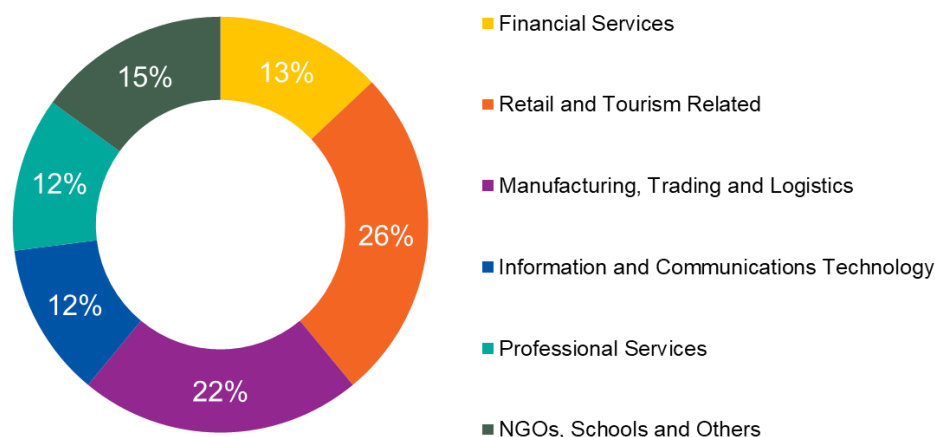
Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

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 442 enterprises in Hong Kong. As shown in the below figure, at least 12% of responses were collected for each business category, with 26% engaging in “Retail and Tourism related” businesses and 22% being “Manufacturing, Trading and Logistics” enterprises, considering the larger numbers of establishments in these categories.



Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

Among these 442 surveyed enterprises, 362 of them were Small-and-Medium Enterprises (SMEs) and 80 of them were Corporates.



362
SMEs



80
Corporates

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

	SMEs		Corporates		Total	
	<u>n</u>	<u>%</u>	<u>n</u>	<u>%</u>	<u>n</u>	<u>%</u>
<i>Financial Services</i>	45	12%	11	14%	56	13%
<i>Retail and Tourism related</i>	97	27%	18	23%	115	26%
<i>Manufacturing, Trading and Logistics</i>	82	23%	15	19%	97	22%
<i>Information and Communications Technology</i>	46	13%	7	9%	53	12%
<i>Professional Services</i>	46	13%	7	9%	53	12%
<i>NGO, Schools and Others</i>	46	13%	22	28%	68	15%
<u>All Business Categories</u>	<u>362</u>	<u>100%</u>	<u>80</u>	<u>100%</u>	<u>442</u>	<u>100%</u>



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: AI Security and Privacy Risks

The survey successfully collected the opinions from 442 enterprises – 362 SMEs and 80 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)
2024	2%	8%	16%	27%	46%	4.1
2023	3%	6%	19%	29%	42%	4.0
2022	4%	8%	22%	29%	36%	3.9
2021	1%	4%	20%	27%	48%	4.1

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

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 4.1.

Similar finding is also observed from the detailed breakdown of the results over the past 4 years. In 2024, 9 out of 10 surveyed enterprises (90%) consider IT systems and data “important” or above. It is also encouraging to see that a larger proportion of enterprises consider IT systems and data “extremely important”, up by 4 percentage points compared to last year (46% in 2024 versus 42% in 2023).

By company size, Corporates, compared with SMEs, consider IT systems and data more important, with average scores of 4.6 and 4.0 respectively.

Company Size	Average score (1 – 5 marks)
SMEs	4.0
Corporates	4.6

Looking into the results by business categories, *Information and Communications Technology* enterprises continue to perceive the importance of IT systems and data most highly, with an average score of 4.4, followed by enterprises in *Financial Services* (4.2), *Manufacturing, Trading and Logistics* (4.1), *Retail and Tourism* (4.0), and *NGOs, Schools and Others* (4.0). *Professional Services* enterprises have the lowest perceived importance score of 3.9.

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	2%	4%	4%	32%	58%	4.4
Financial Services	--	9%	13%	27%	52%	4.2
Manufacturing, Trading and Logistics	2%	7%	18%	26%	47%	4.1
Retail and Tourism related	3%	8%	19%	29%	42%	4.0
NGOs, Schools and Others	1%	10%	21%	24%	43%	4.0
Professional Services	2%	13%	17%	28%	40%	3.9

Note: “--” denotes 0%



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)
2024	*	4%	30%	50%	16%	3.8
2023	3%	5%	31%	46%	15%	3.7

Note: “*” denotes <0.5%

In general, surveyed enterprises are slightly more confident about their level of cyber security relative to last year, with an average score of 3.8 reported, compared with 3.7 last year. In particular, the proportion of enterprises being “unconfident” or “totally unconfident” (4%) has decreased by half compared with last year.

Consistently, Corporates (4.0) are more confident towards their cyber security level than SMEs (3.7).

Company Size	Average score (1 – 5 marks)
SMEs	3.7
Corporates	4.0

Similar as previous finding, *Information and Communications Technology* enterprises rank top with an average score of 4.1, with more than a quarter of them (28%) being “extremely confident”. This is followed by enterprises in *Financial Services* (4.0), *Retail and Tourism* (3.8) and *Manufacturing, Trading and Logistics* (3.7), with 86%, 65% and 60% being “confident” or “extremely confident” in their cyber security level respectively. On the other hand, *NGOs, Schools and Others* and *Professional Services* enterprises are less confident compared with other business categories, both with an average score of 3.6. In particular, 8% of enterprises in *Professional Services* enterprises are “unconfident” or “totally unconfident” in their cyber security level, the highest among all business categories.

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024



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	--	--	21%	51%	28%	4.1
Financial Services	--	4%	11%	70%	16%	4.0
Retail and Tourism related	--	4%	30%	50%	15%	3.8
Manufacturing, Trading and Logistics	--	5%	35%	45%	14%	3.7
NGOs, Schools and Others	1%	3%	41%	41%	13%	3.6
Professional Services	2%	6%	34%	49%	9%	3.6
Overall	*	4%	30%	50%	16%	3.8

Note: "--" denotes 0%; "*" denotes <0.5%

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 1.9 types of data on average, and Corporates store more types of data (2.4) than SMEs (1.7). It is also found that *Manufacturing, Trading and Logistics* (1.6) and *Professional Services* (1.8) enterprises store less types of data compared with enterprises in other business categories.

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

Type of Data Stored in the Network

	Overall	SMEs	Corporates	FS	RT	MTL	ICT	PS	NGO
<i>Base</i>	442	362	80	56	115	97	53	53	68
System data	60%	1 57%	1 76%	3 48%	1 63%	1 62%	1 68%	1 53%	1 63%
Business sensitive data	49%	2 48%	3 54%	2 54%	2 45%	2 52%	2 55%	1 53%	3 41%
Personal sensitive data	37%	3 33%	2 55%	41%	3 37%	18%	3 42%	3 36%	2 57%
Compliance / Regulated data	35%	31%	53%	1 57%	3 37%	3 21%	26%	34%	3 41%
Average	1.9	1.7	2.4	2.0	1.9	1.6	1.9	1.8	2.1

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” (60%) ranks top, followed by “Business sensitive data” (49%). It is also found that significantly more Corporates (53%) store “Compliance / Regulated data” than SMEs (31%).

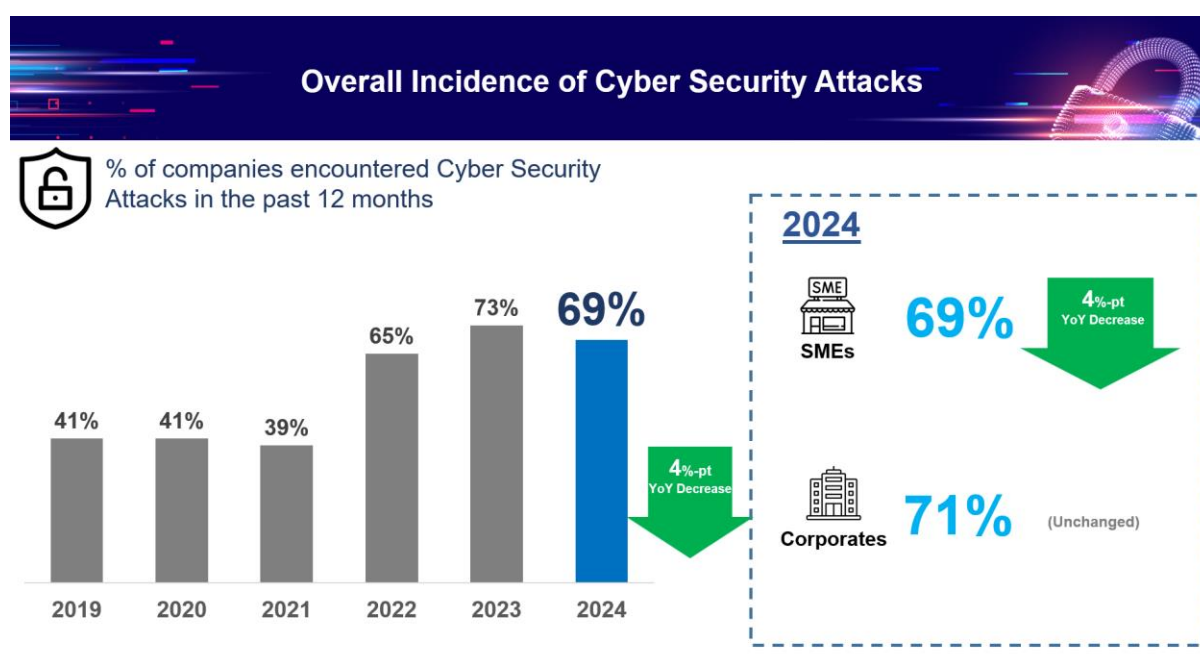
In different business categories, the types of data being stored slightly differ. In particular, “Compliance / Regulated data” is more commonly stored among *Financial Services* enterprises (57%), while more *NGOs, Schools and Others* (57%) store “Personal sensitive data”. On the other hand, less than half of the *Financial Services* enterprises (48%) keep “System data”, the proportion of which is relatively lower when compared with other business categories (ranging from 53% to 68%).

3.1.4 Cyber Security Attacks Experienced in the Past 12 Months

3.1.4.1 Incidence of Cyber Security Attacks in the Past 12 Months

69% of the surveyed enterprises have experienced at least one type of cyber security attack in the past 12 months, which include both attacks that resulted in financial losses to the enterprise(s) concerned and those that did not. Compared with 2023, the incidence rate drops by 4 percentage points.

The decreased incidence of cyber security attacks is mainly from SMEs (69%, -4 percentage points). On the other hand, such incidence remains unchanged among Corporates (71%).



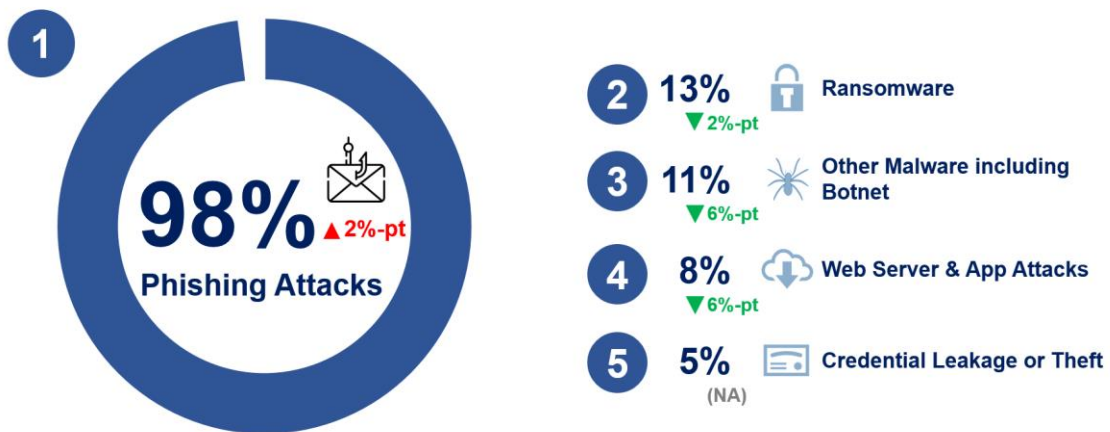
Cyber security attacks can be classified into three types, namely external attacks, internal attacks, and attacks caused by external partners (e.g. outsourced IT / business partners). The following types of cyber security attacks were covered in this year's survey:

- Ransomware
- Other malware attacks, including botnet
- 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. impersonating 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
 - Phishing website or social media counterfeiting your organisation
 - Other phishing attacks
- Web server and App attacks
- Attack on other services like remote access / CCTV (Closed-circuit television) / Internet of Things (IoT)
- Attacks targeting Web3.0, such as theft of crypto assets, and attacking smart contracts or enterprise blockchain
- Supply chain attacks

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

“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 (98%) of the enterprises which encountered cyber security attacks during the reference period. In addition to “phishing attacks”, the forms of cyber security attacks that are more commonly experienced this year are similar to last year’s, which include “ransomware” (13%), “other malware attacks including Botnet” (11%) and “web server and app attacks” (8%). “Credential leakage or theft”, experienced by 5% of the enterprises, is a newly added option in the survey this year.

Top 5 Cyber Security Attacks Encountered in the Past 12 Months

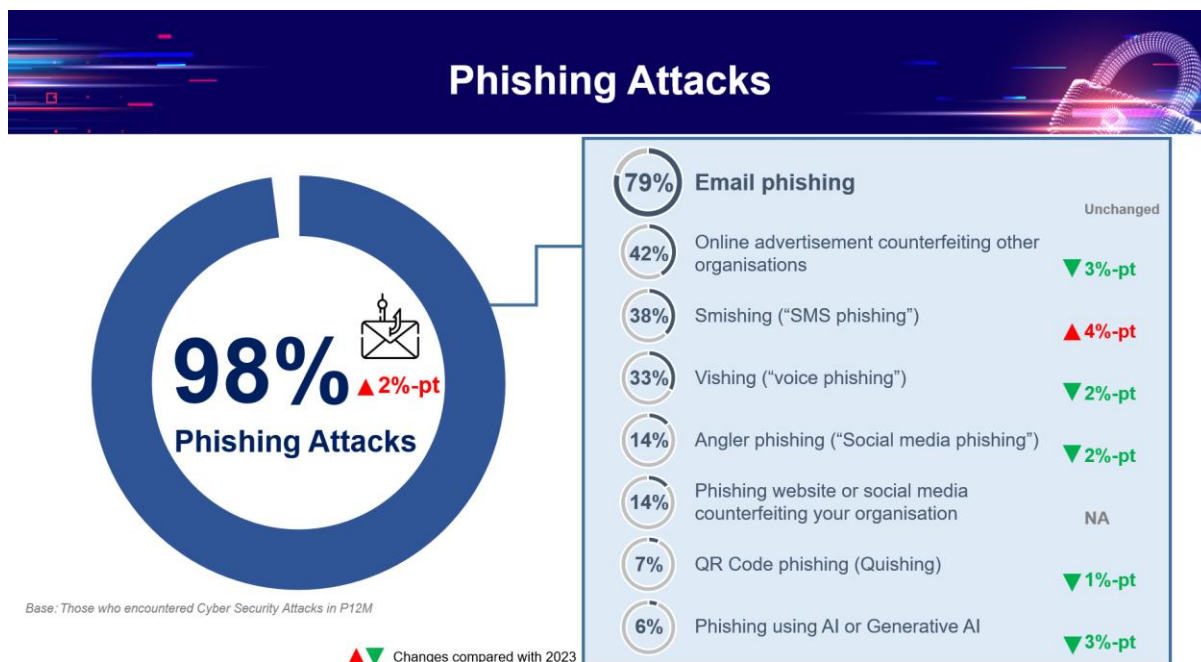


Base: Those who encountered Cyber Security Attacks in P12M

▲ ▼ Changes compared with 2023

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

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” (42%), “Smishing” (38%) and “Vishing” (33%), where increased incidence is observed for the “Smishing” attacks. Meanwhile, emerging phishing attacks such as “Quishing (QR Code phishing)” (7%) and “Phishing using AI or Generative AI” (6%) are also reported by enterprises, showing a sustained occurrence of phishing attacks in the past 12 months.

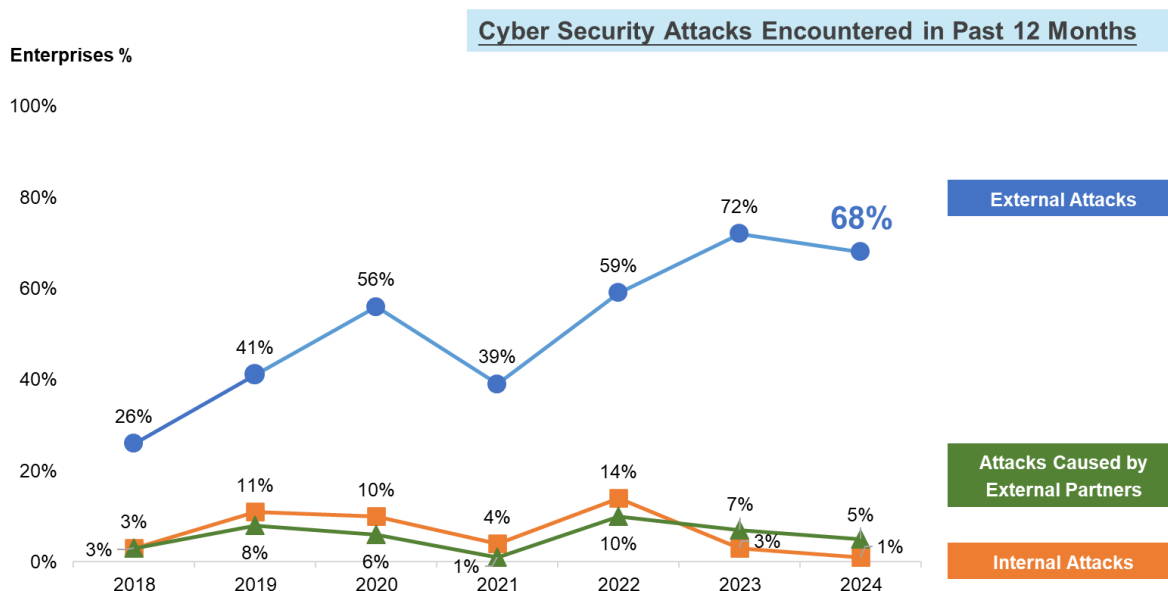


3.1.4.2 External and Internal Attacks Experienced

Surveyed enterprises which encountered at least one type of cyber security attack 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 nearly 7 out of 10 surveyed enterprises (68%) having such encounter over the past 12 months. Compared with last year, such incidence slightly dropped by 4 percentage points.

Occurrences of internal attacks and attacks caused by external partners are significantly lower than those of external attacks, with 1% and 5% of the surveyed enterprises having encountered each type of these cyber security attacks respectively.





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 2024 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 a level (from 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:

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024



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 * Endpoint Detection & Response (EDR) * Has consolidated system event logs of multiple systems * Acquired threat intelligence * Network Access configuration * Red Teaming/Penetration Test (PT) * Zero Trust Architecture (ZTA) * Passwordless authentication * Managed Security Service (MSS) * Data loss prevention (DLP) * Secure Email Gateway * Mobile Device Management * Dark Web monitoring service * Virtual Private Network * Attack Surface Management * 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 * Review access log regularly	

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

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:

$$\text{Overall Index} = \text{Average of Sub-Indices}$$

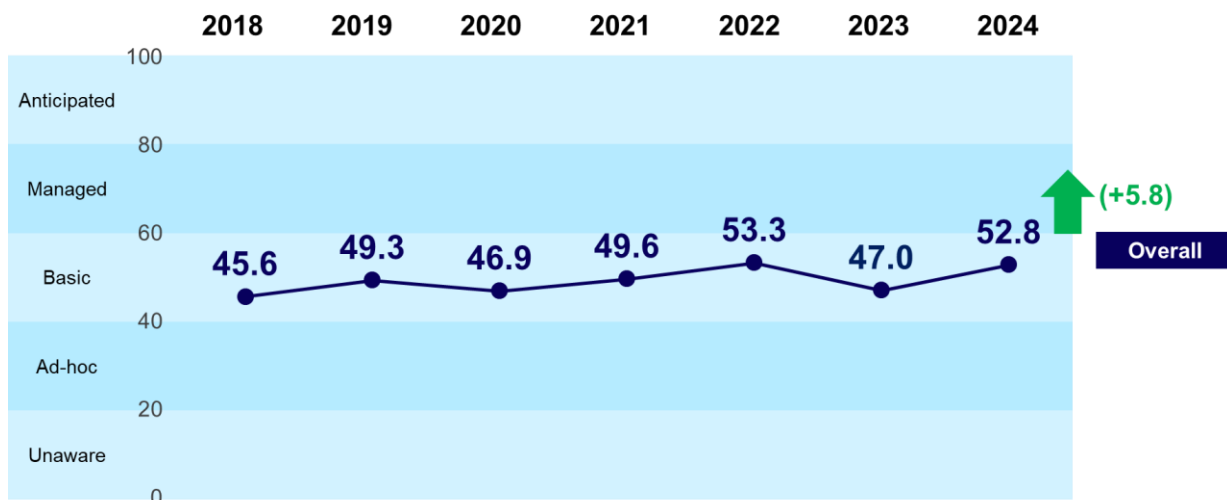
An enterprise's level of cyber security readiness can be understood by its overall index score, and the following table details the description of each level:

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.

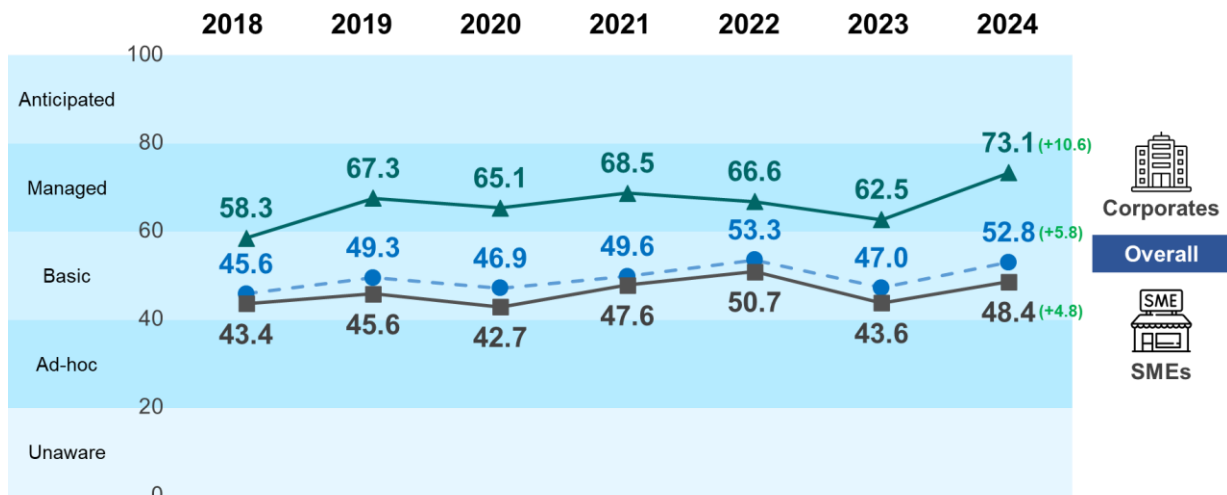
Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

3.2.2 Overall Index



The overall index increases by 5.8 points in 2024 to 52.8 points, the largest yearly increase since the launch of the index in 2018.

The chart below shows the changes of the overall index by company size:



Looking at the index's changes by company size, both the indices for SMEs (48.4 points) and Corporates (73.1 points) increase. The index for Corporates has even reached a record high and it remains in the "Managed" level of cyber security readiness.

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

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

	2018	2019	2020	2021	2022	2023	2024		
	Index	Index	Index	Index	Index	Index	Index	Level	YoY Change
Financial Services	60.5	66.0	62.9	62.9	65.7	64.9	68.3	Managed	+3.4
Information and Communications Technology	51.6	55.8	50.2	52.2	61.1	63.3	58.9	Basic	-4.4
NGOs, Schools and Others	45.5	51.8	51.9	52.3	47.1	45.9	56.4	Basic	+10.5
Manufacturing, Trading and Logistics	41.9	45.8	45.7	49.1	57.5	48.6	50.7	Basic	+2.1
Professional Services	49.5	48.0	42.9	49.0	48.4	43.5	46.0	Basic	+2.5
Retail and Tourism related	41.3	44.0	40.9	42.0	45.8	33.3	45.3	Basic	+12.0
Overall (All Business Categories)	45.6	49.3	46.9	49.6	53.3	47.0	52.8	Basic	+5.8

Regarding the index development by business category, except *Information and Communications Technology* which suffers a decline of 4.4 points, all business categories record increases at different magnitudes compared with 2023.

In particular, *Financial Services* (68.3 points) continues to be the business category with the highest index and it remains at the “Managed” cyber security readiness level.

Information and Communications Technology (58.9 points) is the only industry to have suffered a decline in its index this year (-4.4 points) and its cyber security readiness level has been downgraded from “Managed” to “Basic”.

NGOs, Schools and Others (56.4 points), *Manufacturing, Trading and Logistics* (50.7 points) and *Professional Services* (46.0 points) remain at 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. However, it is encouraging to see that it has recorded an uplift of 12.0 points this year, bringing it back from “Ad-hoc” to the “Basic” level of cyber security readiness.

3.2.3 Sub-indices

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

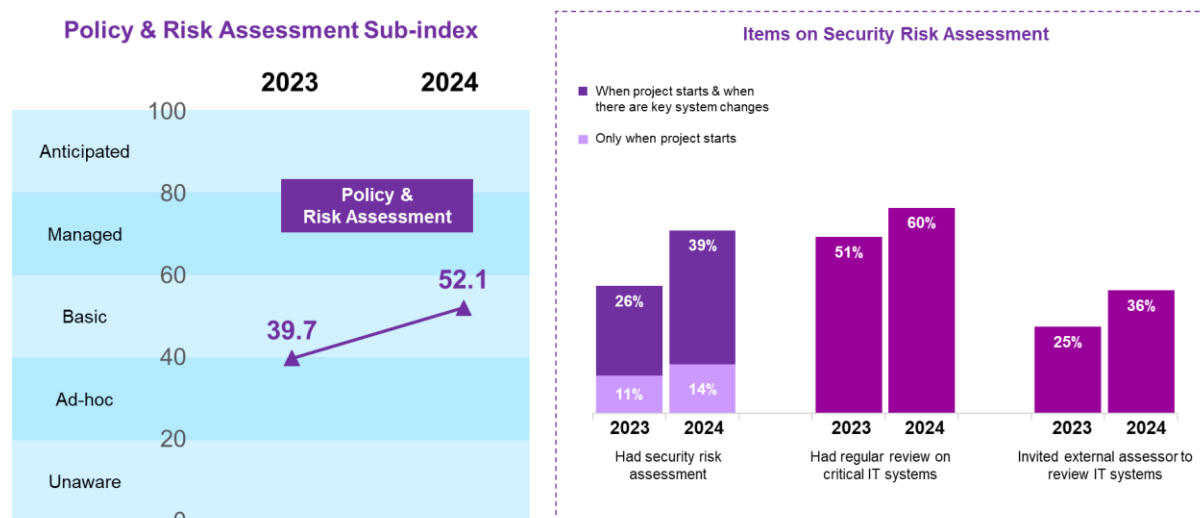
Component of Index	2018	2019	2020	2021	2022	2023	2024	YoY Change
Policy & Risk Assessment	49.4	48.5	46.1	45.5	48.6	39.7	52.1	+12.4
Technology Control	36.9	55.7	60.1	66.7	66.3	55.1	57.3	+2.2
Process Control	57.3	63.4	54.3	58.7	73.1	68.1	70.9	+2.8
Human Awareness Building	38.8	29.5	26.9	27.6	25.1	25.2	30.9	+5.7
Overall = average of sub-index scores	45.6	49.3	46.9	49.6	53.3	47.0	52.8	+5.8

From the results, all four sub-indices increase, with the “Policy & Risk Assessment” rising at a higher magnitude (+12.4 points). “Process Control” continues to lead, maintaining at “Managed” level at 70.9 points.

“Policy & Risk Assessment” and “Human Awareness Building” have shown significant improvements this year. “Policy & Risk Assessment” (52.1 points) has significantly rebounded by 12.4 points this year, returning to the “Basic” level of cyber security readiness. On the other hand, “Human Awareness Building” increases by 5.7 points to 30.9 points this year. Despite the increase, it still remains at the “Ad hoc” level of cyber security readiness.

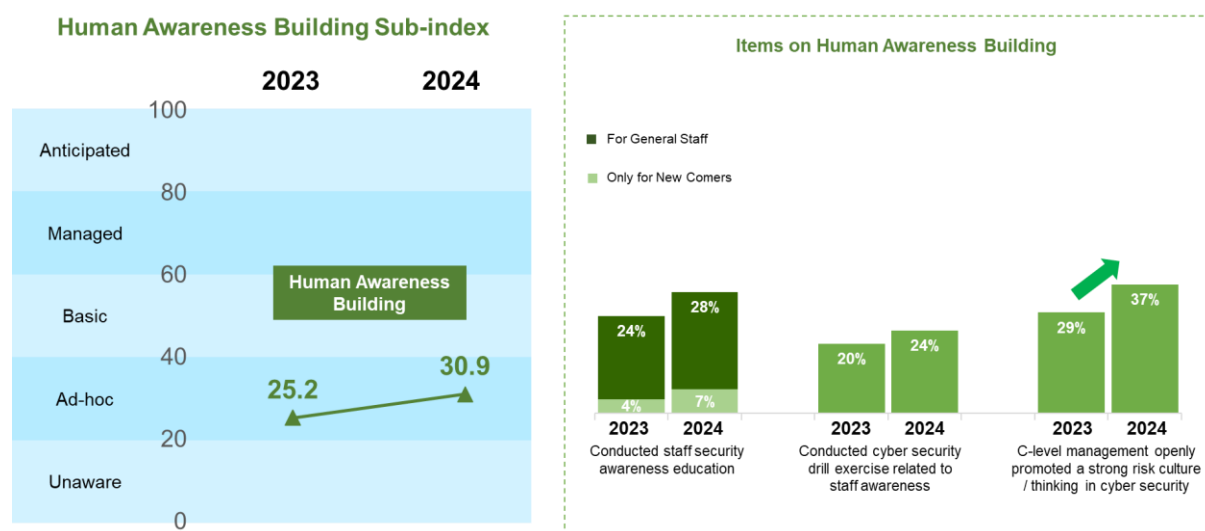
Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

Looking into the development of the components within “Policy & Risk Assessment” sub-index, some improvements are found in the adoption of all relevant measures this year, particularly for “conducting security risk assessment in the past 12 months”, with more than half of surveyed enterprises (53%) claiming to have adopted such measure, a surge of 16 percentage points compared with last year. It is also found that 6 out of 10 surveyed enterprises have conducted regular review on critical IT systems. However, only 36% of the surveyed enterprises have engaged external assessors to review their IT systems in the past 12 months, and merely 28% have conducted annual reviews of their security policies. Overall, the sub-index has consistently remained at the “Basic” level from 2018 (49.4) to 2024 (52.1).



Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

Additionally, the adoption of all relevant measures under “Human Awareness Building” sub-index improves this year. In particular, more of the C-level management are aware of the necessity of cultivating the cyber security culture, up from 29% last year to 37% this year, while those conducting staff security awareness education and cyber security drill exercise increase by 7 percentage points to 35% and by 4 percentage points to 24% respectively this year. Despite the improvement, more enterprises should conduct staff security awareness education and cyber security drill exercise.



Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

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 SMEs and Corporates.

Indicator	Average Rating (0-100)		All
	Corporates	SMEs	
1. Policy & Risk Assessment	78.0	46.4	52.1
2. Technology Control	73.6	53.7	57.3
3. Process Control	84.1	68.0	70.9
4. Human Awareness Building	56.6	25.3	30.9
Sub-index of SMEs / Corporates	73.1	48.4	52.8

Overall speaking, Corporates have across the board higher sub-index scores than SMEs. In particular, their “Process Control” sub-index (84.1 points) reaches the “Anticipated” level this year. For SMEs, “Human Awareness Building” (25.3 points) is the only sub-index which continues to remain low at the “Ad hoc” level, which warrants attention.

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

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	71.7	43.8	48.8	56.6	39.4	61.2	52.1
2. Technology Control	69.5	49.9	57.0	67.3	50.3	58.0	57.3
3. Process Control	80.8	62.6	72.6	79.2	69.3	69.1	70.9
4. Human Awareness Building	51.3	25.0	24.2	32.5	25.0	37.1	30.9
Sub-index of business category	68.3	45.3	50.7	58.9	46.0	56.4	52.8

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* enterprises have better sub-index performance across all sub-indices, whereas *Retail and Tourism* and *Professional Services* enterprises tend to have lower scores across these measures.

In terms of sub-index, “Process Control” is the control most adopted across business categories. All business categories have achieved the “Managed” level or higher in this area. Notably, *Financial Services* enterprises have even reached the “Anticipated” level.

That being said, there is still room for improvement for *Professional Services* enterprises in “Policy and Risk Assessment” (39.4), which remains at the “Ad-hoc” level this year. These enterprises should consider enhancements on their adoption of “Security Risk Assessment” and “Security Policy and Practice” so as to achieve better cyber security readiness.

Human is the last line of defence, and cyber security awareness is the key success factor for the line of human defence. However, the “Human Awareness Building” sub-index is generally low across business categories, except for *Financial Services* enterprises (51.3), which have achieved the “Basic” level. All other business categories remain at the “Ad-hoc” level, with scores ranging from 24.2 to 37.1.

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

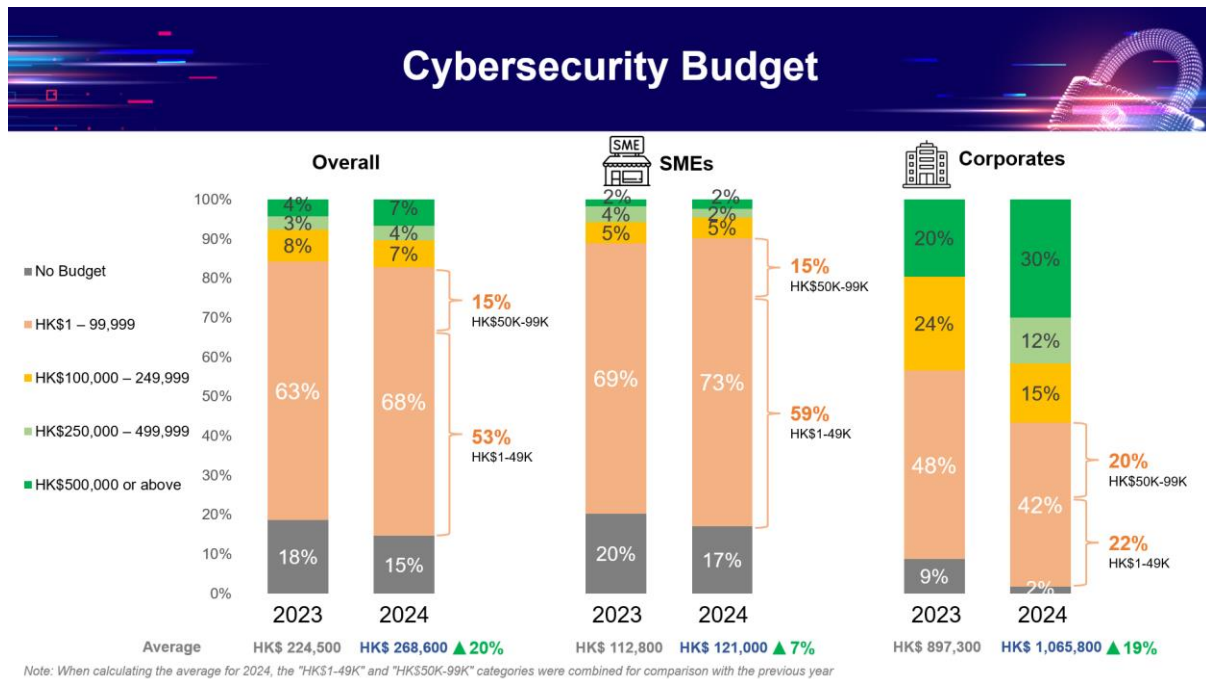
3.3 Cyber Security Investment Plans and Challenges

3.3.1 Cyber Security Budget

Compared with last year, surveyed enterprises are more willing to invest in cyber security. The average cyber security budget is around HK\$268,600 in the past 12 months, which is 20% more than last year's average budget (HK\$224,500).

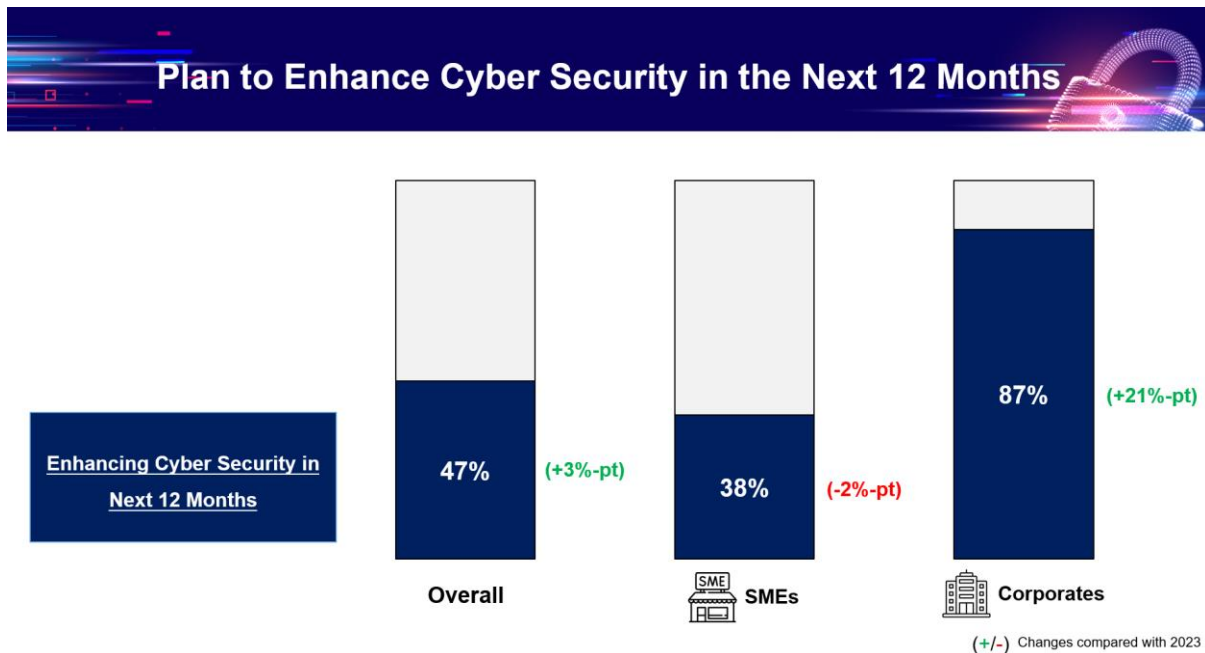
Looking at the results by company size:

- SMEs have slightly increased their cyber security spending, with a 7% rise on the average budget (HK\$121,000).
- Nearly all Corporates (98%) have invested in cyber security in the past 12 months. Their cyber security budget has increased significantly by 19%, raising the average from HK\$897,300 to around HK\$1,065,800 this year.



3.3.2 Enhancement Plans for Cyber Security

47% of surveyed enterprises have plans to enhance cyber security in the next 12 months, up by 3 percentage points compared with the results last year. Looking at the result by company size, Corporates (87%) demonstrate higher eagerness in enhancing their cyber security level, with a surge of 21 percentage points compared with last year.



In terms of business categories, more *NGOs, Schools and Others* (61%) are eager to enhance their cyber security level in the next 12 months compared with other business categories, followed by enterprises in *Financial Services* (53%) and *Information and Communications Technology* (51%). Although *Professional Services* is the business category with a lower Index this year, only 38% of them are planning to enhance cyber security.

	FS	RT	MTL	ICT	PS	NGO	All
Planning to Enhance Cyber Security in Next 12 Months	53%	44%	42%	51%	38%	61%	47%
Not Enhancing Cyber Security in Next 12 Months	47%	56%	58%	49%	62%	39%	53%

FS: Financial Services

RT: Retail and Tourism related

MTL: Manufacturing, Trading and Logistics

ICT: Information and Communications Technology

PS: Professional Services

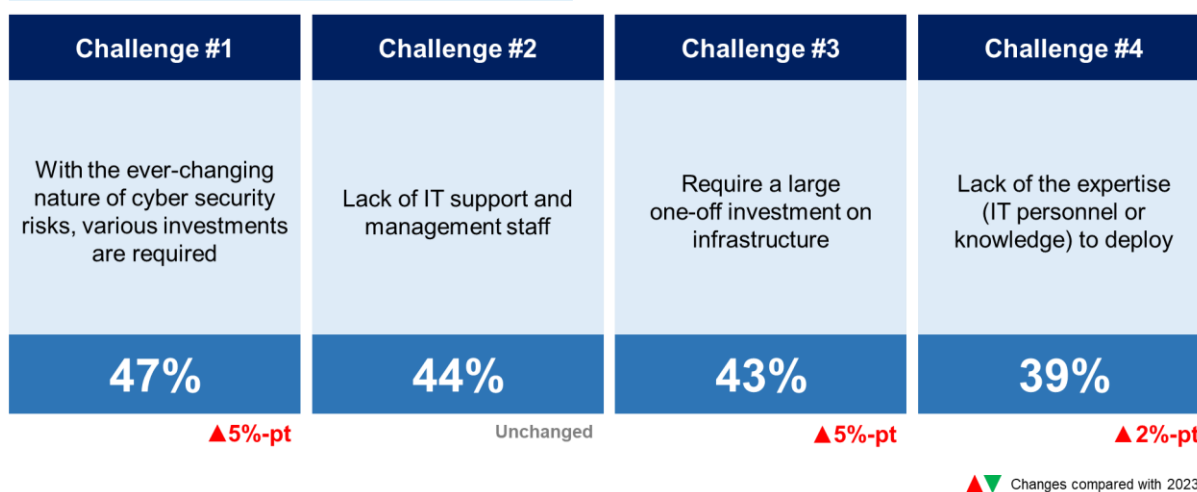
NGO: NGOs, Schools and Others

All: All Business Categories

3.3.3 Challenges of Cyber Security Management

The top four challenges of cyber security management remain the same over the years, which are mainly related to personnel and investment. In particular, “various investments required due to the ever-changing nature of cyber security” (47%) becomes the top challenge facing enterprises for the first time, followed closely by “lack of IT support and management staff” (44%), “large one-off investment on infrastructure required” (43%) and “lack of expertise (IT personnel or knowledge) to deploy” (39%).

Top 4 Challenges of Cyber Security Management



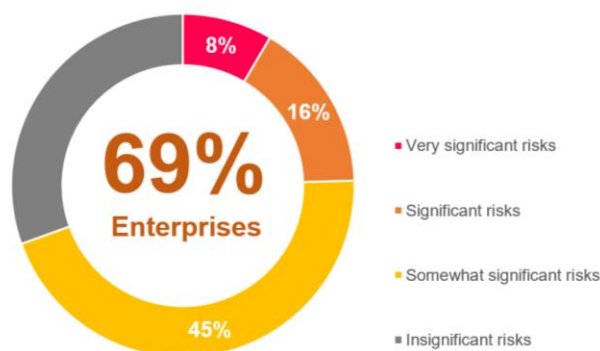
3.4 Thematic Survey of the Year: AI Security and Privacy Risks

This year's thematic survey looks into AI security and privacy risks, which covers enterprises' awareness of privacy risks involved in the use of AI technologies, their current practices in employing AI and their readiness over safe and responsible use of AI, including whether they have implemented data security measures, provided AI training to employees and formulated internal policy related to the use of AI.

3.4.1 Privacy Risks in Using AI in Operations

3.4.1.1 Perceived Level of Risk to Privacy when Using AI in Operations

Enterprises were asked to what extent they consider the use of AI in their operations poses privacy risks. The survey results reveal that a majority of enterprises (69%) consider the use of AI in their operations as posing significant privacy risks. Nearly half of the surveyed enterprises perceive the use of AI in operations as posing somewhat significant risks (45%), while 16% perceive it as posing significant risks and 8% as posing very significant risks.



Perceived the use of AI in operations will pose significant privacy risks

Base: All surveyed enterprises (excluded those answered "Don't Know") (N=436)

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

Looking into the results by business categories, more enterprises from *Financial Services* (88%) perceive the use of AI in operations poses significant privacy risks, followed by *Manufacturing, Trading and Logistics* (71%), *NGOs, Schools and Others* (71%), and *Professional Services* (68%). In contrast, over one-third of enterprises in the *Information and Communications Technology* (38%) and *Retail and Tourism* (37%) sectors believe that the privacy risks posed are insignificant.

	FS	RT	MTL	ICT	PS	NGO	All
Very significant risks	16%	4%	9%	10%	9%	7%	8%
Significant risks	27%	12%	13%	23%	15%	13%	16%
Somewhat significant risks	45%	47%	48%	29%	43%	50%	45%
Insignificant risks	13%	37%	29%	38%	32%	29%	31%

FS: Financial Services

RT: Retail and Tourism related

MTL: Manufacturing, Trading and Logistics

ICT: Information and Communications Technology

PS: Professional Services

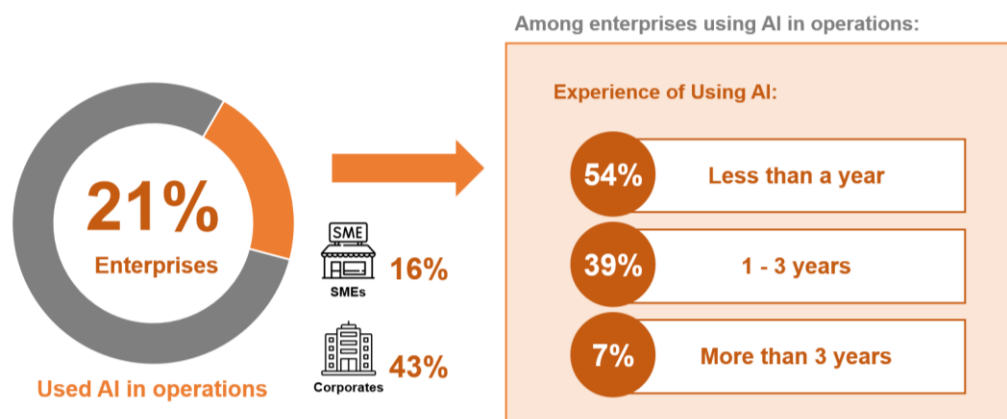
NGO: NGOs, Schools and Others

All: All Business Categories

3.4.1.2 Usage of AI Technologies

In general, around 1 in 5 (21%) of the surveyed enterprises incorporate AI technologies in their operations. Corporates (43%) have a higher rate of adopting AI technologies compared to SMEs (16%).

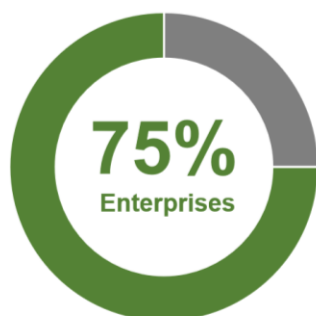
Furthermore, the surveyed enterprises have limited experience with AI. Among those enterprises which use AI, over half of them (54%) have less than a year of experience. Only 7% of surveyed enterprises have more than three years of experience with using the technology in operations.



3.4.1.3 Data Provided to Third Parties when Using AI

Three-quarters (75%) of the surveyed enterprises that use AI in their operations reported that they would not share data with third parties. Among those who would provide data to third parties, the majority provide publicly available data and anonymised and aggregated data, which generally pose fewer privacy risks. Only a limited number of enterprises would share more sensitive categories of data, such as internal operation data, personal information, customer data, and business sensitive data (ranging from 0% to 7%). This indicates that enterprises are adopting a more cautious approach to data handling and onward transmission of data.

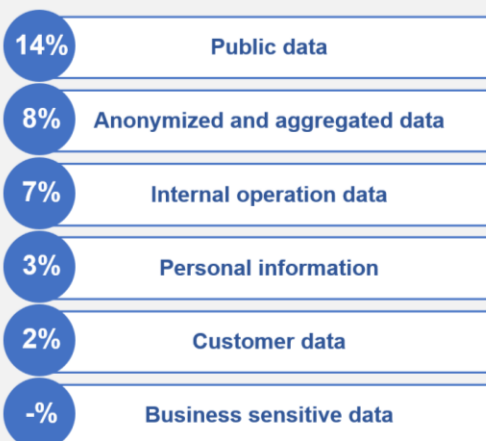
Among enterprises using AI in operations:



Would **NOT** provide data to the third parties

Base: Enterprises using AI in operations (N=92)

Data Provided to the Third Parties:



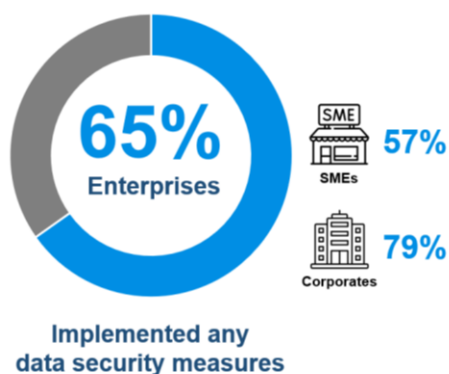
3.4.2 Current Practices in AI Security

3.4.2.1 Implementation of Data Security Measures

Among enterprises which use AI in their operations, close to two-thirds (65%) have implemented at least one data security measure. The implementation of various data security measures is significantly more common among Corporates, with close to 80% of them (79%) having implemented at least one measure. Meanwhile, 57% of the surveyed SMEs have implemented at least one measure. This reflects that Corporates place greater emphasis on ensuring data security when using AI in operations.

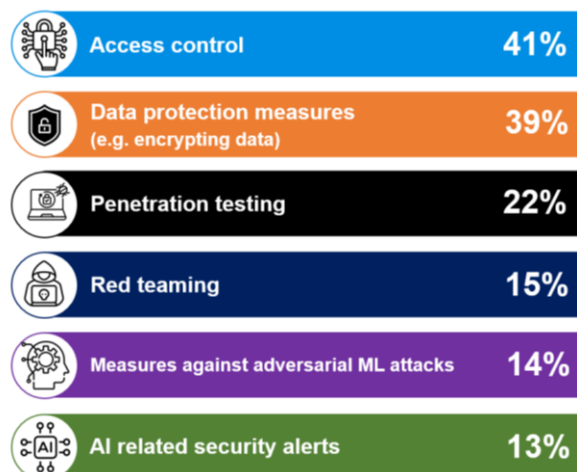
The most commonly adopted data security measures include “access control” (41%) and “data protection measures” such as data encryption and anonymisation of personal data (39%). Some enterprises also adopted other data security measures such as “penetration testing” (22%) and “red teaming” (15%). Nevertheless, fewer enterprises deployed security measures specifically designed for defending against adversarial machine learning attacks (14%) or set up AI-related security alerts (13%).

Among enterprises using AI in operations:



Base: Enterprises using AI in operations (N=92)

Data Security Measures Implemented :

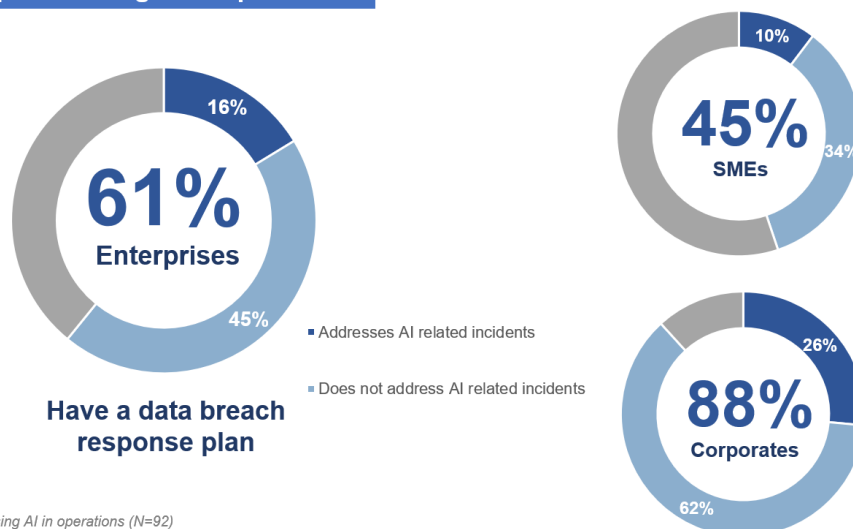


3.4.2.2 Availability of Personal Data Breach Response Plan

Enterprises were asked about the presence of a personal data breach response plan within their organisation. Among those that use AI in their operations, 61% have established such a plan. However, only 16% of the data breach response plans specifically address AI-related incidents, illustrating that many enterprises may not be prepared to handle data breach incidents involving AI. This may in turn has a more severe impact on the protection of data security and entail more complex data security issues.

Looking at the results by company size, nearly 90% of Corporates (88%) using AI in operations have established a data breach response plan, compared to only 45% of SMEs. Additionally, more than 1 in 4 Corporates (26%) have data breach response plans in place that address AI-related incidents, whereas only 10% of SMEs have such a response plan in place.

Among enterprises using AI in operations:



Base: Enterprises using AI in operations (N=92)

3.4.2.3 Availability of Training and Security Policy in relation to the Use of AI

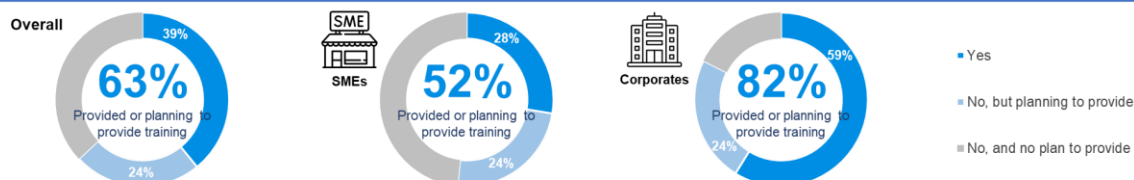
Among enterprises using AI in their operations, 63% have either provided (39%) or are planning to provide training for employees on AI (24%), while 55% have either established (28%) or are in the process of developing an AI security policy (27%). This suggests that enterprises are generally more ready to provide training on AI for employees than to formulate AI security policy.

Nonetheless, these percentages are notably lower for SMEs when compared to Corporates. Fewer SMEs are committed to providing training on AI (52% for SMEs vs. 82% for Corporates) and to developing an AI security policy (45% for SMEs vs. 74% for Corporates).

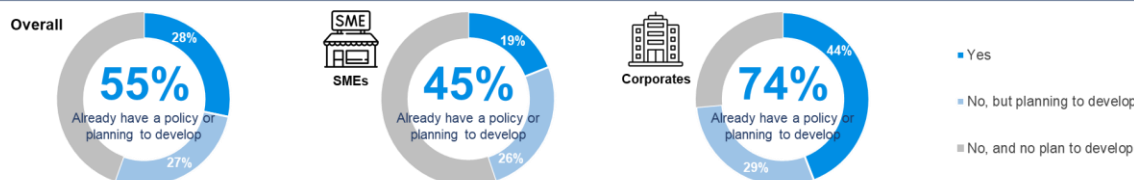
Among enterprises using AI in operations:

Base: Enterprises using AI in operations (N=92)

Provided training for employees on AI



Have an AI security policy

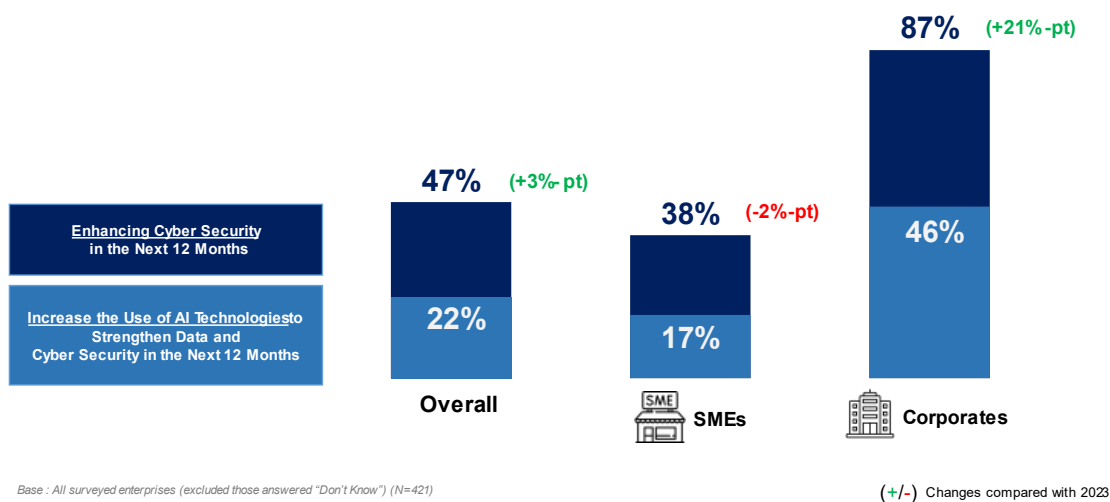


3.4.3 Enhancement Plans for Data Security and Cyber Security using AI Technologies

Almost half of the surveyed enterprises (47%) plan to enhance their cyber security in the next 12 months, with about half of them intending to increase the use of AI technologies for this purpose as well as for data security (22%), representing around one-fifth of all enterprises.

The results are encouraging as 87% of Corporates plan to strengthen their cyber security in the coming year, with almost half of them (46%) intending to implement that and enhance data security with an increase in the use of AI. The percentage of SMEs which are planning to enhance cyber security is significantly lower when compared with Corporates, with only 38% of them intending to do so, but it is noted that a similar proportion of these SMEs (17%, i.e. around half of 38%) plan to deploy AI for such purpose and enhancing data security as well.

Plan to Increase the Use of AI Technologies to Strengthen Data and Cyber Security in the Next 12 Months



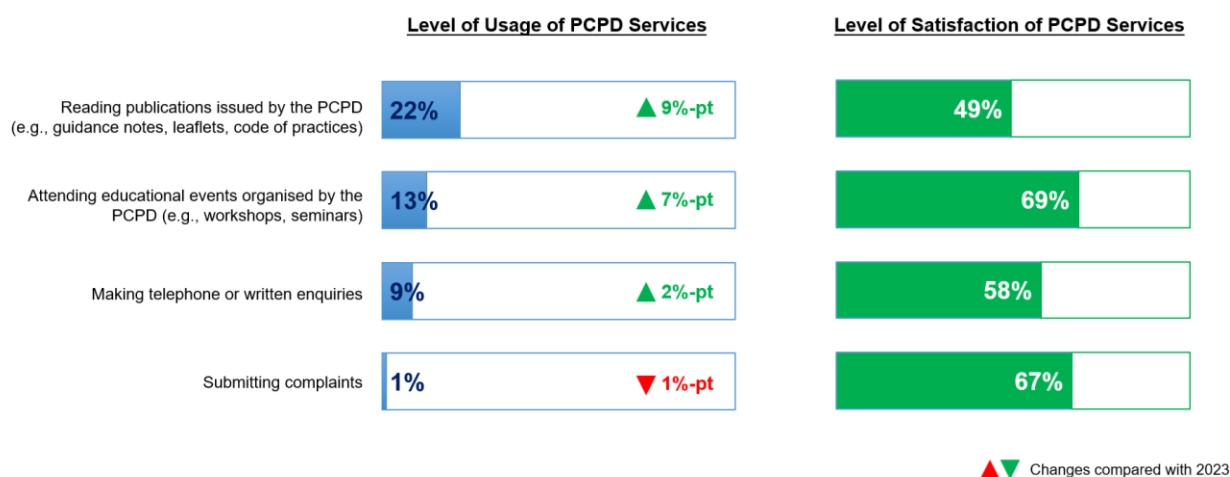
3.4.4 Usage of the PCPD’s Services and Level of Satisfaction

The thematic survey also gauged enterprises’ usage of the PCPD’s services and their level of satisfaction.

The most commonly used service of the PCPD by enterprises is reading the publications issued by the PCPD (such as guidance notes, leaflets and code of practices). This year, more than one-fifth (22%) of the surveyed enterprises have read the PCPD’s publications, representing a 9 percentage-point increase compared with last year (13%). Among these enterprises, nearly half (49%) consider that this type of services met their expectations.

Other PCPD’s services used by enterprises include participating in educational events organised by the PCPD (such as workshops and seminars) (13%), making enquiries via phone or in writing (9%), or submitting complaints (1%)². The level of satisfaction is higher among the enterprises that used these three types of the PCPD’s services, with 69%, 58% and 67% of the enterprises expressing, respectively, that they consider the services met their expectations.

Additionally, the proportion of enterprises that have participated in educational activities has doubled (13% vs. 6% in 2023). The number of enterprises that have made telephone or written enquiries rises marginally by 2 percentage points, and the number of enterprises who have submitted complaints fall by 1 percentage point.



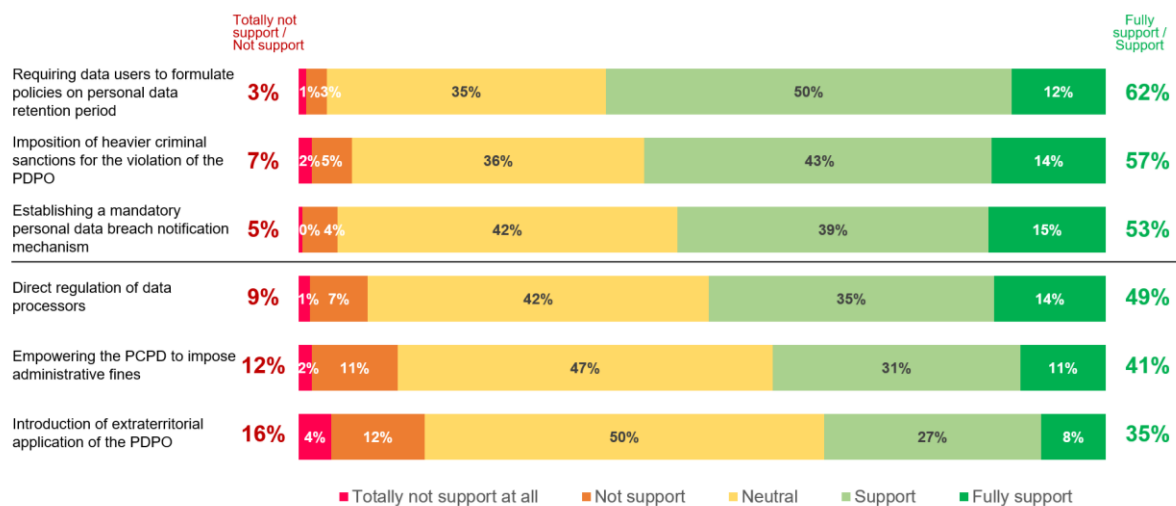
² Small base size for level of satisfaction of “submitting complaints”.

3.4.5 Level of Support towards Various Proposed Amendments to the Personal Data (Privacy) Ordinance (PDPO)

Enterprises were also asked about their 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, “Requiring data users to formulate policies on personal data retention period” is the proposed amendment which has gained the highest level of support, with 62% of the surveyed enterprises “fully supporting” or “supporting” such amendment. This is followed by “Imposition of heavier criminal sanctions for the violation of the PDPO” and “Establishing a mandatory personal data breach notification mechanism”, with 57% and 53% of enterprises indicating their support respectively. Around half of the enterprises support “direct regulation of data processors” (49%), while 41% support “empowering the PCPD to impose administrative fine”. “Introduction of extraterritorial application of the PDPO” receives the lowest level of support, with only around one-third of the enterprises (35%) stating they “fully support” or “support” the amendment.

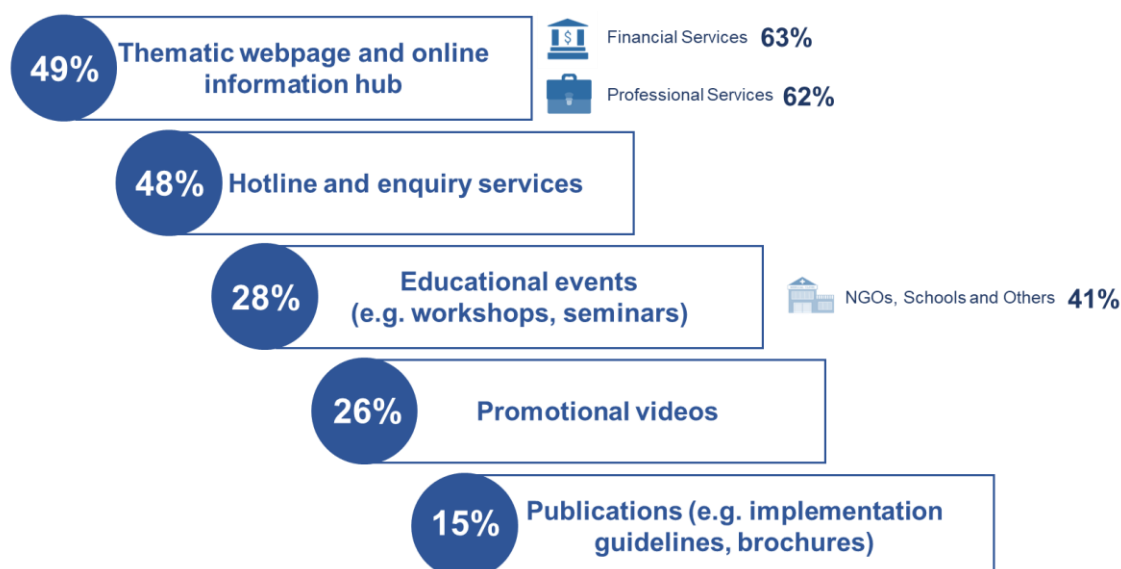
On the other hand, it is notable that a considerable proportion (ranging from 35% to 50%) of the surveyed enterprises hold a neutral stance towards each of the proposed amendments.



Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

Enterprises were also asked what types of support the PCPD should prioritise to facilitate compliance with the relevant provisions of the PDPO after they are amended. Among the options, “Thematic webpage and online information hub” (49%) and “hotline and enquiry services” (48%) are identified as the top two channels which would be the most facilitative of enterprises’ compliance with the amended PDPO, followed by “Educational events (e.g., workshops, seminars)” (28%), “Promotional videos” (26%) and “Publications (e.g., implementation guidelines, brochures)” (15%).

In particular, 63% of *Financial Services* enterprises and 62% of *Professional Services* enterprises express their preference for having “thematic webpages and online information hubs” as their primary resource for compliance, and 41% of enterprises from the *NGOs, Schools and Others* sector prefer to have access to educational events, including workshops and seminars.

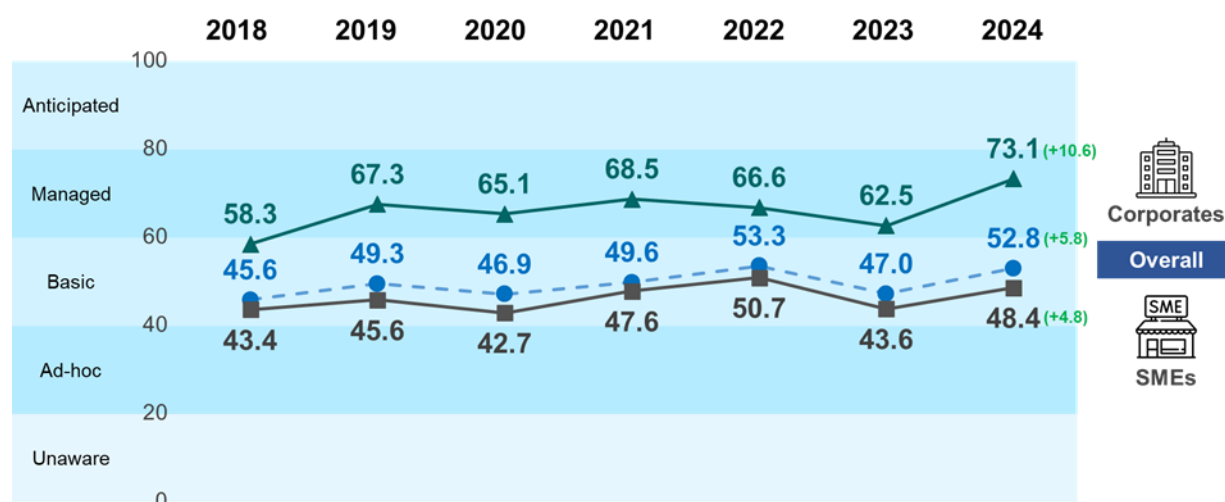


4. Summary & Recommendations

4.1 Key Findings

Hong Kong Enterprise Cyber Security Readiness Index

The overall Index increases by 5.8 points to 52.8 points, which is the largest yearly increase since the launch of the Index in 2018. The indices for both SMEs (48.4 points) and Corporates (73.1 points) increase, with Corporates' index reaching its highest level on record. However, despite the overall increase in the Index and Corporates still remaining at the “Managed” level, the cyber security readiness of SMEs still remains at the “Basic” level.



- *Financial Services* (68.3 points) continues to be the business category with the highest index, and it remains at the “Managed” cyber security readiness level.
- *Information and Communications Technology* (58.9 points) is the only industry to have suffered a decline in its index this year (-4.4 points) and its cyber security readiness level has been downgraded from “Managed” to “Basic”.
- *NGOs, Schools and Others* (56.4 points), *Manufacturing, Trading and Logistics* (50.7 points) and *Professional Services* (46.0 points) continues to stay at “Basic” level of cyber security readiness.
- *Retail and Tourism* (45.3 points) continues to be the business category with the lowest index among all business categories.

Cyber Security Attacks Encountered in the Past 12 Months

69% of the surveyed enterprises have experienced at least one type of cyber security attack in the past 12 months, which include both attacks that resulted in financial losses to the enterprise(s) concerned and those that did not. Compared with 2023, the incidence rate drops by 4 percentage points.

“Phishing attacks” continue to be the most common type of cyber security attacks, encountered by 98% of those that have experienced cyber security attacks in the past

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

12 months. “Email phishing” (79%) is still the most common type of phishing attacks, while “Smishing” (38%, +4% points) has become more common. In addition, emerging types of phishing attacks, namely “QR code phishing” and “Phishing using AI or Generative AI”, are also respectively reported by 7% and 6% of those enterprises that have encountered cyber security attacks in the past 12 months.

Ongoing Need for Enhancing Cyber Security Risk Assessment

Comprehensive policy reviews and system security assessments are also essential for enterprises to stay ahead of emerging threats and strengthen their defences against cyberattacks.

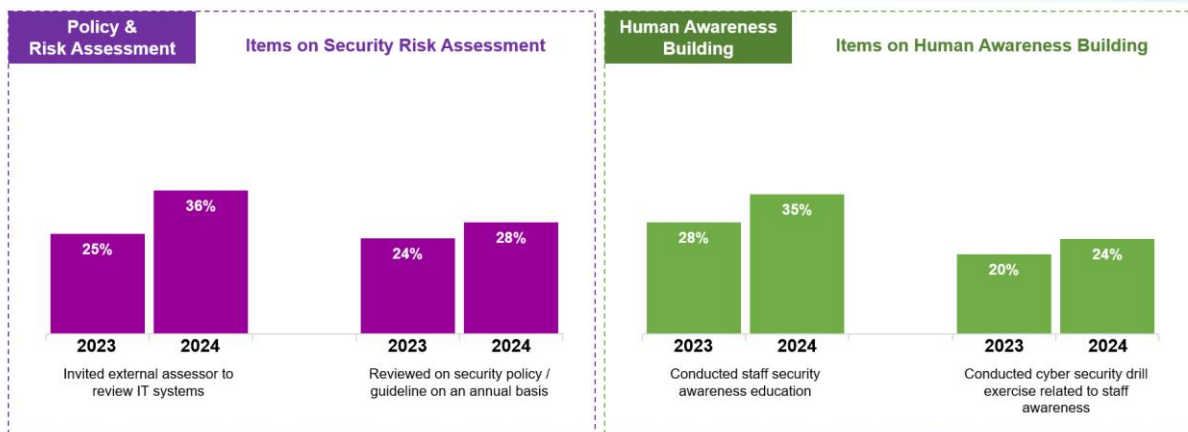
Although improvement is shown in the “Policy and Risk Assessment” sub-index this year (from 39.7 points in 2023 to 52.1 points in 2024), it has consistently remained at the “Basic” level over the years (49.4 in 2018 vs. 52.1 in 2024). Only 36% of the surveyed enterprises have engaged external assessors to review their IT systems in the past 12 months, and merely 28% have conducted annual reviews of their security policies.

A Need for Drawing Attention to Human Awareness of Cyber Security

Phishing attacks remain 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, although there has been some improvement in the “Human Awareness Building” sub-index, it remains low at 30.9 points, which is still at the “Ad hoc” level. Alarmingly, only 35% of the surveyed enterprises have conducted staff security awareness education in the past 12 months, and only 24% of the surveyed enterprises have conducted cyber security drill exercise.

Sub-indices – Improvement Areas





Perception of Privacy Risks brought by AI Technologies and Use of AI Technologies by Enterprises

The survey found that a majority of enterprises (69%) consider the use of AI in their operations poses significant privacy risks.

Regarding the usage of AI, currently around 1 in 5 (21%) of the surveyed enterprises incorporate AI technologies in their operations. Corporates (43%) have a higher rate of adopting AI technologies compared to SMEs (16%).

Among enterprises using AI in operations, three-quarters (75%) of the surveyed enterprises reported that they would not share data with third parties. Among those who would provide data to third parties, the majority provide publicly available data and anonymised and aggregated data, which generally pose fewer privacy risks. Only a limited number of enterprises would share more sensitive categories of data, such as internal operation data, personal information, customer data, and business sensitive data (ranging from 0% to 7%). This indicates that enterprises are adopting a more cautious approach to data handling and onward transmission of data.

Implementation of Data Security Measures

Among enterprises which use AI in their operations, close to two-thirds (65%) have implemented at least one data security measure. More Corporates (79%) have implemented at least one data security measure than SMEs (57%).

The most commonly adopted data security measures include “access control” (41%) and “data protection measures” such as data encryption and anonymisation of personal data (39%). Some enterprises also adopted other data security measures such as “penetration testing” (22%) and “red teaming” (15%). Nevertheless, fewer enterprises deployed security measures specifically designed for defending against adversarial machine learning attacks (14%) or set up AI-related security alerts (13%).

Availability of AI Training, AI Security Policy and Data Breach Response Plan in relation to the Use of AI

Among enterprises which use AI in their operations, 39% are currently providing employees with training on AI, while 28% have an AI security policy in place and only 16% have devised an AI-related data breach response plan.

The survey also found that the provision of training, the development of AI security policy and the establishment of personal data breach response plan in relation to the use of AI are less common among SMEs:

1. Around half (52%) of SMEs have either provided or are planning to provide training for employees on AI, but the corresponding figure is 82% among Corporates;
2. Fewer SMEs are committed to developing an AI security policy (45% for SMEs vs. 74% for Corporates); and

3. Only 10% of SMEs using AI in operations have established a data breach response plan that addresses AI-related incidents, compared to 26% of Corporates.

Enhancement Plans for Data Security and Cyber Security using AI Technologies

Almost half of the surveyed enterprises (47%) plan to enhance their cyber security in the next 12 months, with about half of them intending to increase the use of AI technologies for this purpose, as well as for data security (22%), representing around one-fifth of all enterprises.

87% of the surveyed Corporates plan to strengthen their cyber security in the coming year, with almost half of all of them (46%) intending to implement that and enhance data security with an increase in the use of AI. The percentage of SMEs which are planning to enhance cyber security is significantly lower when compared with Corporates, with only 38% of them intending to do so, but it is noted that a similar proportion of these SMEs (17%, i.e. around half of 38%) plan to deploy AI for such purpose and enhancing data security as well.

4.2 Recommendations

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

(1) Corporates Should Maintain Efforts on Cyber Security, while SMEs with Higher Risk Exposure Should Elevate Security Readiness to the “Managed” Level

The Overall Enterprise Cyber Security Readiness Index for Corporates has increased significantly, reaching a record high this year. Despite this progress, given their larger workforce and business scale, Corporates should continue to prioritise cyber security efforts and retain their “Managed” level or even to aim higher.

On the other hand, the index for SMEs has remained at the “Basic” level for several years, showing only minimal improvement. Whether SMEs should further enhance their cyber security readiness and strive for a higher level depends on their levels of risk exposure. In assessing risk exposure, various factors should be considered, such as the amount and sensitivity of the data being held or processed by the enterprises, whether the business is internet-facing (for example, operating an online store), and the potential impacts of a cyberattack on the enterprises’ operations and reputation.

Enterprises should consider stepping up their efforts to address the weaker areas, especially “Human Awareness Building”, which remains at a relatively low level of 30.9 points. “Policy & Risk Assessment” is of importance as well, as improvement in this area has been modest since the index’s inception.

To strengthen cyber security, it is suggested that organisations adopt the following cyber security measures:

- **Comprehensive scope and regular updates**
 - Expand risk assessment scope: Ensure that the risk assessment encompasses all aspects of the organisation, including IoT devices, BYOD (Bring Your Own Device), cloud services, and third-party vendors. This helps in identifying potential vulnerabilities and assessing supply chain risks.
 - Conduct regular reviews and updates: Continuously review and update risk assessments and policies to address and reflect changes in the organisation’s technology landscape, emerging threats, and regulatory requirements.
- **Adopt and adapt cyber security frameworks**
 - Implement renowned frameworks: Adopt established cyber security frameworks such as NIST, or ISO/IEC 27001. These frameworks provide structured guidelines for managing and improving security posture.

- Customise frameworks: Tailor the chosen framework to fit the specific needs and context of the organisation, ensuring it aligns with business objectives and regulatory obligations.
- **Implement a feedback loop**
 - Review and learn from incidents: After a security incident, conduct a thorough review to identify lessons learned and update policies and procedures accordingly.

(2) Raise Cyber Security Awareness through Education

Humans are always the Achilles' heel in cyber security, yet cyber security awareness education is usually not placed as a top priority until enterprises encounter cyberattacks. In this year's survey, "phishing attacks" continues to be the most common type of cyber security attacks facing enterprises, with nearly every enterprise that encountered cyber security attacks in the past 12 months having encountered this type of attack. 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, which may lead to the data on the enterprise's server being encrypted and becoming inaccessible.

As such, enterprises are advised to raise cyber security awareness through:

- Providing regular training to all general staff and newcomers; and encouraging them to undergo role-based training on Cybersec Training Hub (<https://cyberhub.hk/en/home>);
- Attending seminars organised by HKCERT and the PCPD on emerging cyber threats and risks of new technologies;
- Conducting regular phishing quiz and cyber security drill exercises, monitoring the performance, and addressing areas of weakness;
- 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 the 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);
- (For SMEs) Downloading the Incident Response Guideline for SMEs (<https://www.hkcert.org/security-guideline/incident-response-guideline-for-smes>) on the actions and procedures to prevent and handle cyber security attacks;
- Referring to the guidelines published by the PCPD, including the "Guidance on Data Breach Handling and Data Breach Notifications" (https://www.pcpd.org.hk/english/resources_centre/publications/files/gu

[idance_note_dbn_e.pdf](#)) and the “Guidance Note on Data Security Measures for Information and Communications Technology” (https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_datasecurity_e.pdf).

To strengthen the capabilities of schools, NGOs and SMEs in safeguarding data security and cyber security, the PCPD launched the “Data Security” Package in October 2024 wherein participating organisations will receive free quotas to join professional workshops and seminars organised by the PCPD upon completion of an assessment by the “Data Security Scanner” on the adequacy of the data security measures adopted.

(3) Improve Policy Review and System Security Assessment

To stay ahead of emerging threats, enterprises should take a proactive approach by regularly reviewing their security policies and guidelines, and conducting comprehensive system security assessments. It is recommended that enterprises take the following steps:

- **Annual policy review:** Enterprises should review their internal policies and guidelines at least once a year to ensure that the organisation remains vigilant and prepared against evolving threats such as phishing, ransomware and other kinds of cyberattacks. By keeping abreast with the latest security trends and best practices, enterprises can identify gaps in their existing policies and make necessary adjustments to address new vulnerabilities.
- **Utilise third-party system security risk assessment services:** As independent security risk assessments can provide an unbiased evaluation of the organisation’s security posture and help identify vulnerabilities that internal teams might overlook, enterprises should consider employing third-party system security risk assessment services. It is particularly important to prioritise assessments for internet-facing systems or services, as these are more exposed to external threats and are often the primary targets for cyberattacks.

(4) Adopt AI Technologies in a Safe, Responsible and Privacy-friendly manner

With the anticipated increase in the usage of AI, it is imperative for enterprises to ensure the safe and responsible deployment of AI to address and mitigate its inherent risks, including personal data privacy risks. Currently, while 65% of the enterprises that use AI technologies have implemented data security measures, less than half have an AI security policy in place, provide employees with training on AI and have devised an AI-related data breach response plan. Therefore, enterprises are strongly urged to take appropriate actions to address the gaps and prevent the privacy risks arising from the use of AI technologies.

With a view to adopting the AI technology in a safe, responsible and privacy-friendly manner, it is recommended that enterprises should enhance AI security

through the following means:

- **Leveraging AI technology to detect and identify cyber security threats and automate response:**
 - Detection – AI can continuously monitor systems and networks to identify unusual patterns or behaviours that may indicate a security threat, such as unauthorised access attempts, unusual data transfers, or irregular login times. AI algorithms can also analyse vast amounts of data in real-time, allowing potential threats to be immediately detected as they occur;
 - Identification – AI can help classify threats based on their severity and potential impact, assist security teams in prioritising their responses based on the severity and impact. By identifying the nature and severity of threats at an early stage, enterprises can allocate resources more effectively to nip potential threats in the bud; and
 - Automate response – AI can help automate initial response to detected threats by taking actions such as isolating affected systems, blocking malicious IP addresses, and/or terminating suspicious processes, to contain threats quickly to reduce potential damage and minimise disruption.
- **Implementing adequate measures to protect data security of AI systems:** Implementing data security measures such as setting up access control, conducting red teaming, adopting data protection measures (e.g. encryption of data and anonymisation of data), adopting measures against adversarial Machine Learning attacks, carrying out penetration tests, and setting up AI-related security alerts. The adoption of adequate measures could help safeguard AI systems from cyberattacks to ensure the security of data (including personal data) and mitigate the risks of data leakage.
- **Formulating comprehensive policies that enhance AI security** by incorporating internationally-recognised best practices to ensure data security throughout the AI lifecycle when devising their AI security policies. Enterprises may consider, for example, adopting international standards and guidelines developed and published by professional associations such as the International Organization for Standardization.
- **Developing an AI Incident Response Plan:** Set up a comprehensive plan with reference to the PCPD’s recommendations in “Artificial Intelligence: Model Personal Data Protection Framework” (“PCPD’s Model Framework”). It is recommended in the PCPD’s Model Framework that a contingency plan specific to AI incidents, namely, an AI Incident Response Plan, be developed to monitor and address incidents that may inadvertently occur. The plan may encompass elements such as defining, monitoring, reporting, containing, investigating and recovering from an AI-related incident. Enterprises should also establish a data breach response plan which addresses AI-related incidents, in case a data breach incident occurs as part of an AI incident.

- **Providing adequate training on AI for employees:** Provide adequate training to employees to ensure they have the appropriate knowledge, skills and awareness to facilitate enterprises to properly apply AI-related policies, as well as to foster a culture of responsible use of AI. Given the diverse nature of enterprises in operations, a one-size-fits-all approach to training may not be ideal. It is therefore recommended that the training should be role-based, meaning that, depending on the nature of operations of the enterprise, tailored training contents to the specific needs and responsibilities should be offered to different personnel within an enterprise to ensure that each employee receives the most relevant and applicable training based on their interaction with AI in their respective roles.

- End of Report -

Hong Kong Enterprise Cyber Security Readiness Index and AI Security Survey 2024

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. As a nationwide leader in innovative, market-driven research and development (R&D), specialising in leading technologies and all-rounded manufacturing services, HKPC promotes new industrialisation in Hong Kong and the Greater Bay Area and facilitates the development of new productive forces, leveraging innovation and technology (I&T), as well as bolstering Hong Kong to be an international innovation and technology centre 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, and strengthens talent nurturing and Hong Kong's competitiveness with FutureSkills training for enterprises and academia to enhance 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

The content and data in this report is co-owned by Hong Kong Productivity Council (HKPC) and PCPD. The content of this report is provided under the Creative Commons Attribution 4.0 International License, or "CC BY 4.0" (<https://creativecommons.org/licenses/by/4.0>). You may share and adapt the content for any purpose, provided that you attribute the work to HKPC and PCPD.

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.

© Hong Kong Productivity Council. All rights reserved.

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