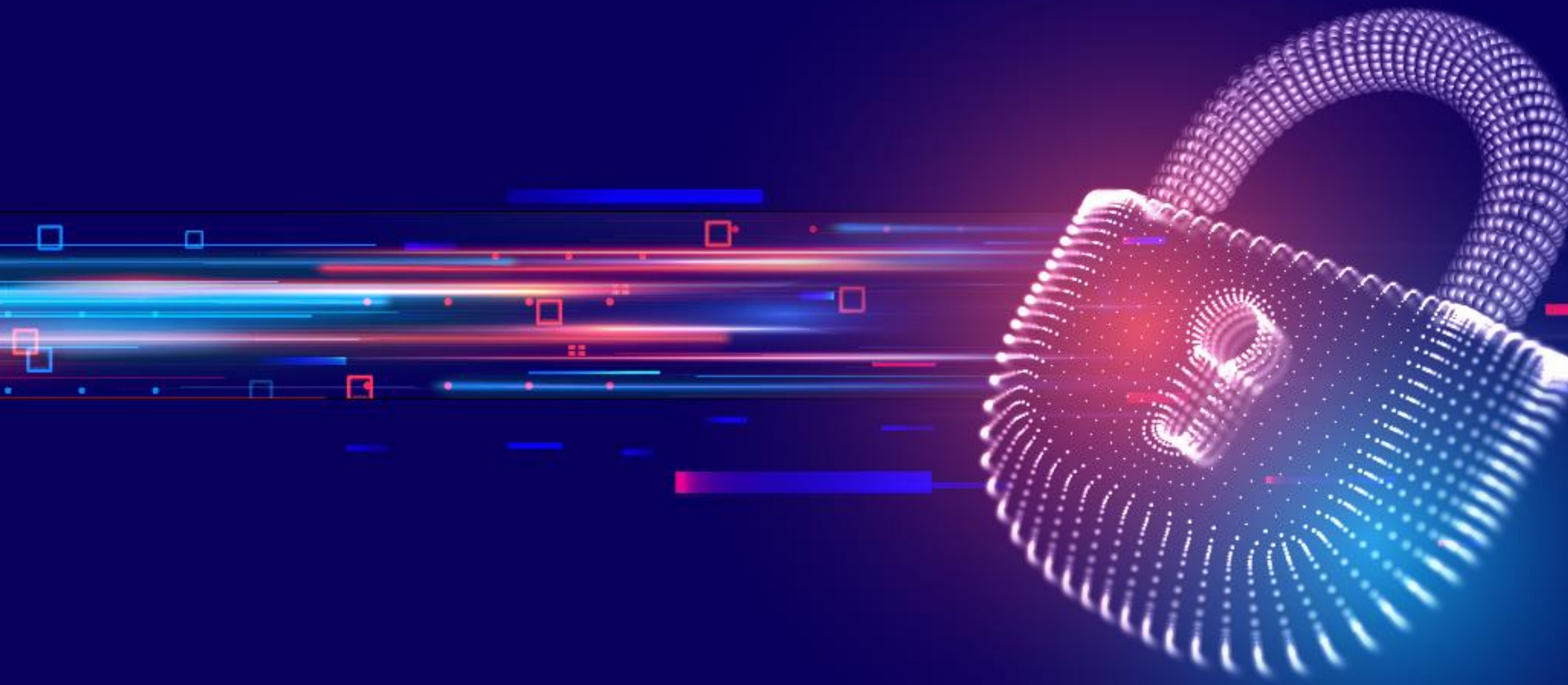
Organised by
主辦機構

Supported by
支持機構

Sponsored by
贊助機構

# HKT Hong Kong Enterprise Cyber Security Readiness Index 2022



## 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 inter-connected 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 impact and damage.

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 living 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 have to be made to regularly monitor the status of cyber security readiness and ensure it can keep up with technological change.

## 1.2 HKT Hong Kong Enterprise Cyber Security Readiness Index 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, 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 2022, HKPC conducted the fifth round of survey using this framework with the sponsorship of HKT and the support of Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), named **HKT Hong Kong Enterprise Cyber Security Readiness Index** (the Index) to reflect this collaboration. The methodology of the survey, the design of questionnaire and the execution of the interviews were decided and conducted by HKPC independently.

## 1.3 Thematic Survey of the Year

In addition to the Index, this annual survey also picks one special topic for in-depth understanding. For 2022, the chosen special topic continued to be “Managed Security Services” (MSS).

MSS is an outsourcing model of security expertise. With the growing success of cloud computing as the forerunner of IT infrastructure and application outsourcing, more people are looking into outsourcing their security management. An all-round MSS provider aims at helping enterprises to assess, mitigate and prevent the threats of cyber-attacks. It offers all levels of enterprise network security services, ranging from designing security policies and measures, conducting security tests, to integrating security solutions and providing secure broadband connectivity, so as to meet the demands from customers ranging from Small-Medium Enterprises (SMEs) to the most demanding multinational companies.

Hence, it is worthwhile to study the status of demand and current deployment of MSS among Hong Kong enterprises and its upcoming trend.

## 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 study in details;
- Chapter 3 presents the survey findings; and
- Chapter 4 lays out the conclusions and recommendations based on the findings illustrated in Chapter 3.

# 2. Methodology

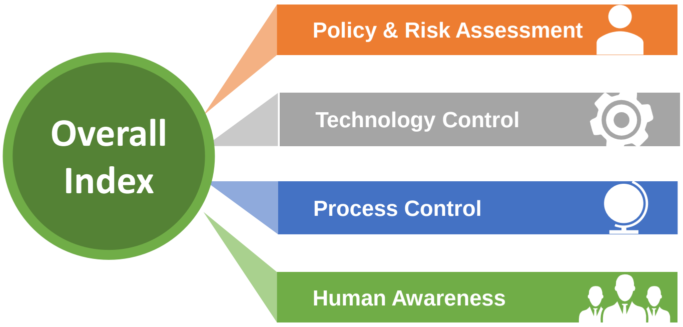
## 2.1 Framework of the Index

The Index is constructed by assessing the comprehensiveness of security measures of the surveyed enterprises in four key areas: Policy and Risk Assessment, Technology Control, Process Control and Human Awareness. 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 in scores based on the comprehensiveness level.

**Components of the Index**

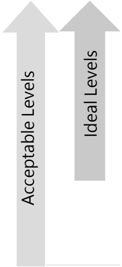
The Index is composed of sub-indices from four aspects:

- 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. In the range of 0 to 100, the higher the Index, the better resistance and survivability to cyber security risks.



| Level | Index Score (0-100) | Description |
|---|---|---|
| Anticipated | 80 – 100<br>★★ | Proactive and aware of emerging threats |
| Managed | 60 – 79<br>★ | 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 2022, the survey collected the data through telephone interviews with no less than 350 enterprises, with at least 50 of them being Large Enterprises[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 Communication Technology;
5. Professional Services; and
6. Non-Government Organisation (NGOs), Schools and Others.

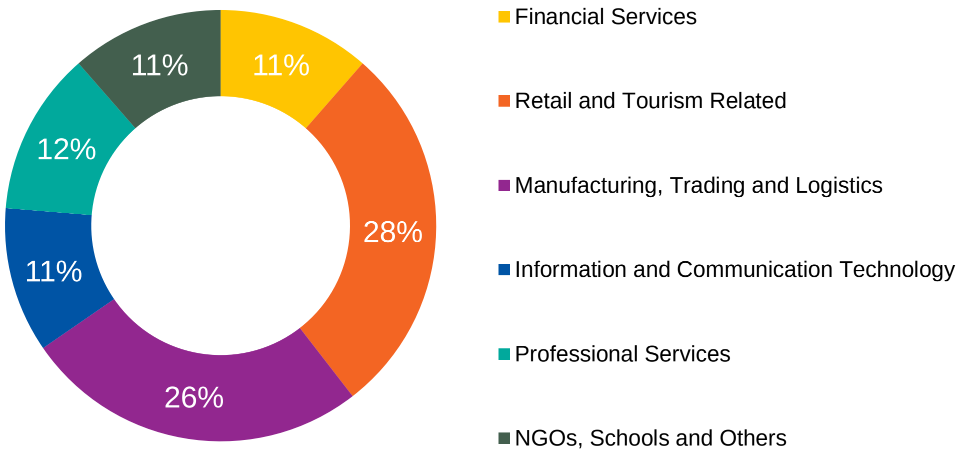
[1] Large Enterprises are "Manufacturing establishments with more than 100 employees; or non-manufacturing establishments with more than 50 employees". https://www.success.tid.gov.hk/english/aboutus/sme/service_detail_6863.html

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 Communication Technology | Information and Communication 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 367 companies in Hong Kong. As shown in the below figure, at least 11% of responses were collected for each business category, with 28% from "Retail and Tourism Related" and 26% from "Manufacturing, Trading and Logistics", considering the larger numbers of establishments in these categories.



Among the 367 surveyed enterprises, 308 of them were SMEs and 59 of them were Large Enterprises.

308
SMEs

59
Large Enterprises

The breakdown of sample by business category within SMEs and Large Enterprises is summarised in the table below:

| | SMEs | | Large Enterprises | | Total | |
|---|---|---|---|---|---|---|
| | n | % | n | % | n | % |
| *Financial Services* | 35 | 11% | 7 | 12% | 42 | 11% |
| *Retail and Tourism related* | 86 | 28% | 17 | 29% | 103 | 28% |
| *Manufacturing, Trading and Logistics* | 79 | 26% | 16 | 27% | 95 | 26% |
| *Information and Communication Technology* | 35 | 11% | 5 | 8% | 40 | 11% |
| *Professional Services* | 38 | 12% | 7 | 12% | 45 | 12% |
| *NGO, Schools and Others* | 35 | 11% | 7 | 12% | 42 | 11% |
| ***All Business Categories*** | **308** | **100%** | **59** | **100%** | **367** | **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. Thematic Survey of the Year: MSS
4. Investment Plans in the Next 12 Months

The survey successfully collected the opinions from 367 enterprises - 308 SMEs and 59 Large Enterprises 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 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 – 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) |
|---|---|---|---|---|---|---|
| **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 3.9. However, such score is slightly down by 0.2 compared with 2021.

Similar findings are also observed looking at the detailed breakdown of the results. In 2022, close to 9 out of 10 surveyed enterprises (88%) consider IT systems and data "important" or above, which is down by 7%-points from 95% in 2021. Over one-third (36%) consider IT systems and data "extremely important", but the corresponding figure was 48% in 2021.

By company size, Large Enterprises (4.4) consider IT systems and data more important than SMEs (3.8).

| Company Size | Average score (1 – 5 marks) |
|---|---|
| SMEs | 3.8 |
| Large Enterprises | 4.4 |

Looking into the results by business categories, *Information and Communication Technology* continues to have the highest perceived importance of IT systems and data with an average score of 4.3, followed by *Financial Services* (4.2), *NGOs, Schools and Others* (4.0), *Manufacturing, Trading and Logistics* (3.8), and *Professional Services* (3.7). *Retail and Tourism* continues to have the lowest perceived importance score of 3.6, with the highest proportion of enterprises considering IT systems and data "somewhat important" or "not that important" (18%).

| 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 Communication Technology** | 5% | -- | 13% | 30% | 53% | **4.3** |
| **Financial Services** | -- | -- | 29% | 19% | 52% | **4.2** |
| **NGOs, Schools and Others** | 2% | 12% | 12% | 29% | 45% | **4.0** |
| **Manufacturing, Trading and Logistics** | 3% | 9% | 20% | 36% | 32% | **3.8** |
| **Professional Services** | 7% | 9% | 27% | 20% | 38% | **3.7** |
| **Retail and Tourism related** | 6% | 12% | 27% | 32% | 23% | **3.6** |

Note: "--" denotes 0%

### 3.1.2 Level of Confidence towards the Cyber Security Level

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

| 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 Communication Technology** | -- | -- | 18% | 53% | 30% | **4.1** |
| **Financial Services** | -- | 2% | 21% | 38% | 38% | **4.1** |
| **NGOs, Schools and Others** | 2% | 2% | 29% | 50% | 17% | **3.8** |
| **Manufacturing, Trading and Logistics** | 1% | 5% | 27% | 54% | 13% | **3.7** |
| **Retail and Tourism related** | 1% | 3% | 35% | 47% | 15% | **3.7** |
| **Professional Services** | 2% | 2% | 47% | 42% | 7% | **3.5** |
| **Overall** | **1%** | **3%** | **30%** | **48%** | **18%** | **3.8** |

Note: "--" denotes 0%

In general, surveyed enterprises are relatively confident in their cyber security level, with an average score of 3.8. Two-thirds (66%) of them are "confident" or "extremely confident" in their cyber security level.

Consistently, *Information and Communication Technology* and *Financial Services* rank top with an average score of 4.1; and 83% and 76% are "confident" or "extremely confident" in their cyber security level respectively. On the other hand, *Professional Services* are less confident compared with other business categories, with an average score of 3.5. Less than half of the enterprises in this business category are "confident" or "extremely confident" in their cyber security level.

Again, compared with SMEs (3.7), Large Enterprises (4.2) are more confident in their cyber security level.

| Company Size | Average score (1 – 5 marks) |
|---|---|
| SMEs | 3.7 |
| Large Enterprises | 4.2 |

### 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. contact details, credits, intellectual properties)
- System Data (e.g. control data, system log, system configuration, access records)
- Compliance / Regulated Data (e.g. General Data Protection Regulations, Personal Data Privacy Ordinance, Securities and Futures Ordinance)
- Other Sensitive Data (e.g. patient data)

Surveyed enterprises store 1.6 types of data on average, and Large Enterprises store more types of data (2.0) than SMEs (1.5). It is also found that *Professional Services* (1.4), *Retail and Tourism* (1.5) and *Manufacturing, Trading and Logistics* (1.5) store less types of data compared with other business categories.

**Type of Data Stored in the Network**

| | Overall | Large Enterprise | SMEs | Financial Services | Retail and Tourism Related | Manufacturing, Trading and Logistics | Information and Communication Technology | Professional Services | NGOs, Schools and Others |
|---|---|---|---|---|---|---|---|---|---|
| *Base* | *367* | *59* | *308* | *42* | *103* | *95* | *40* | *45* | *42* |
| **System data** | 55% | ② 59% | ① 54% | ① 57% | ① 55% | ① 60% | ① 68% | ② 42% | 40% |
| **Business sensitive data** | 49% | ① 73% | ② 44% | ③ 52% | ② 48% | ② 48% | ② 53% | ① 49% | ① 48% |
| **Compliance / Regulated data** | 31% | ③ 37% | ③ 29% | ① 57% | 20% | ③ 23% | 30% | ③ 29% | ① 48% |
| **Personal sensitive data** | 28% | 31% | 27% | 29% | ③ 29% | 18% | ③ 38% | 18% | ③ 45% |
| ***Average*** | *1.6* | *2.0* | *1.5* | *2.0* | *1.5* | *1.5* | *1.9* | *1.4* | *1.8* |

In terms of the types of data stored, over half of the SMEs and Large Enterprises store "System data", and significantly more Large Enterprises (73%) store "Business sensitive data" than SMEs (44%).

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 and *NGOs, Schools and Others*, while more *Information and Communication Technology* enterprises and *NGOs, Schools and Others* store "Personal sensitive data". On the other hand, less than half of the enterprises in *Professional Services* (42%) and *NGOs, Schools and Others* (40%) keep "System data", much lower compared with other business categories (ranging from 55% to 68%).

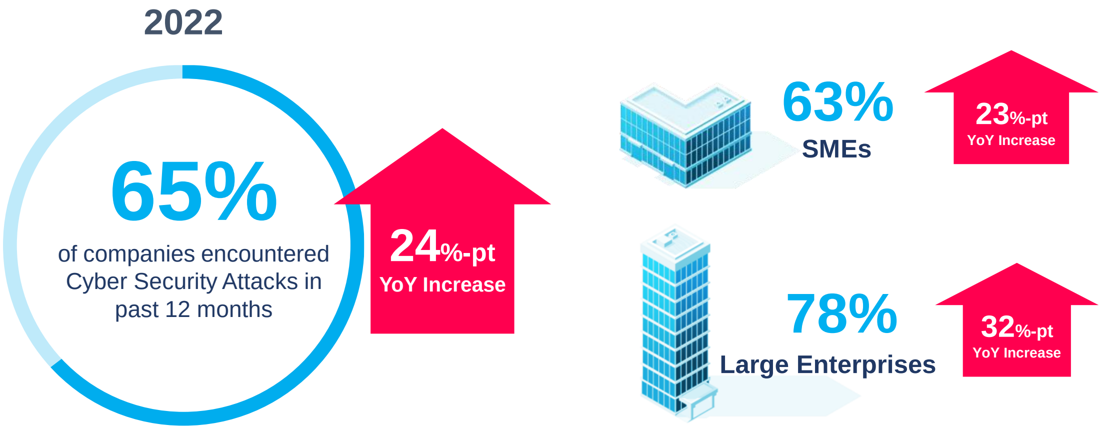
## 3.1.4 Cyber Security Attacks Experienced in the Past 12 Months

### 3.1.4.1 Incidence of Cyber Security Attacks in Past 12 Months

65% of the surveyed enterprises have experienced any types of cyber security attacks in the past 12 months, regardless of whether such attacks caused financial losses to the enterprise(s) concerned or not. Compared with 2021, the incidence rate uplifted significantly by 24%-points.

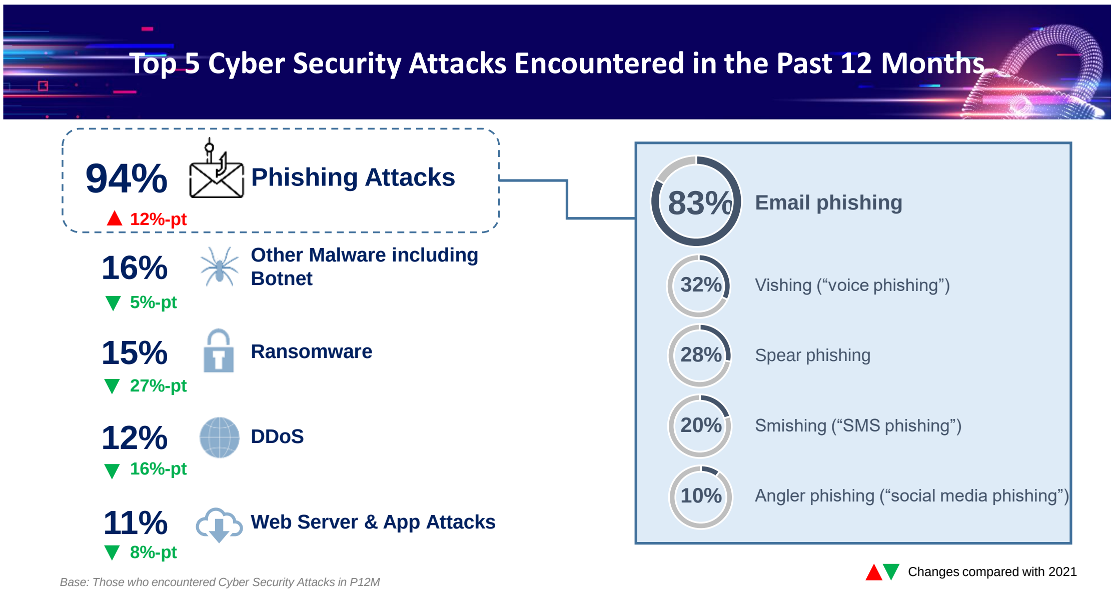
Increased incidence of cyber security attacks is observed across both SMEs (63%) and Large Enterprises (78%), with uplifts of 23%-points and 32%-points respectively.

**Overall Incidence of Cyber Security Attacks**



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
- Corporate Espionage
- Phishing attacks
  - Phishing email
  - Spear phishing
  - Vishing (Voice phishing)
  - Smishing (SMS phishing)
  - Angler phishing (Social media phishing)
- DDoS (Distributed Denial of Service)
- Web server & App attacks
- Attack on other services like POS (Point of Sale) / remote access / CCTV (Closed-circuit television)
- Hacking targeting corporate service accounts
- Loss of equipment (e.g. laptop, USB)
- Abuse of usage
- Data / Credential leakage
- Inside threat
- Others



Top 5 Cyber Security Attacks Encountered in the Past 12 Months

94% Phishing Attacks ▲ 12%-pt

16% Other Malware including Botnet ▼ 5%-pt

15% Ransomware ▼ 27%-pt

12% DDoS ▼ 16%-pt

11% Web Server & App Attacks ▼ 8%-pt

83% Email phishing

32% Vishing ("voice phishing")

28% Spear phishing

20% Smishing ("SMS phishing")

10% Angler phishing ("social media phishing")

*Base: Those who encountered Cyber Security Attacks in P12M*

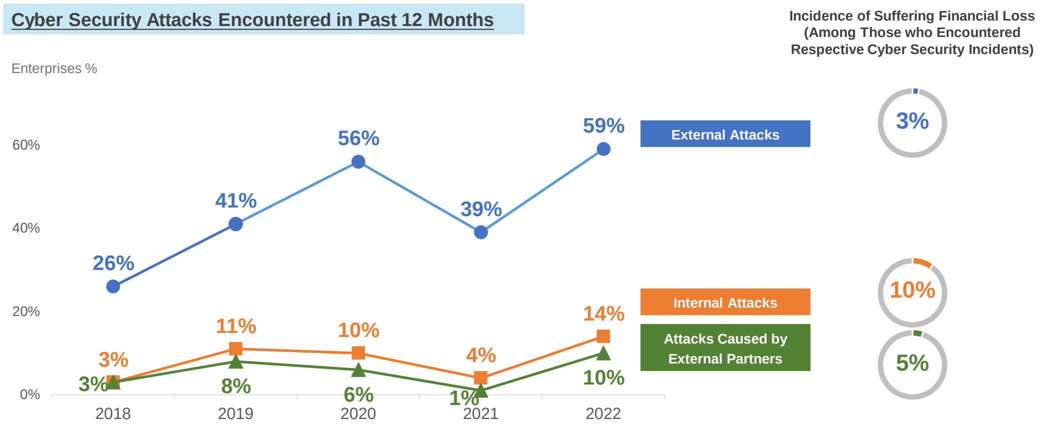
▲▼ Changes compared with 2021

"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 (94%) of the enterprises during the reference period, a significant rise of 12%-points compared with 2021. In particular, "email phishing" (83%) is the most common type of "phishing attacks", while "Vishing" (32%) and "Spear phishing" (28%) are other emerging types of phishing attacks.

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” (16%), “Ransomware” (15%), “DDoS” (12%) and “web server and app attacks” (11%), but the incidence rates are lower than last year.

### 3.1.4.2 External and Internal Attacks Experienced and Financial Loss

Surveyed enterprises encountering any cyber security attacks over the past 12 months were also asked each of the cyber security attacks they have encountered were caused by external attacks, internal attacks, and / or attacks caused by external parties; as well as whether such attacks had caused any financial losses to them.



External attack continued to be the most common type of cyber security attacks encountered by enterprises, with around 6 out of 10 surveyed enterprises had such encounter over the past 12 months.

Although occurrence of internal attacks and attacks caused by external partners were significantly lower than external attacks, still 14% and 10% of the surveyed enterprises have encountered each type of these cyber security attacks respectively.

However, it is worth to note that the incidence rates of external attacks, internal attacks and attacks caused by external partners recorded rebound this year and reached new peaks.

In this year, surveyed enterprises encountering respective type of cyber security attacks were asked if they suffered financial loss due to such encounter. In particular, although the occurrence of internal attacks was low (14%), 1 in 10 attacks could successfully cause financial loss to the enterprise concerned.

## 3.2 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 2022 are listed in the table below:

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

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:<br>* Review critical IT systems regularly<br>* Assess security risks of non-IT projects<br>* 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:<br>* Have a security policy / guideline to classify data according to sensitivity<br>* Have a security / guideline on the responsibility of security attack response<br>* Review or update on security policy / guideline | |
| **2.1 Cyber Threats Detection** | None | | +1 for each of the following, max. 4 marks:<br>* Normal firewall and antivirus<br>* Application Firewall<br>* IDS / IPS<br>* Two-factor/Multi-factor Authentication<br>* Cloud Security Technology<br>* Backup and Recovery solution<br>* Endpoint Detection & Response (EDR)<br>* Has consolidated system event logs of multiple systems<br>* Vulnerability scanning and fixing<br>* Acquired threat intelligence<br>* Network Access configuration<br>* Access Control solution<br>* Security control monitoring solution<br>* Shared threat intelligence with other parties<br>* Other relevant ones | | |

| 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** |
| **2.2 Patch Management** | None | Occasionally when some people told to do | It is done regularly | +1 for each of the following:<br>* Have a central patch management<br>* Verify and test the patch before deploying in production environment<br>* 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:<br>* Turn on logging / alert for errors for systems<br>* Do regular scanning to detect system vulnerabilities | |
| **3.1 Privileged Access Management** | None | Yes | Record in access log | * Review access log when needed (+1)/ Regular review of access log (+2)<br>* Deploy any privileged access management system (+1) | |
| **3.2 Data Backup Management** | None | Yes, but not regularly | Yes, at least weekly | +1 for each of the following:<br>* Keep offline/offsite copy<br>* Conduct recovery drill exercise<br>* 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:

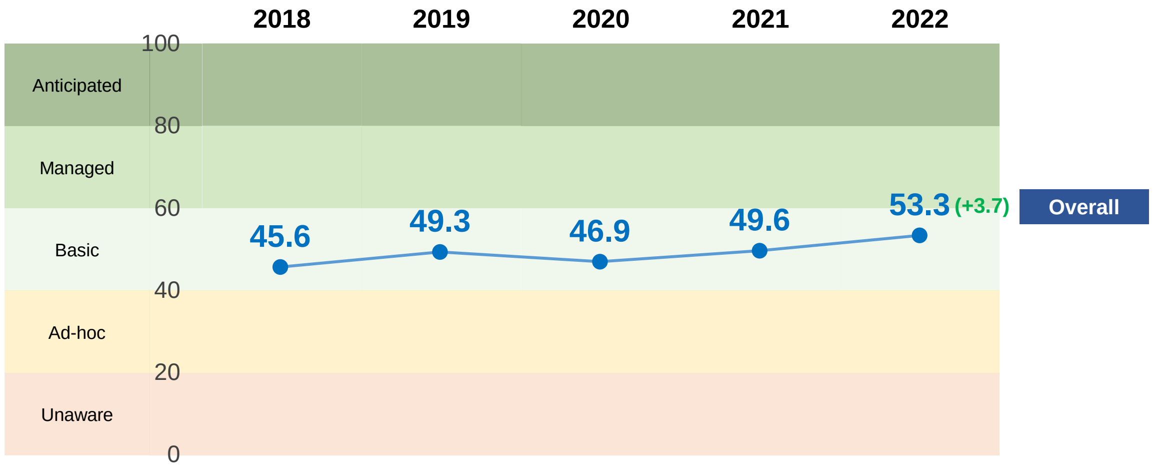
Overall Index = Average of Sub-Indices

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 |

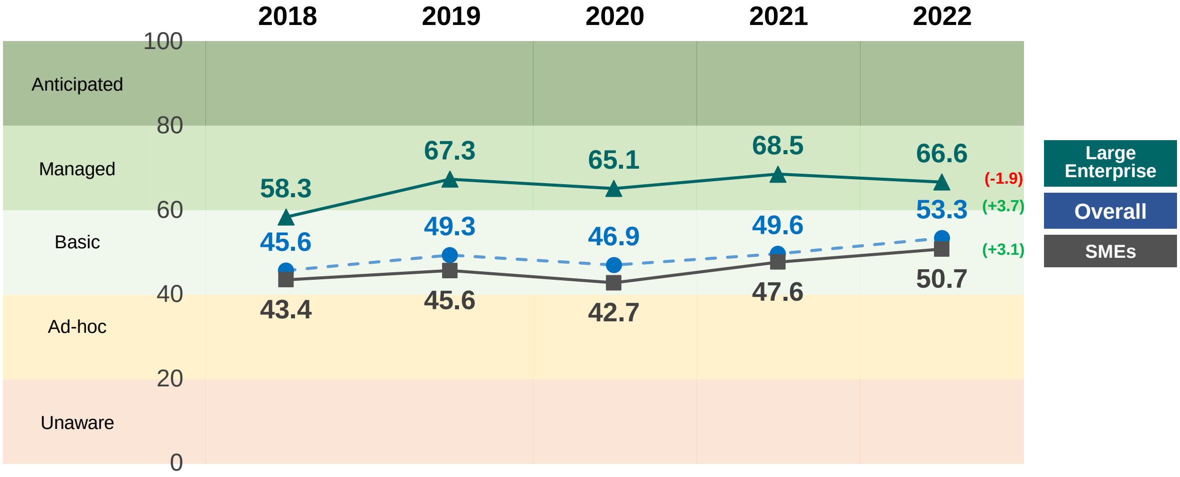
It is recommended that an enterprise should at least attain "Basic" level (40 points or above) for resistance and survivability in case of cyber security attacks.

### 3.2.2 Overall Cyber Security Index



The overall index continues to increase by 3.7 points in 2022 and reaches 53.3, the first time above 50 points. However, there are still further rooms for enterprises to enhance their cyber security to "Managed" level (i.e. 60 points).

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



Looking at the index development by company size, SMEs' index (50.7) improves by 3.1 points and reached 50 points level for the first time. Although the index for Large Enterprises (66.6) slightly weakens compared with 2021, it still remains at the upper "Managed" level.

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

| | 2018 Index | 2019 Index | 2020 Index | 2021 Index | 2022 Index | 2022 Level | YoY Change |
|---|---|---|---|---|---|---|---|
| **Financial Services** | 60.5 | 66.0 | 62.9 | 62.9 | **65.7** | **Managed** | **+2.8** |
| **Information and Communication Technology** | 51.6 | 55.8 | 50.2 | 52.2 | **61.1** | **Managed** | **+8.9** |
| **Manufacturing, Trading and Logistics** | 41.9 | 45.8 | 45.7 | 49.1 | **57.5** | **Basic** | **+8.5** |
| **Professional Services** | 49.5 | 48.0 | 42.9 | 49.0 | **48.4** | **Basic** | **-0.7** |
| **NGOs, Schools and Others** | 45.5 | 51.8 | 51.9 | 52.3 | **47.1** | **Basic** | **-5.2** |
| **Retail and Tourism related** | 41.3 | 44.0 | 40.9 | 42.0 | **45.8** | **Basic** | **+3.8** |
| **Overall (All Business Categories)** | **45.6** | **49.3** | **46.9** | **49.6** | **53.3** | **Basic** | **+3.7** |

Regarding the development of index by business category, most business categories register increments in index compared with 2021, except *Professional Services* which remains stable (-0.7 point) and *NGOs, Schools and Others* which weakens (-5.2 points).

In particular, *Financial Services* (65.7) continues to be the business category with highest index, followed by *Information and Communication Technology* (61.1) with the highest uplift of 8.9 points registered. Both of them are in "Managed" cyber security level, meaning that the cyber security is centrally managed with fine-grained control.

All other business categories are still in "Basic" cyber security level, among which *Manufacturing, Trading and Logistics* (57.5) is the only business category in upper "Basic" level. On the other hand, *Retail and Tourism* (45.8) continues to be the business category with the lowest index among all business categories amid the increment of 3.8 points compared with 2021.

### 3.2.3 Sub-indices

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

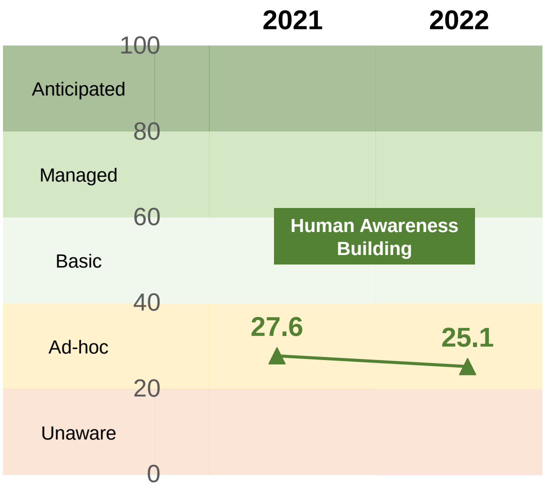
| Component of Index | 2018 | 2019 | 2020 | 2021 | 2022 | YoY Change |
|---|---|---|---|---|---|---|
| **Policy & Risk Assessment** | 49.4 | 48.5 | 46.1 | 45.5 | **48.6** | **+3.1** |
| **Technology Control** | 36.9 | 55.7 | 60.1 | 66.7 | **66.3** | **-0.4** |
| **Process Control** | 57.3 | 63.4 | 54.3 | 58.7 | **73.1** | **+14.4** |
| **Human Awareness Building** | 38.8 | 29.5 | 26.9 | 27.6 | **25.1** | **-2.5** |
| **Overall**<br>**= average of sub-index scores** | **45.6** | **49.3** | **46.9** | **49.6** | **53.3** | **+3.7** |

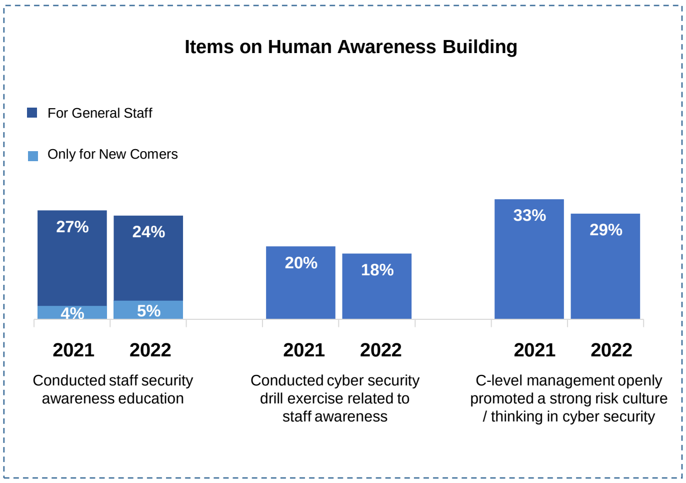
From the results, both "Process Control" (+14.4) and "Policy & Risk Assessment" (+3.1) register improvements in 2022, but the further enhancements are still required for the latter which is still below 50 points (48.6).

Meanwhile, performance of "Technology Control" maintains (-0.4) at "Managed" level at 66.3 points.

However, "Human Awareness Building" continues to be an area which warrants enterprises' attention, as such score has been gradually declining. In 2022, such sub-index (25.1) is further down and approaching "Unaware" level.

Deep diving into the components within "Human Awareness Building" sub-index, it is found that the adoption of all components within the sub-index dip further this year, particularly there are only 18% of enterprises claiming to have conducted cyber security drills in the past 12 months. In addition, only 29% of the enterprises with C-level management openly promote a strong risk culture in cyber security, a dip of 4%-points compared with last year.





The following table shows a summary of the sub-index scores by company size. The bottom row of the table shows the SME / Large Enterprise sub-index.

| | Average Rating (0-100) | | |
|---|---|---|---|
| **Indicator** | **Large Enterprises** | **SMEs** | **All** |
| **1. Policy & Risk Assessment** | **65.9** | **45.3** | **48.6** |
| **2. Technology Control** | **81.6** | **63.4** | **66.3** |
| **3. Process Control** | **80.1** | **71.7** | **73.1** |
| **4. Human Awareness Building** | **39.0** | **22.4** | **25.1** |
| **Sub-index of SMEs / Large Enterprises** | **66.6** | **50.7** | **53.3** |

Overall speaking, Large Enterprises have across the board better sub-index scores than SMEs. However, its "Human Awareness Building" sub-index (39.0) is still marginally below Basic level, indicating that there is no consistent measure in such area. For SMEs, on top of "Human Awareness Building" which stays at lower "Ad-hoc" level, "Policy & Risk Assessment" 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.

| | Average Rating (0-100) | | | | | | |
|---|---|---|---|---|---|---|---|
| **Indicator** | **FS** | **RT** | **MTL** | **ICT** | **PS** | **NGO** | **All** |
| **1. Policy & Risk Assessment** | **65.2** | **38.3** | **54.9** | **55.0** | **41.1** | **44.6** | **48.6** |
| **2. Technology Control** | **74.0** | **58.7** | **70.4** | **77.1** | **64.8** | **59.5** | **66.3** |
| **3. Process Control** | **83.9** | **65.4** | **77.8** | **82.2** | **66.9** | **68.2** | **73.1** |
| **4. Human Awareness Building** | **39.9** | **20.9** | **27.1** | **30.0** | **20.6** | **16.1** | **25.1** |
| **Sub-index of business category** | **65.7** | **45.8** | **57.5** | **61.1** | **48.4** | **47.1** | **53.3** |

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

"Technology Control" and "Process Control" are the top two controls adopted across business categories. Looking at "Technology Control", all business categories have attained "Managed" level, except *Retail and Tourism* and *NGOs, Schools and Others* which are at high "Basic" level with scores were deducted from "Security hardening".

"Policy and Risk Assessment" is one area which can be further enhanced, especially for *Retail and Tourism* (38.3), *Professional Services* (41.1) and *NGOs, Schools and others* (44.6), where these 3 business categories could have better performance in "Security risk assessment". On top of the adoption of "Security risk assessment", *Retail and Tourism* will also need to improve the adoption of "Security policy and practice". On the other hand, only *Financial Services* reaches "Managed" level in "Policy and Risk Assessment" sub-index.

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 all business categories. Although *Financial Services* (39.9) has the highest score among all business categories, it is still marginally below "Basic" level. In addition, *Retail and Tourism* (20.9) and *Professional Services* (20.6) stay at the verge at "Ad-hoc" level, and *NGOs, School and Others* (16.1) is only at "Unaware" level, indicating the management is not aware the necessity of such measures or cultivating the cyber security culture.

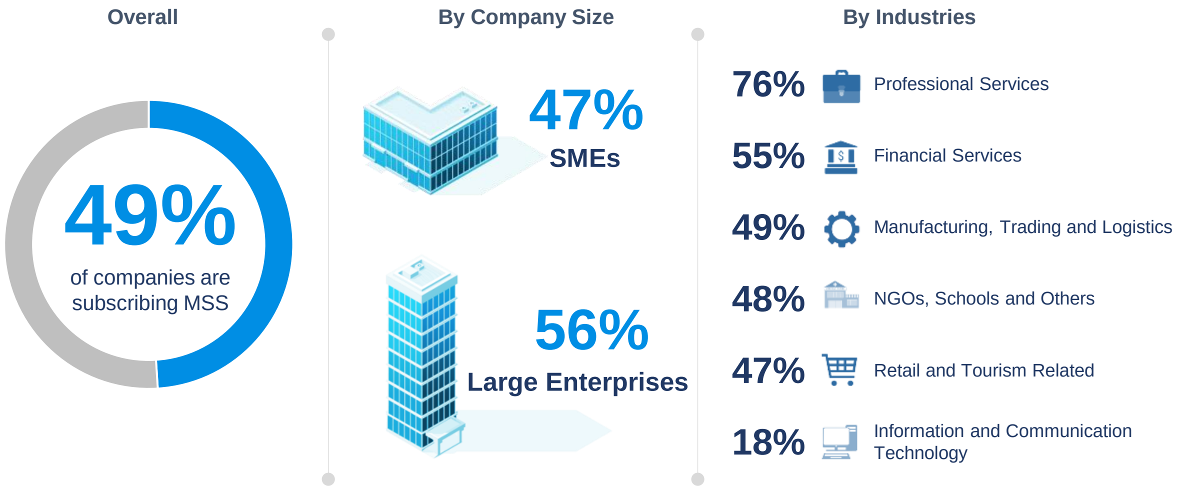
## 3.3 Thematic Survey of the Year: Managed Security Services (MSS)

The thematic survey in this year continues to be MSS, which is an outsourcing model of security expertise. An all-round MSS provider aims at helping enterprises to assess, mitigate and prevent the threats of cyber-attacks. It offers all levels of enterprise network security services, ranging from designing security policies and measures, conducting security tests, integrating security solutions and providing secure broadband connectivity, so as to meet the demands from customers ranging from Small-Medium Enterprises (SMEs) to the most demanding multinational companies.

### 3.3.1 MSS Adoption Rate

Close to half (49%) of the enterprises have subscribed to MSS, which is around 9%-points higher than last year.

Adoption of MSS is relatively more common among Large Enterprises (56%). By business categories, except *Professional Services* and *Information and Communication Technology* with high MSS subscription rate of 76% and low subscription rate of 18% respectively, MSS subscription rate of other industries was around overall average (ranging between 47% and 55%).



### 3.3.2 Challenges of Cyber Security Management and Corresponding Benefits of MSS

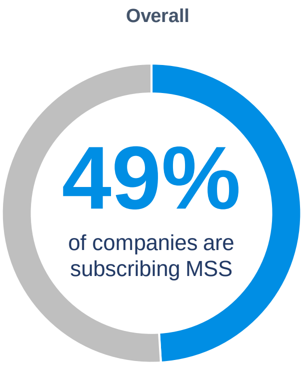
Looking at the challenges of cyber security management, "lack of IT support and management staff" is the top challenge facing nearly half (48%) of the surveyed enterprises, a rise of 3%-points compared with last year. The "lack of expertise (IT personnel or knowledge) to deploy" (35%) is another talent-related issue facing the surveyed enterprises. To this end, MSS can help "mitigate internal IT personnel demand" (31%) and "provide support from cyber security experts" (35%), which are 2 of the top 3 benefits subscribing MSS.

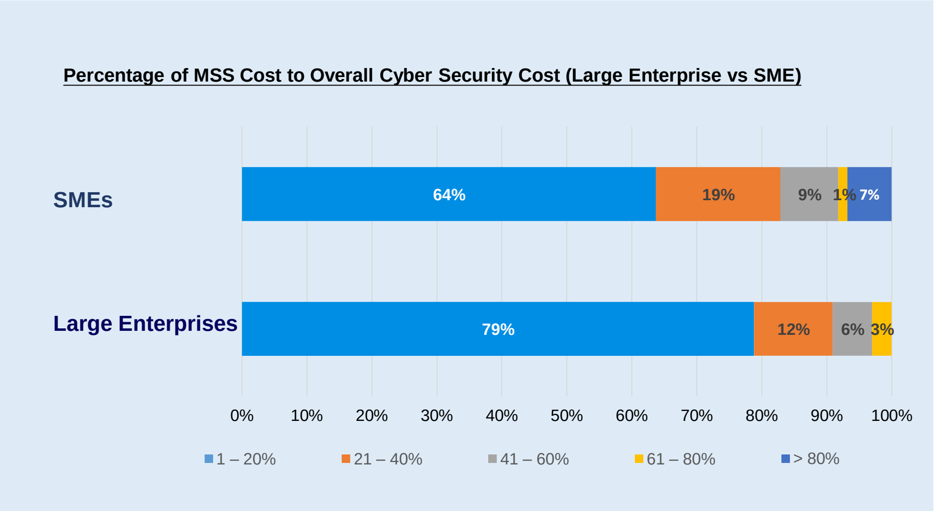
Other top cyber security challenges were mainly on investment, with 44% of surveyed enterprises prefer having "higher level of flexibility in investment". To this, nearly half of the enterprises subscribing MSS appreciate its benefits for offering "higher flexibility allowing users to adjust the service level to business needs" (49%). Another top investment concern facing by SMEs is the "need for one-off investment on infrastructure" (40% among surveyed enterprises), where 35% of MSS subscribers agree that MSS can help "lower the one-off investment" and 30% think that "service providers continuously enhance technology and service standards to increase competitiveness".

| Top Challenges of Cyber Security Management | Corresponding Top Benefits of MSS |
|---|---|
| Lack of IT support and management staff (48%) | Mitigate internal IT personnel demand (31%) |
| With its ever-changing nature, investments on projects related require a high level of flexibility (44%) | Higher flexibility, which allows the users to adjust the service level to business needs (49%) |
| Require a large one-off investment on infrastructure (40%) | Low one-off investment as Capital Expense is substituted by Operation Expense (35%) |
| | Service providers continuously enhance technology and service standards to increase competitiveness (30%) |
| Lack of the expertise (IT personnel or knowledge) to deploy (35%) | Support from cyber security experts (35%) |

### 3.3.3 MSS Budget

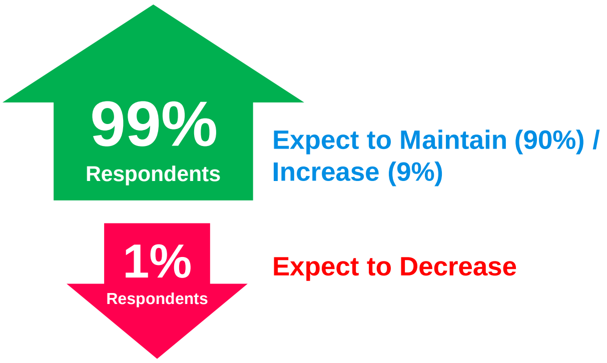
Among majority of the enterprises subscribing MSS, such spending contributes to less than 20% of the total cyber security budget.





In the next 12 months, nearly all surveyed enterprises subscribing to MSS expect to maintain the same level of or increase their MSS budget. Among those expecting an increase in MSS budget, the top reason for increasing MSS budget is "meeting digital transformation / remote and hybrid workplace", where a 9%-points increment is observed compared with last year. This somehow indicates the increased importance of remote workplace solutions.

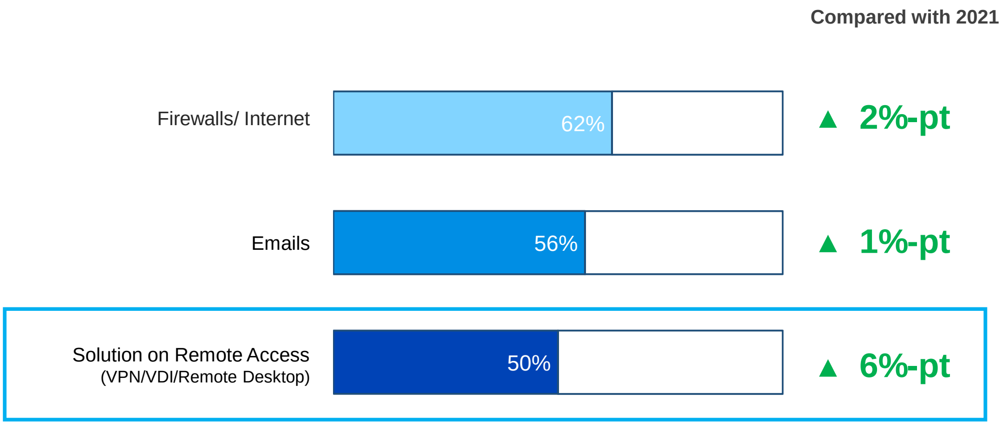
Change on MSS Budget in the Next 12 Months



| Top 3 Reasons to Increase MSS Budget | Compared with 2021 |
|---|---|
| Meet with Digital Transformation / Remote and Hybrid Workplace | ▲ 9%-pt |
| Meet with Organisation Development | ▲ 3%-pt |
| Respond to the Increasing Security Threats | +/-0%-pt |

As a side note, half (50%) of the enterprises consider “solution on remote access (VPN / VDI / Remote desktop)” as one of the top 3 most important cyber security services, increased by 6%-points compared with last year.

## Top 3 Important Cyber Security Services

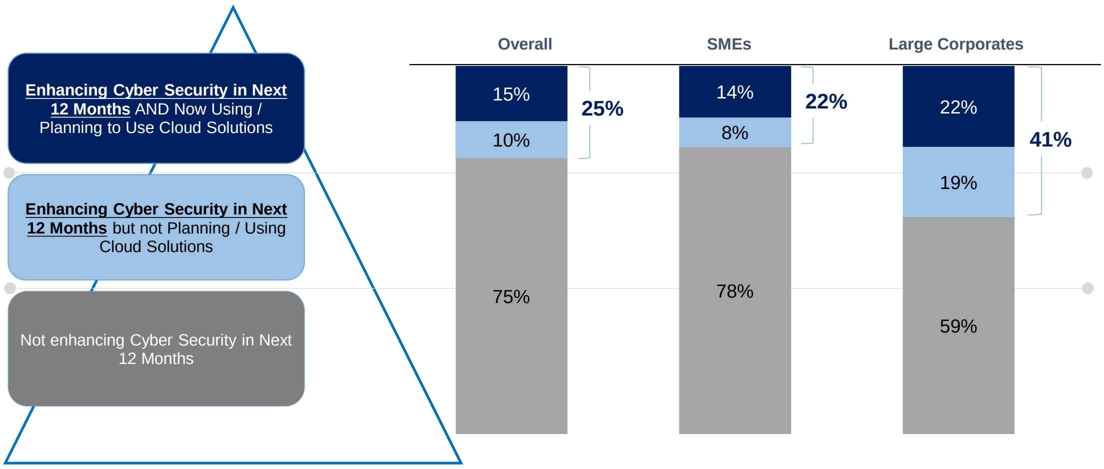


## 3.4 Investment Plans in the Next 12 Months

### 3.4.1 Enhancement Plans for Cyber Security

1 in 4 (25%) surveyed enterprises have plans to enhance cyber security in the next 12 months. Compared with SMEs (22%), Large Corporates (41%) are more proactive in enhancing their cyber security level.

Among those enterprises planning to enhance cyber security in next 12 months, 62% of them are currently using / planning to use cloud service. Such proportion is higher among SMEs (64%).



In terms of business categories, more enterprises in *NGOs, Schools and Others* (31%) and *Financial Services* (29%) have plans to enhance their cyber security in the next 12 months, while *Manufacturing, Trading and Logistics* (19%) is less active.

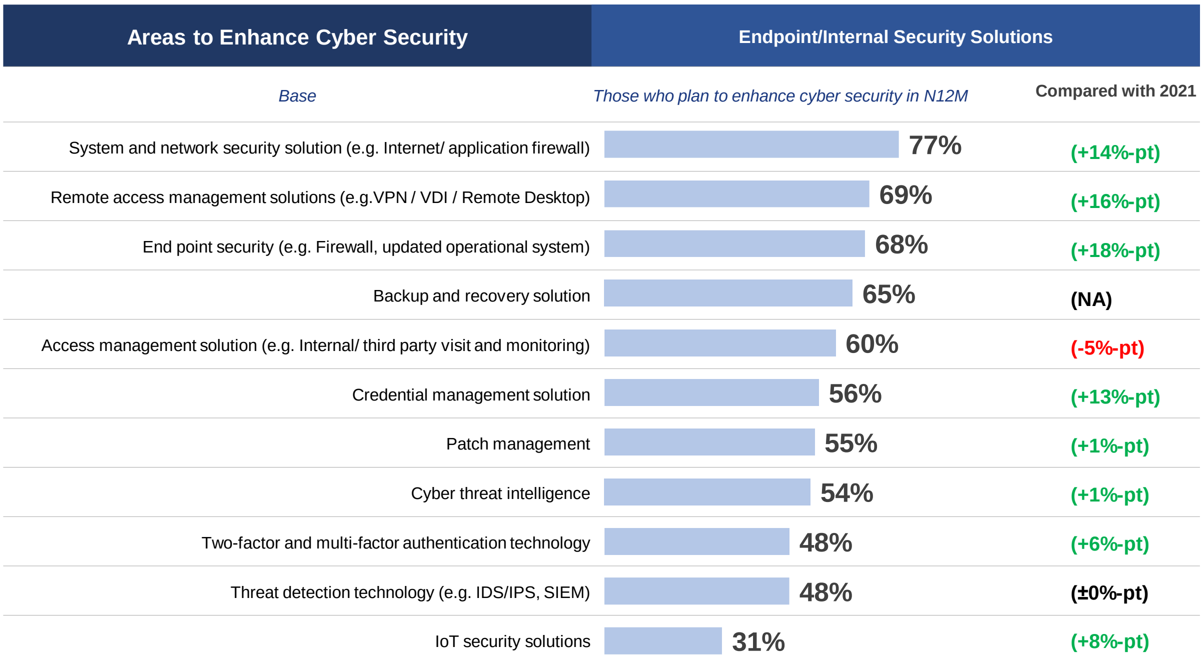
Among enterprises planning to enhance cyber security, higher proportion of (planned) cloud solutions usage is found in *Information and Communication Technology* (82%) and *Professional Services* (67%) compared with other business categories (between 54% and 59%).

| | FS | RT | MTL | ICT | PS | NGO | All |
|---|---|---|---|---|---|---|---|
| NET - Planning to Enhance Cyber Security in Next 12 Months | **29%** | **25%** | **18%** | **28%** | **27%** | **31%** | **25%** |
| *Currently Using / Planning to Use Cloud Solutions* | *17%* | *15%* | *11%* | *23%* | *18%* | *17%* | *15%* |
| *Not Planning / Using Cloud Solutions* | *12%* | *11%* | *7%* | *5%* | *9%* | *14%* | *10%* |
| Not Enhancing Cyber Security in Next 12 Months | **71%** | **75%** | **82%** | **73%** | **73%** | **69%** | **75%** |

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

## 3.4.2 Areas to Enhance Cyber Security – End-point / On-premise Solutions

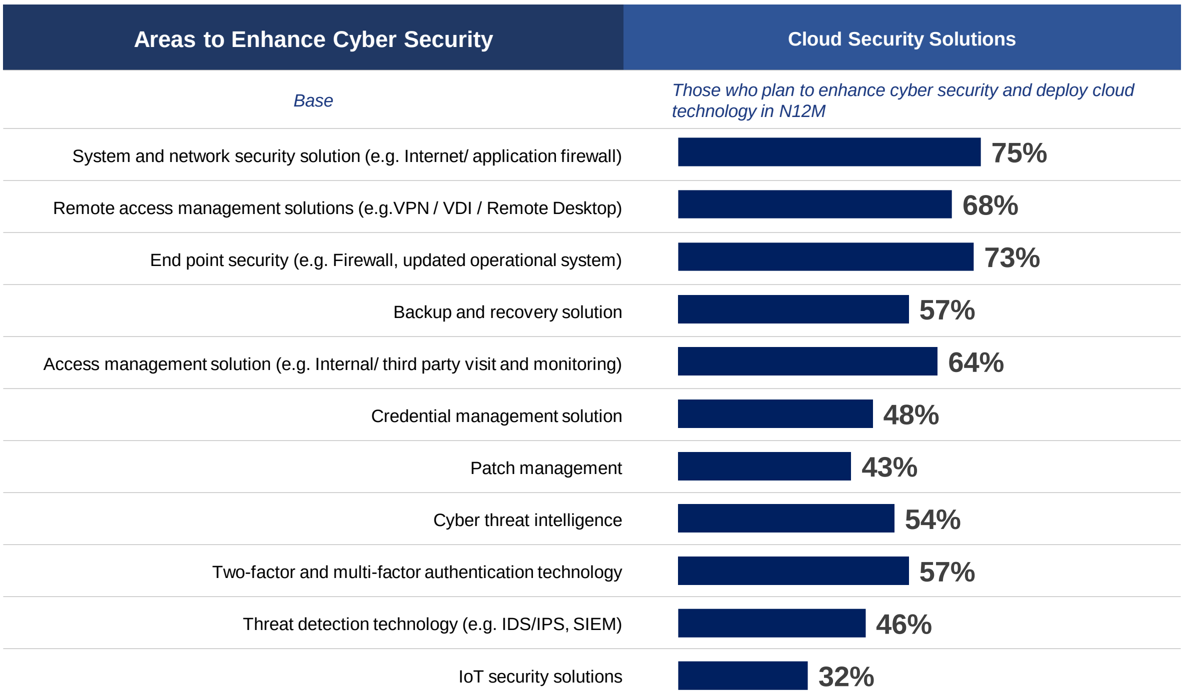
Among the 25% enterprises with plans to enhance cyber security in the next 12 months, "System and Network Security Solution" ranks first with 77% of them planning to enhance such end-point solution. This is followed by "Remote access management solutions" (69%), "endpoint security solution" (68%) and "backup and recovery solution" (65%). It should be noted that the proportion of enterprises choosing to enhance "remote access management" registers an uplift of 16%-points compared with last year, echoing previous finding that hybrid working solutions has become more important compared with last year.



### 3.4.3 Areas to Enhance Cyber Security – Cloud Solutions

62% of the surveyed enterprises planning to enhance cyber security in next 12 months have been deploying or planning to deploy cloud technology in the coming 12 months.

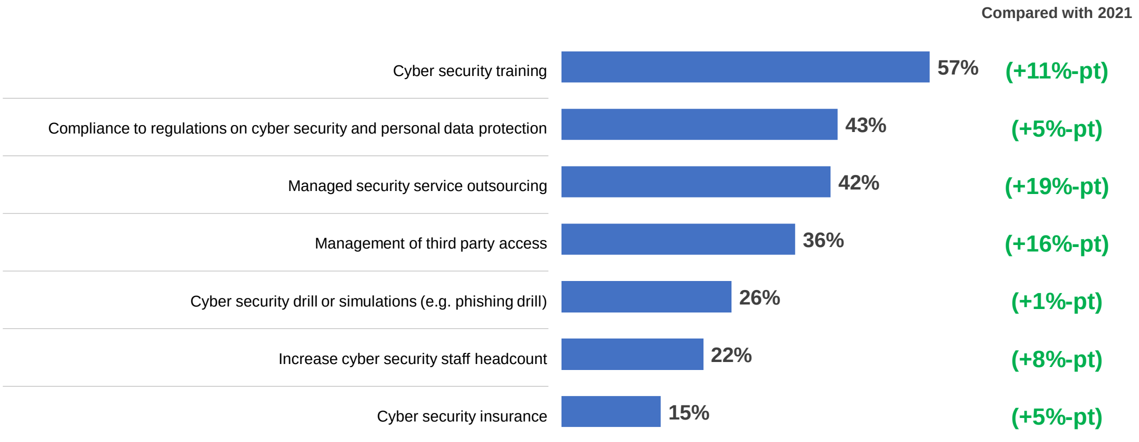
Similar to the previous results on the areas on enhancing endpoint solutions, “system and network security solutions” (75%), “endpoint security” (73%) and “remote access management solutions” (68%) are the top 3 popular areas of Cloud Security Solutions that enterprises intended to enhance.



### 3.4.4 Areas to Enhance Cyber Security – Non-Technical Measures

Those 25% enterprises intending to enhance their cyber security in next 12 months were also asked of the non-technical measures that they would like to enhance.

Areas to Enhance Cyber Security – Non-Technical Measures



*Base: Those who plan to enhance cyber security in the coming 12 months*

From the results in the chart above, “Cyber security training” (57%) continues to rank top as the most popular non-technical measure to be enhanced, followed by “Compliance to regulations on cyber security and personal data protection” (43%) and “MSS outsourcing” (42%).

Compared with last year, enterprises have shown higher interest in enhancing various non-technical measures, with year-on-year increments ranging from 5%-points to 19%-points. In particular, the proportion of enterprises planning to enhance “MSS outsourcing” has uplifted by 19%-points compared with last year, which is in line with previous findings on increased MSS adoption.

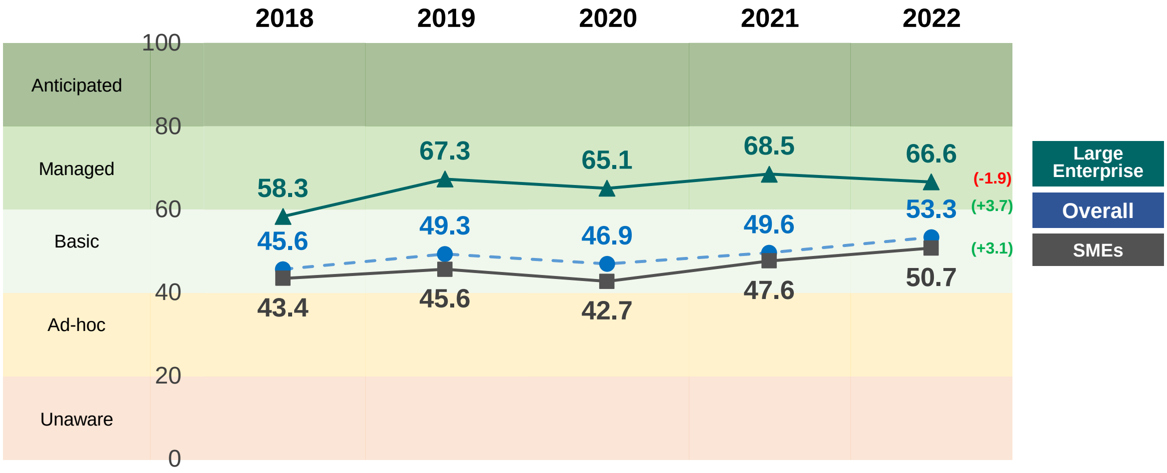
However, “Cyber security drill or simulation” (26%) is the only measure with similar proportion (+1%-point).

# 4. Conclusion & Recommendations

## 4.1 Key Findings

### Cyber Security Index

Overall cyber security readiness index increased by 3.7 points to 53.3 points, the first time surpassing 50-point level. Although the overall index is higher among Large Enterprises (66.6), SMEs (50.7) have slightly narrowed down the gap with a further uplift of 3.1 points.



*Financial Services* (65.7) and *Information and Communication Technology* (61.1) are the 2 categories in "Managed" level of cyber security. All other categories are still at "Basic" level, with *Manufacturing, Trading and Logistics* (57.5) at the upper "Basic" level and the remaining at the lower "Basic" level ranging between 45.8 and 48.4. *Retail and Tourism* (45.8) remains the business category with lowest overall index amid the improvement of 3.8 points.

### Cyber Security Attacks Encountered in Past 12 Months

Close to two-thirds (65%) of the surveyed enterprises have encountered cyber security attacks in the past 12 months, a surge of 24%-points compared with last year. Cyber security attacks are more common in Large Enterprises (78%) than SMEs (63%).

"Phishing attacks" are the most common type of cyber security attacks, with an incidence rate of 94% among those who have encountered cyber security attacks in past 12 months. "Email phishing" (83%) is the most common type of phishing attacks, while "vishing" (32%) and "spear phishing" (28%) are emerging.

The types of cyber security attacks (external attacks, internal attacks and attacks caused by external parties) encountered by the surveyed enterprises rebound across the board, with external attacks (59%) continue to be most common, indicating that cyber-attacks have also been advancing together with technological enhancements. Although incidence of internal attacks stays at a relatively low level at 14%, 1 in 10 attacks can cause financial loss to the enterprises concerned.

**A Need for Recalling Attention on Human Awareness of Cyber Security**

Although the level of cyber security has been improving which can help detect and prevent most of the cyber security attacks, humans are still playing a vital role, so "Human Awareness Building" can help prevent cyber security attacks from happening. From the results from this round of survey, such awareness has further declined:

1. Perceived importance of cyber security has weakened compared with 2021, where the proportion of enterprises considering cyber security "Extremely important" drops from 48% to 36%;
2. A further decline (-2.5 points) in "Human Awareness Building" sub-index is observed and it is now at the verge of "Ad hoc" level; and
3. While enterprises planning to enhance cyber security in next 12 months have plans to enhance most of the non-technical measures, "cyber security drill or simulation" (26%) is the only measure with minimal increment (+1%-point).

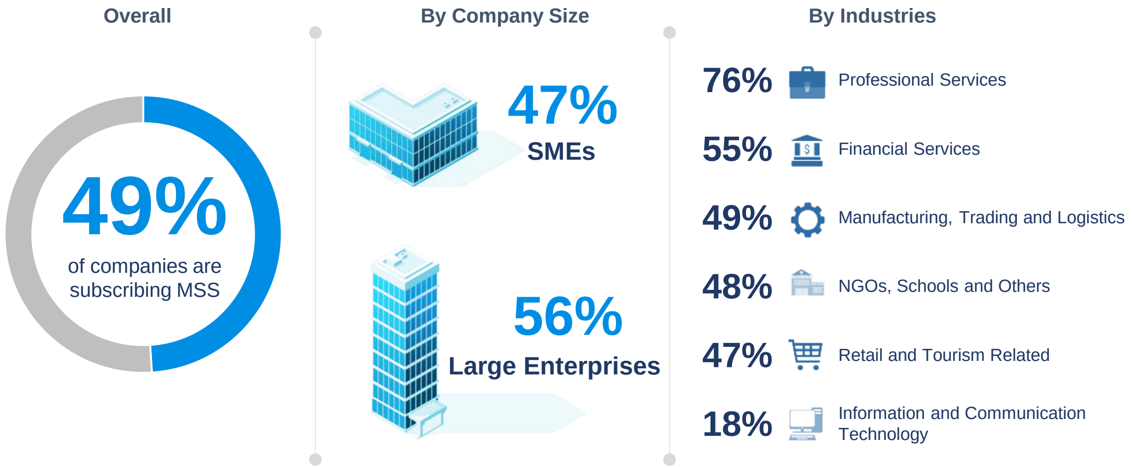
**Increased Importance of Remote Access Solutions**

With the fifth wave of the pandemic took place earlier this year forcing "work from home" policy to be implemented, coupled with the increasing adoption of flexible work locations across employees from different sectors, remote access has been increasingly important and enterprises are willing to invest more on such areas:

1. Although "solutions on remote access" such as VPN / VDI / Remote Desktop (50%) rank third as the most important cyber security services; there is a 6%-point increment compared with last year while the corresponding figures for the other 2 most important cyber security services remain similar to last year;
2. "Meeting with Digital Transformation / Remote and Hybrid Workplace" remains the top reason for increasing cyber security budget this year, with an uplift of 9%-points from last year; and
3. "Remote access management solutions" are among to top 3 endpoint / Internal security solutions and cloud security solutions planned to be enhanced in the next 12 months.

## Managed Security Services (MSS)

Adoption of MSS has increased compared with last year, with around half of the surveyed enterprises having subscribed to it.



MSS can address the talent-related and investment-related challenges facing enterprises, in particular to the “lack of IT support and management staff” which marks a 3%-point increase from last year. Also, over half (53%) of those enterprises subscribing to MSS claim to be lacking IT management professionals.

Nearly all companies using MSS plan to maintain the same level of MSS in the next 12 months.

## Cyber Security Investment Plan in the Coming 12 Months

25% of the surveyed enterprises have plans to enhance cyber security in the next 12 months. Among them, 62% of them are currently using / planning to use cloud service.

Large Corporates (41%) are more proactive in enhancing their cyber security level compared with SMEs (22%). By business categories, more enterprises in *NGOs, Schools and Others* (31%) and *Financial Services* (29%) have plans to enhance their cyber security in the next 12 months.

Among those enterprises planning to enhance cyber security in the next 12 months, a 19%-point increment is observed in terms of the interest in MSS outsourcing.

## 4.2 Recommendations

(1) **HKPC recommends enterprises to put more effort into cyber security to move the security readiness level up to "Managed" level.**

Amid escalation of cyber threats, more and more enterprises are digitalising their business. This trend will continue even after the normalisation of the pandemic. The average cyber security readiness index has been in the "Basic Level" for several years with very small improvement. Enterprises, especially smaller ones, should further enhance their cyber security readiness to move up into the "Managed" level.

To attain the most significant improvement, efforts could be directed towards addressing the weaker areas, especially "Human Awareness Building" which has been on a downward trend amid improvements in "Process Control" and the stable performance in "Technology Control".

(2) **Raise Cyber Security Awareness via Education**

Humans is always the weakness link in cyber security, yet cyber security awareness education is usually not put as top priority until there is huge media exposure of prominent cyber attacks. In the 2022 survey, it is found that "phishing attacks" continue 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 have received "phishing attacks". In fact, "phishing attacks" leverage on human vulnerability, for example, a staff member accidentally opens an attachment with ransomware, causing the data on the enterprise server to be encrypted and become inaccessible.

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

- Providing regular training to all general staff and newcomers; and encouraging them to undergo training on Cybersec Training Hub (https://cyberhub.hk/);
- 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) to exchange information and industry peers for building up collaborative defence
- Having senior management's open commitment to reinforcing a culture of security;
- Subscribing to 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 as well as the benefits and constrains of MSS;

- (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) Enhance Education on MSS**

Although adoption of MSS has improved compared with last year, the adoption rate could be further enhanced, especially for SMEs with less than half of them having subscribed. From the results of the survey, MSS subscribers recognise the benefits that MSS brings along with - helping them tackle key cyber security management challenges, especially in terms of talent and investment.

On the other hand, those who are currently not subscribing to MSS may not have all information about the benefits, constraints of MSS as well as its budget requirements, such that they cannot make informed decisions.

Hence, enterprises shall be given more education on the benefits that MSS can bring to them, which include but not limited to extensive coverage of cyber security solutions with low set-up budget requirements and flexible pricing options, as well as the comprehensive support from cyber security experts.

**(4) Enhancing Cyber Security for the Need for Increasing Remote Workplace**

With the outbreak of the 5th wave of the pandemic as well as the increasing popularity of “Work From Home” policy as HR benefits across different sectors. Implementation of hybrid workplace increased compared with last year, which could be reflected by the increasing demand for hybrid workplace solutions from the results of this year’s survey. The increased adoption of hybrid workplace policy has also presented a stronger need to enforce cyber security and maintain data privacy. To this, enterprises are recommended to conduct Cyber Security & Privacy Maturity Assessment for Hybrid Workplace to evaluate and understand their current maturity level in cyber security and privacy.

- 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 HKCERT

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

For more information, please visit https://www.hkcert.org.

## About HKT

HKT (SEHK: 6823) is Hong Kong's premier telecommunications service provider and a leading innovator. Its fixed-line, broadband, mobile communication and media entertainment services offer a unique quadruple-play experience. HKT meets the needs of the Hong Kong public and local and international businesses with a wide range of services including local telephony, local data and broadband, international telecommunications, mobile, media entertainment, enterprise solutions and other telecommunications businesses such as customer premises equipment sales, outsourcing, consulting and contact centers.

HKT is the first local mobile operator to launch a true 5G network with differentiated value-added services. Backed by its substantial holding of 5G spectrum across all bands and a robust and extensive fiber backhaul infrastructure, HKT is committed to providing comprehensive 5G network coverage across the city.

HKT delivers end-to-end integrated solutions employing emerging technologies such as 5G, cloud computing, Internet of Things (IoT) and artificial intelligence (AI) to accelerate the digital transformation of enterprises and contribute to Hong Kong's development into a smart city.

Riding on its massive loyal customer base, HKT has also built a digital ecosystem integrating its loyalty program, e-commerce, travel, insurance, FinTech and HealthTech services. The ecosystem deepens HKT's relationship with its customers thereby enhancing customer retention and engagement.

For more information, please visit www.hkt.com.

## License

## Disclaimer

HKPC and HKCERT 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 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 |