

PCPD



H K

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

Personal Data Privacy and Protection in Higher Education

Seminar at the University of Hong Kong

11 July 2024

Ms Ines LEE

Head of Legal Division

Trends in the Global Privacy Landscape

Technology (e.g. AI, Big Data, cloud, IoT, social media) is increasingly making impact on personal data privacy

Many jurisdictions have passed or proposed **new/revised personal data protection law**

The adoption of data protection and privacy legislation **increased by 11%** between 2015 and 2020[#]

66% of nations of the world have data protection legislation[#]



EU GDPR (effective May 2018) raised the benchmark of personal data protection and people's **privacy expectation** to new heights

[#]Source: United Nations Conference on Trade and Development (UNCTAD)

New Laws/Bills

<u>Jurisdiction</u>	<u>Status</u>	<u>Law</u>
Brazil	New Passed in Aug 2018 (date for implementation T.B.D.)	General Data Protection Law (LGPD)
California, US	New Implemented in Jan 2020	California Consumer Privacy Act (CCPA)
India	New Proposed in Dec 2019	Personal Data Protection Bill, 2019
Thailand	New Passed in May 2019 (most provisions effective from May 2021)	Personal Data Protection Act (PDPA)

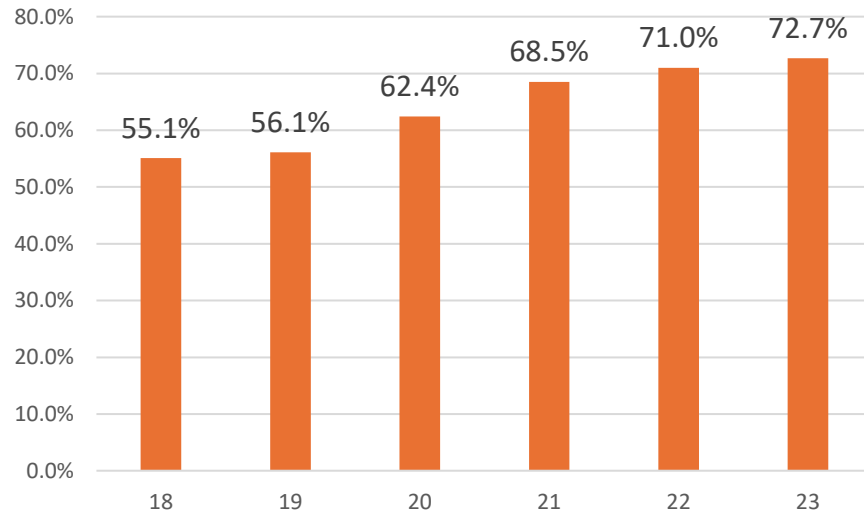
Global Data Security Crisis

The bad news is that cyber attacks are rising, with more and more cases reported

Cyberattacks around the world

Annual share of organizations affected by ransomware attacks worldwide

2018 - 2023

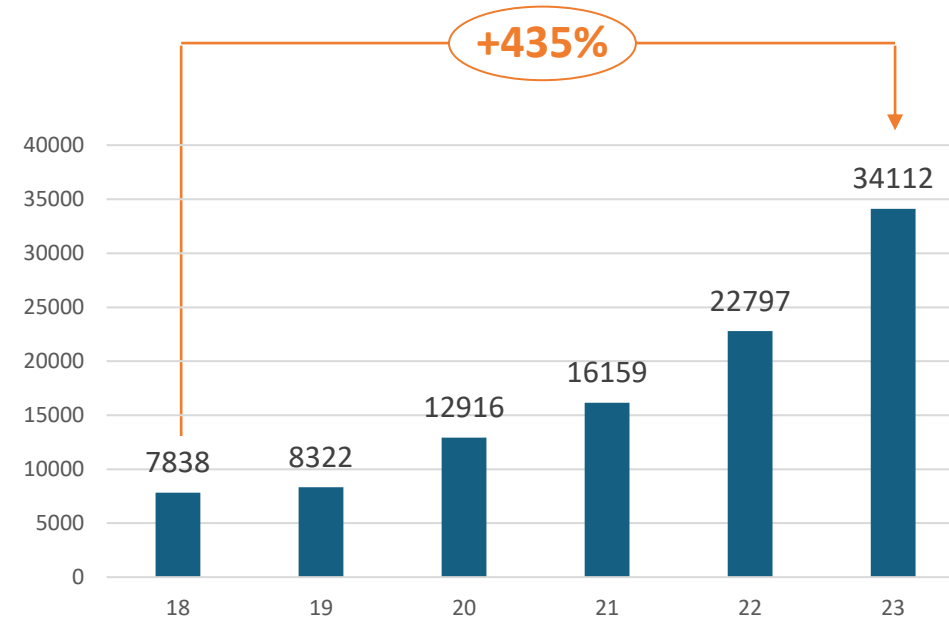


Source: [Statista](#)

Cybercrimes in HK

Overall technology crimes in HK

2018 - 2023



Source: [Hong Kong Police](#)

Global Incidents

Financial firms are prime targets for cyber attacks

Medibank says hacker accessed data of 9.7 million customers, refuses to pay ransom

Reuters

November 8, 2022 5:05 AM GMT+8 · Updated a year ago



Medibank (2022)

- Hackers used the credential stolen from an employee account with preferential access to the internal system of the insurer
- Health data of over 9 million customers breached

Source: [Reuters \(2022\)](#)



MGM Resorts (2023)

- Cyberattack disrupted operation of hotel and casinos
- Contact information, gender, date of birth, social security numbers etc. breached
- \$100m hit to Q3 2023 results

Source: [Casino giant MGM expects \\$100 million hit from hack that led to data breach | CNN Business](#)

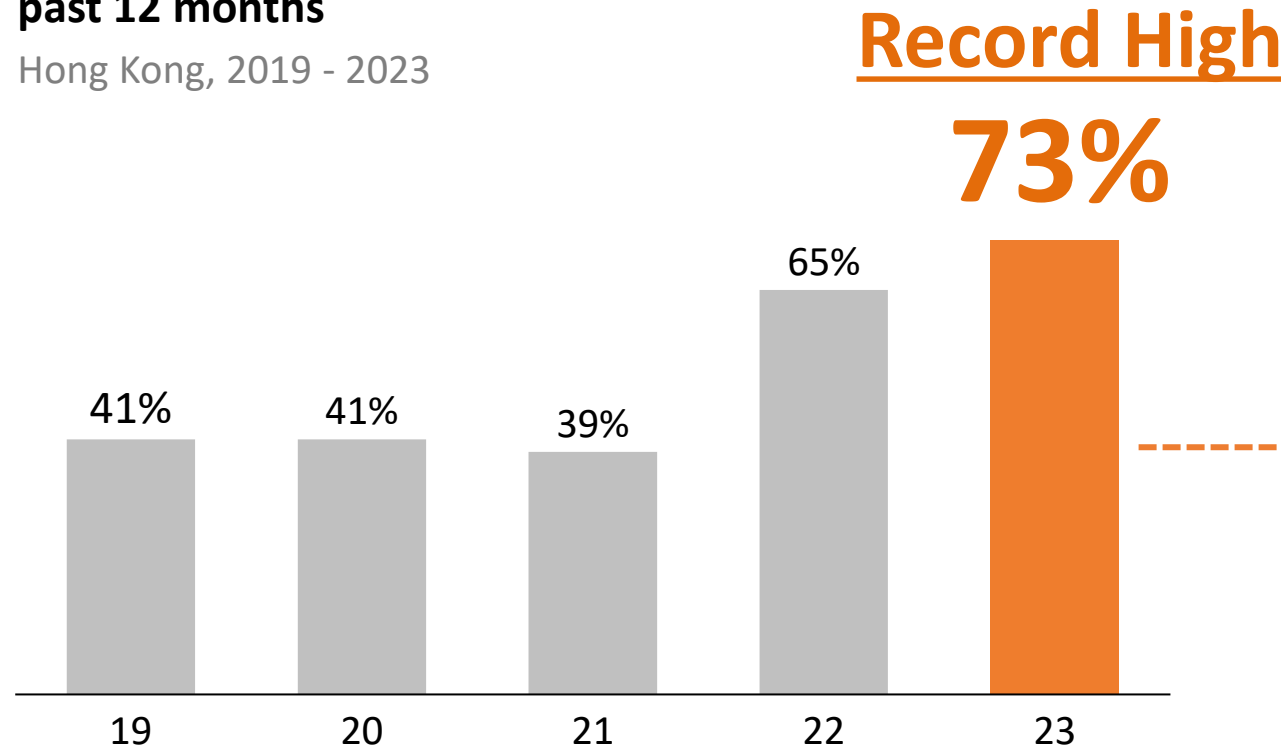
Local Cyber Security Attacks

Organisations faced a record high incidence of cyber security attacks this year

Yearly comparison

% of enterprises that encountered cyber security attacks in the past 12 months

Hong Kong, 2019 - 2023



Source: [Hong Kong Enterprise Cyber Security Readiness Index](#)

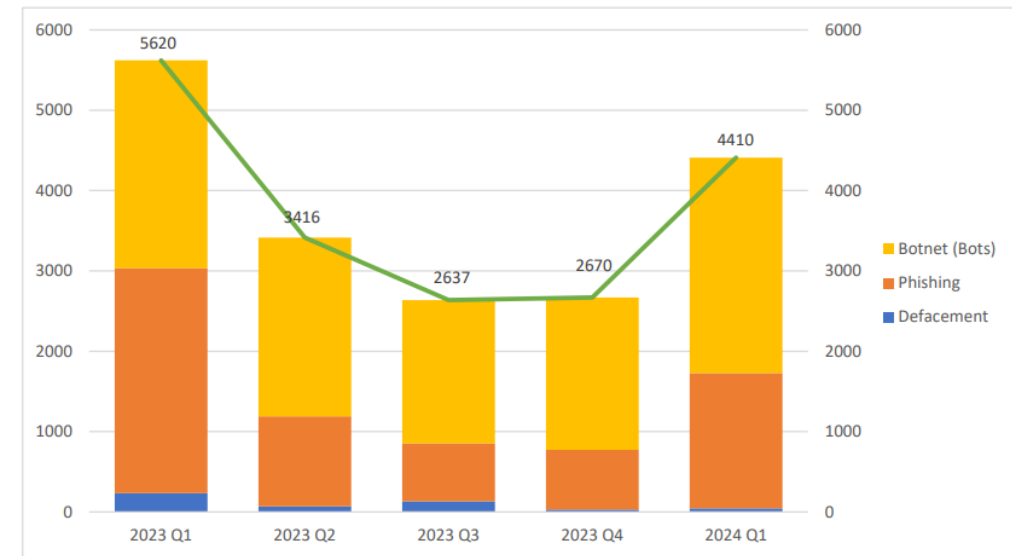
Highlights of the 2024 Q1 Report

Unique security events related to Hong Kong

Quarter-to-quarter

4,410

65.2%↑



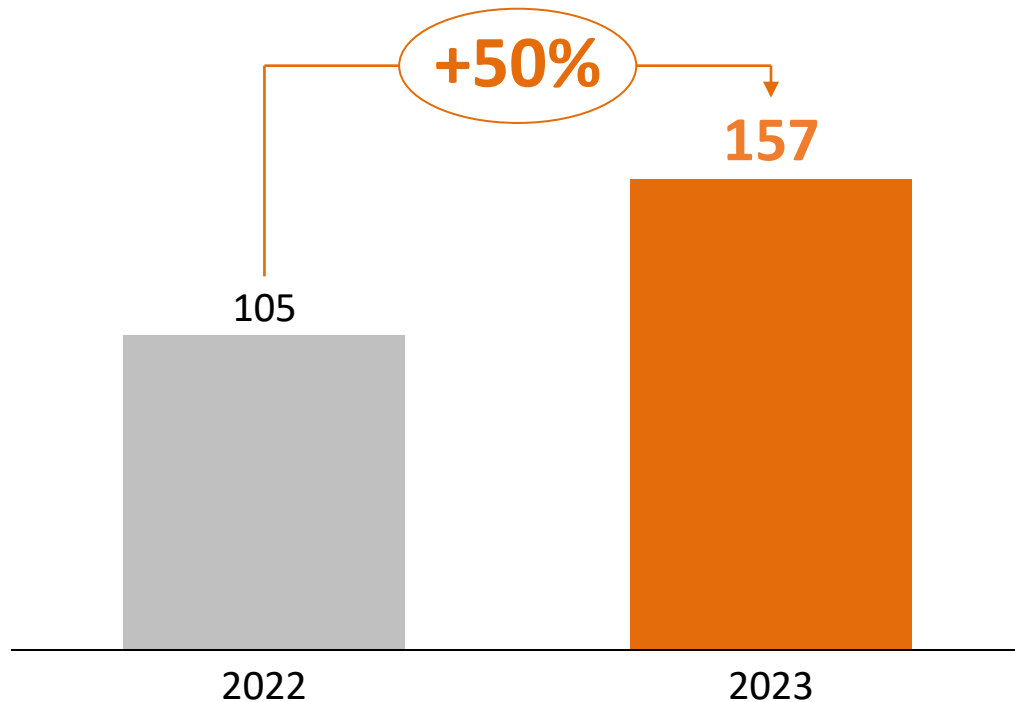
Source: [2024Q1 HK SecurityWatchReport \(English\).pdf \(hkcert.org\)](#)

Local Data Breaches

Data breach notifications surged in 2023; hacking was a major contributor

Compared with 2022, DBNs in 2023 rose substantially by 50%

Data breach notifications to PCPD



Source: [PCPD](https://www.pcpd.org.hk)

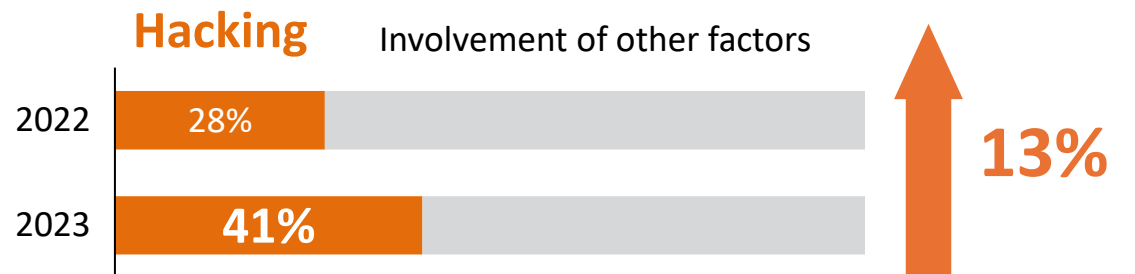
DBNs involving hacking rose both absolutely and relatively

Data breach notifications involving hacking

Absolute numbers



As a percentage of total



PCPD's Data Security Initiatives

PCPD is helping data users enhance data security and prevent data breaches

Data Security Thematic Webpage

One-stop access to resources on data security



Data Security Scanner

Self-assessment toolkit for enterprises to assess adequacy of data security measures of ICT systems



Data Security Hotline

Provide SMEs with a channel to make enquiries about compliance with the PDPO



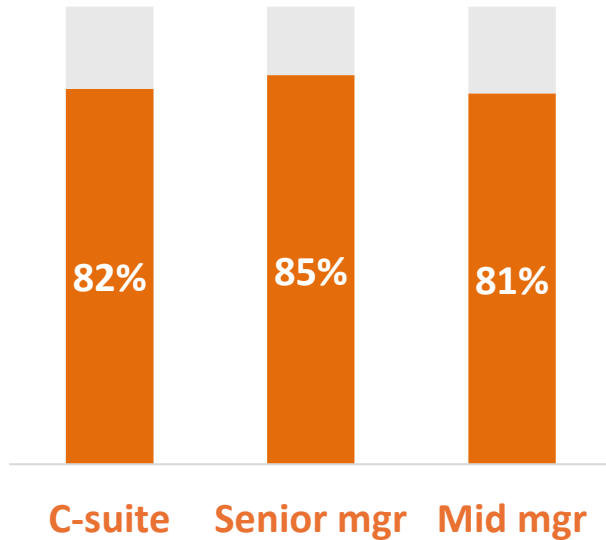
Guidance Materials

- **Data Breach Response Plan**
- **Guidance Note on Data Security Measures for ICT**
- **Privacy Management Programme (PMP)**

Growing popularity of AI

High AI use across levels

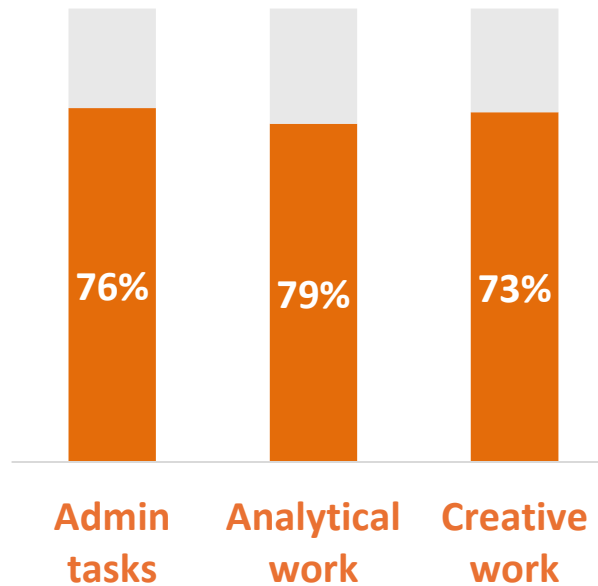
Exposure to generative AI tools
% who tried at least once, by job title



Source: McKinsey (2023)

Workers comfortable with AI

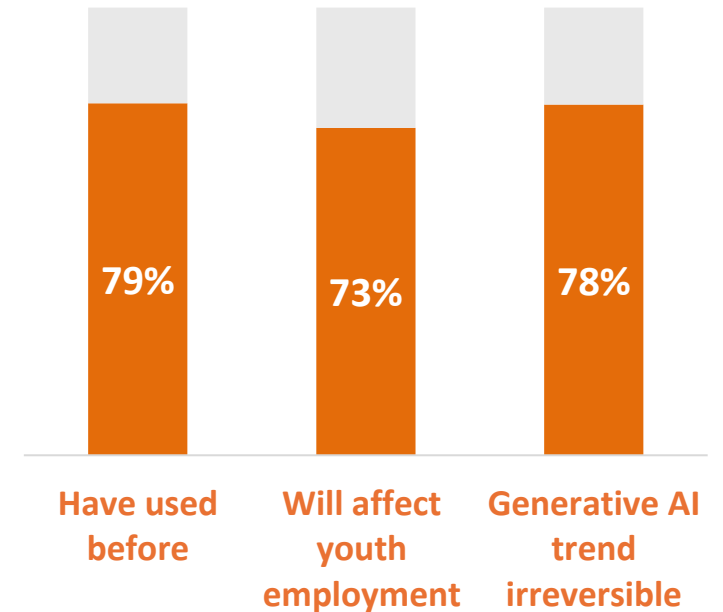
Views on AI in work
Respondents comfortable with AI for...



Source: Microsoft (2023)





Youth find AI impactful

Use/Views on generative AI
Selected Hong Kong youth, age 15-34



Source: Youth I.D.E.A.S (2023)

Privacy issues of AI

Issue	Explanation	Illustration
 Excessive data collection	AI applications tend to collect and retain as many data as possible, which includes personal data	OpenAI reportedly scraped 300 billion words online to train ChatGPT
 Use of data	AI models can be so advanced that people find it hard to understand how their personal data would be used	The “Black box” problem: users of AI are unable to know the internal logic of the AI systems
 Identity re-identification	Some AI models may be able to re-identify individuals’ identities by collecting & matching data from different sources	Studies show that it is possible to identify 93% of people in dataset with 60mn people using 4 pieces of data
 Data accuracy	Training AI models requires lots of data, and data quality & accuracy is an issue	AI may make incorrect analysis because of inaccurate data, which hampers decision-making

AI's risks vis-à-vis Data Protection Principles (DPP)

DPP1

PURPOSE AND MANNER OF COLLECTION

- Large amount of personal data collected
- Disclose little about collection

DPP2

ACCURACY AND RETENTION

- Outdated/incorrect data becomes part of training data and is kept longer than necessary

DPP3

USE OF DATA

- User conversations become new training data and may be reproduced for another purpose

DPP4

DATA SECURITY

- Security risks of storing large amount of conversations

DPP5

OPENESS AND TRANSPARENCY

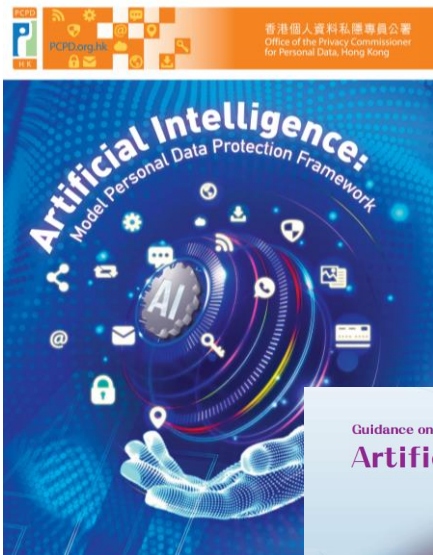
- Data subjects are not fully informed of what personal data is held or how personal data is used

DPP6

ACCESS AND CORRECTION

- Outdated/incorrect data that is part of training data is hard to be accessed or corrected

Practical Guides related to AI



The Commissioner has issued two practice guides, namely, the *Guidance on the Ethical Development and Use of Artificial Intelligence* and *Artificial Intelligence: Model Personal Data Protection Framework*.

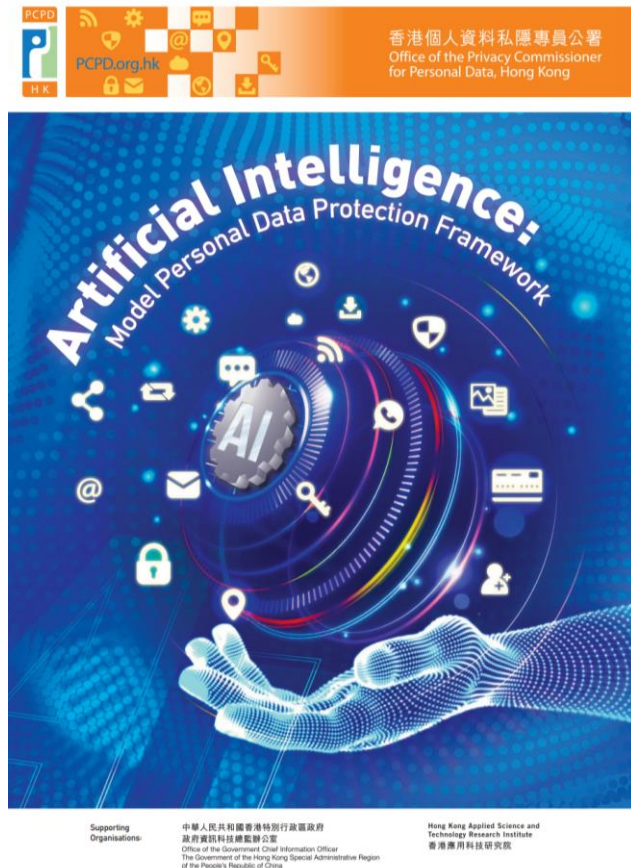
They cover AI governance recommendations with regard to business processes in the following areas: **establishing AI strategy and governance, conducting risk assessment and human oversight, executing development or customisation of AI models and management of AI systems, and fostering communication and engagement with stakeholders**. The former guide focuses on the responsibilities of organisations that develop in-house AI models, while the latter targets organisations that procure and implement AI solutions from third-party suppliers.

Practical Guides related to AI

• Artificial Intelligence: Model Personal Data Protection Framework

• Recommendations and best practices regarding governance of AI

- Establish AI Strategy and Governance
- Conduct Risk Assessment and Human Oversight
- Customisation of AI Models and Implementation and Management of AI Systems
- Communication and Engagement with Stakeholders



Thank you



2827 2827



www.pcpd.org.hk



communications@pcpd.org.hk

