

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

# Addressing Privacy Risks in Fintech: Safeguarding Data Security

MPF Symposium 2023

12 December 2023

**Ada CHUNG Lai-ling**

**Privacy Commissioner for Personal Data**

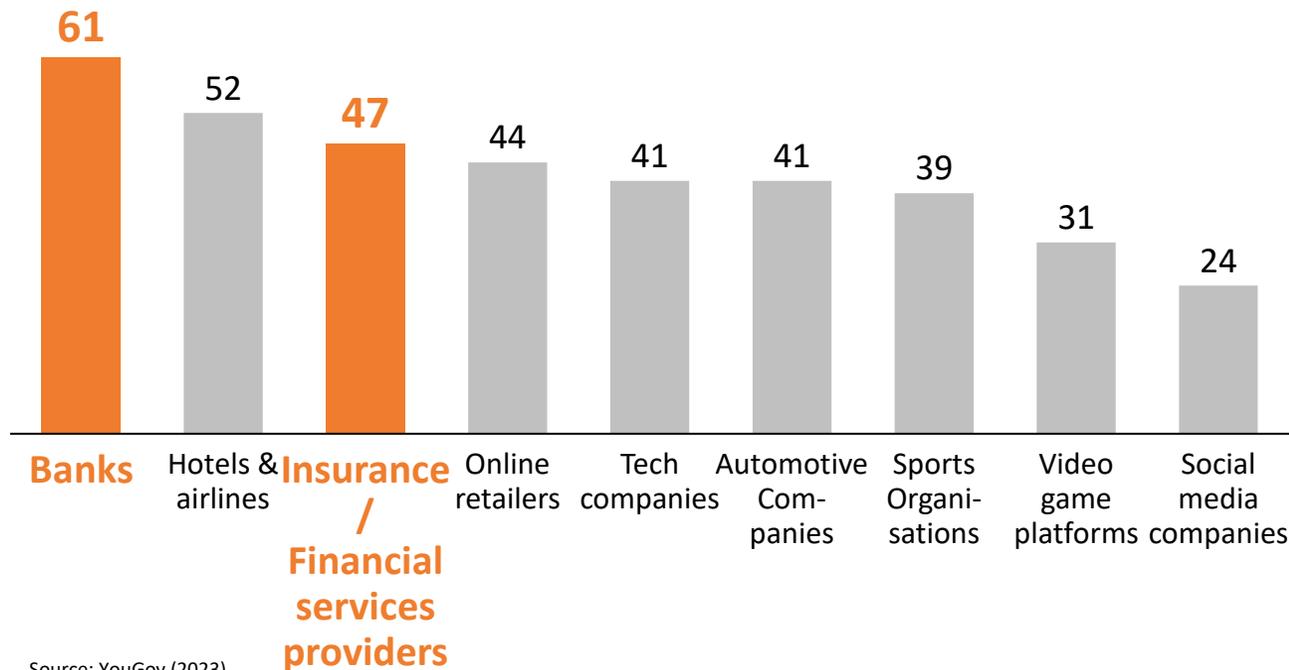
# Statistics

## Customers, including those in HK, trust the financial sector over data

The banking, insurance and financial services sectors rank high in a survey of trust with personal data...

### Which sectors do customers trust most with their personal data?

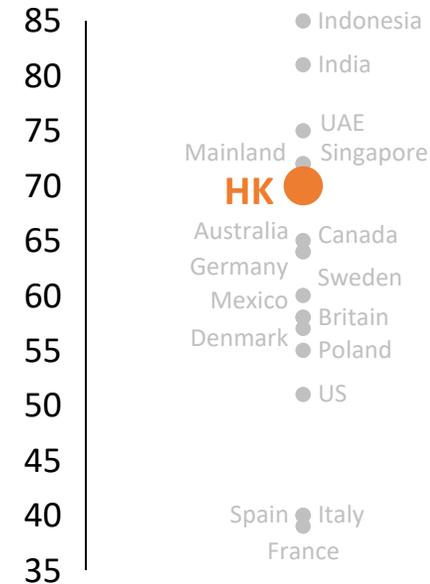
%, 2023, 18 markets across the world



Source: YouGov (2023)

... with HK ranking 6<sup>th</sup> among the 18 markets surveyed for banks

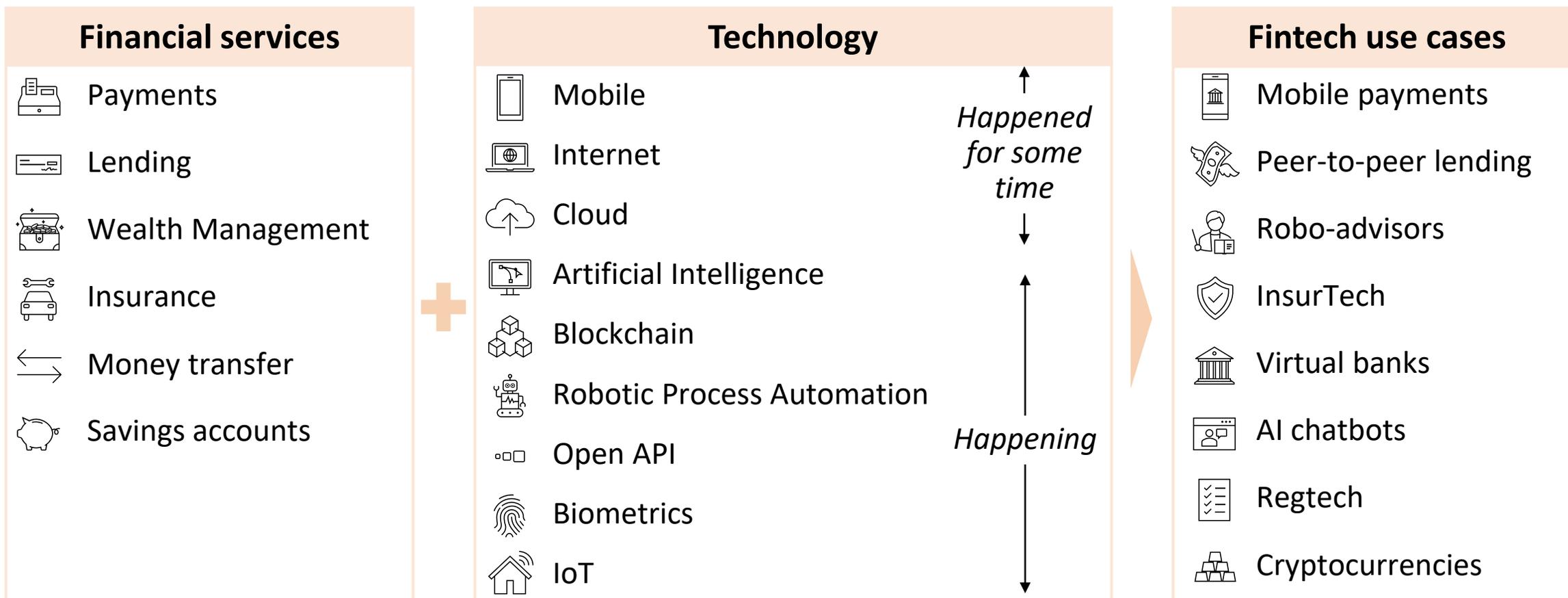
### Net trust in banks to handle personal data %, 2023



Source: YouGov (2023)

# Fintech

This “technology-enabled innovation in financial services” lives on data



81% of fintechs identify data issues as their biggest technical challenge

Source: [BIS](#) (definition); [MIT Management Review](#) (services); [Investopedia](#) & [Mckinsey](#) (services & use cases); [MIT Course “FinTech: Shaping the Financial World”](#) (technology), [Federal Reserve Bank St. Louis](#) (use cases); [InterSystems](#) (Stat)

# Privacy Risks

The reliance on data has privacy implications

## Risks

## Descriptions

## Fintech examples



**Excessive collection of personal data**

- Technology companies tend to collect and retain as much data as possible for analytics
- The data may include personal data

*Virtual banks:* information such as IP addresses, location, online behaviour of users is collected for analytics, delivering personalised services and fraud detection



**Collection and use of personal data without notice or users' meaningful consent**

- Data is **used** or **disclosed** by the providers/operators **beyond users' reasonable expectations or meaningful consent**

*Mobile payment:* phone no., identity card no., location, transaction records may be used for **new purposes such as profiling and credit scoring** and it may involve **sensitive personal data**



**Lack of effective means to erase or rectify obsolete or inaccurate personal data**

- While fintech may **collect and keep as much data** as possible, an effective mechanism for correction might not exist

*Blockchains:* **immutable by design**



**Data security**

- The wealth of personal data stored may well be **treasure troves for hackers**, making individuals susceptible to **impersonations, scams, identity thefts** etc.

*Mobile payment & Open APIs:* transmitting personal data electronically among organizations and end-users, increasing **risk of data leakage/interception**



**Obscurity of the identities of data users and data processors**

- During use and operation, many parties get involved
- Obscurity as to identity of data users and processors **obstructs tracing of liabilities**

*Open API:* **many developers having access** to same individuals' personal data  
*Blockchain:* **no central administrator or authority** to take responsibility

PCPD



HK



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

# Benefits

Imagine that if the risks are contained, the benefits of Fintech can be realised



## Increased consumer trust

- Ethical and safe use of technology can enhance consumers' trust and confidence
- Adoption is up, and existing customers may become loyal customers
- Marketability is up and financial performance rises



## Greater market penetration

- Fairness and inclusion can be achieved to ensure the underprivileged get access to financial services
- Ethical and privacy-friendly nature serves as a competitive advantage



## Regulatory compliance

- Regulatory compliance: help avoid fines and legal issues and help protect reputation



## Innovation

- Strong privacy and ethical practices can attract collaboration opportunities with traditional institutions that face stringent regulations
- Cost savings and efficiency gains

Source: [Int. J. Financial Stud \(2023\)](#); [Tech Ahead](#); [CFA Institute](#); [IME](#)

5

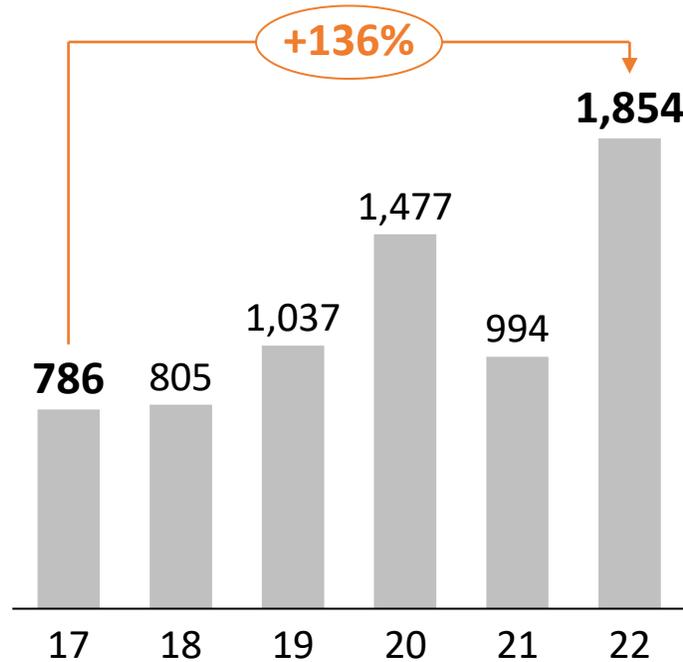
# Global Data Security Crisis

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

## Cyberattacks around the world

### Publicly disclosed cyber attacks

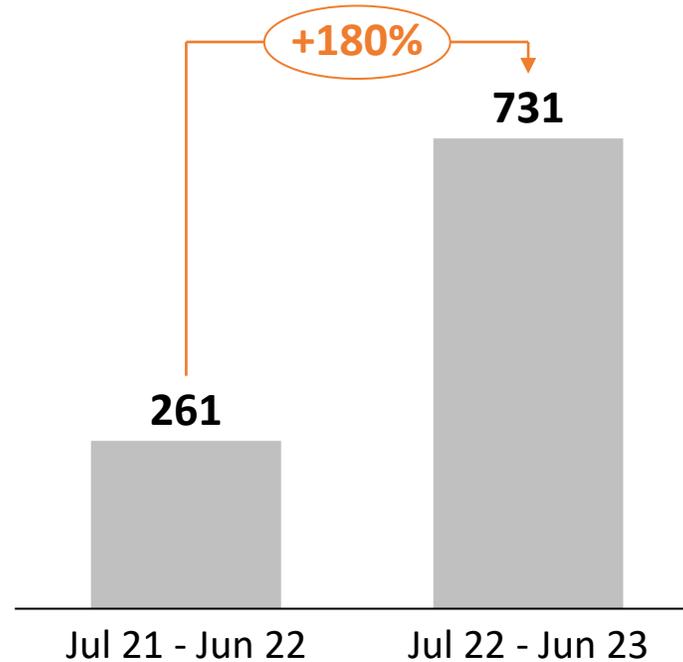
2017 - 2022



Source: [University of Maryland CISSM Cyber Attacks Database](#)

### Cyber attacks in finance in UK

Finance, insurance and credit sector,  
Jun 2021 – Jun 2023

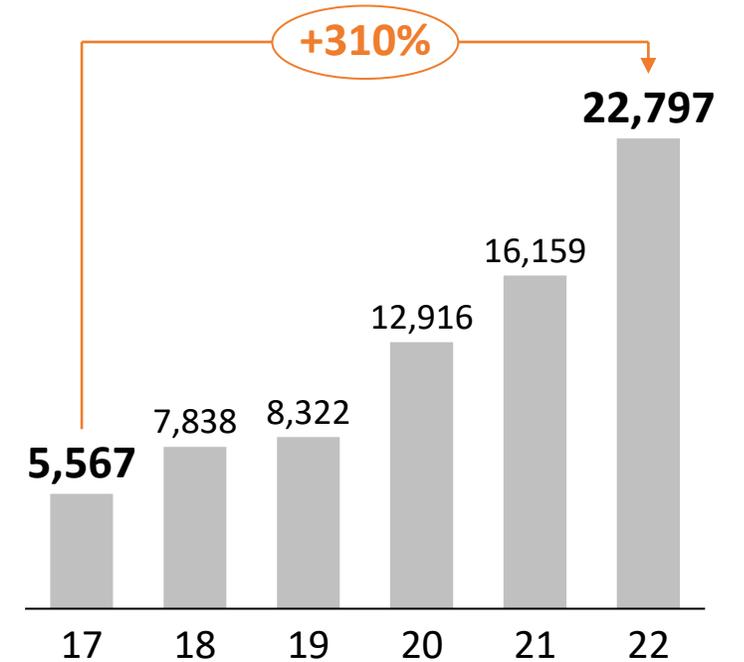


Source: [ICO](#)

## Cybercrimes in HK

### Overall technology crimes in HK

2017 - 2022



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 \(2022\)](#)

Data breach exposes records of 2.5 million student loan borrowers

By Madeline Lauver, Editor in Chief



### Nelnet (2022)

- Hackers reportedly exploited a vulnerability in the system of the student loan service provider
- Data of 2.5 million students, including addresses, phone numbers and social security numbers were breached

Source: [Security Magazine \(2022\)](#)

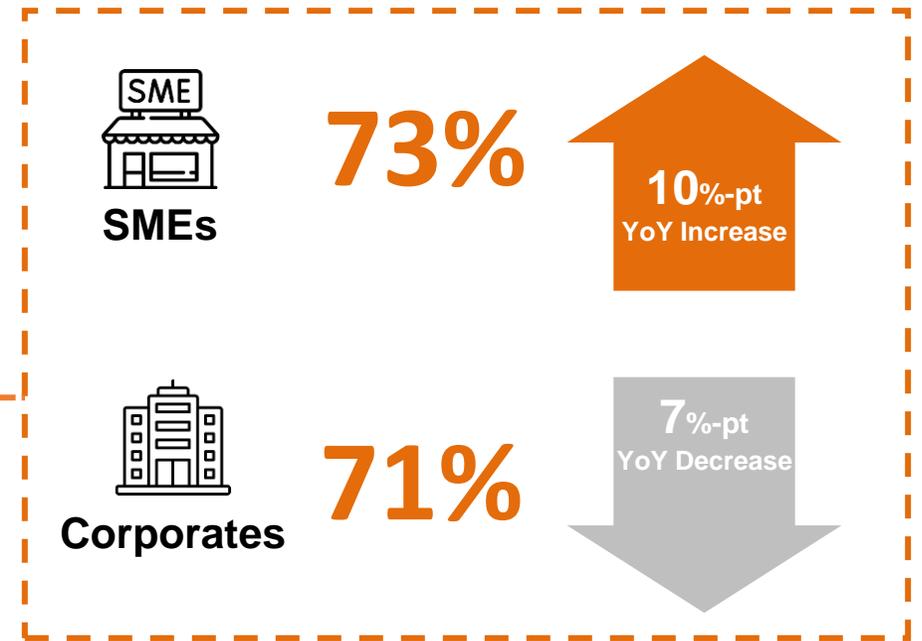
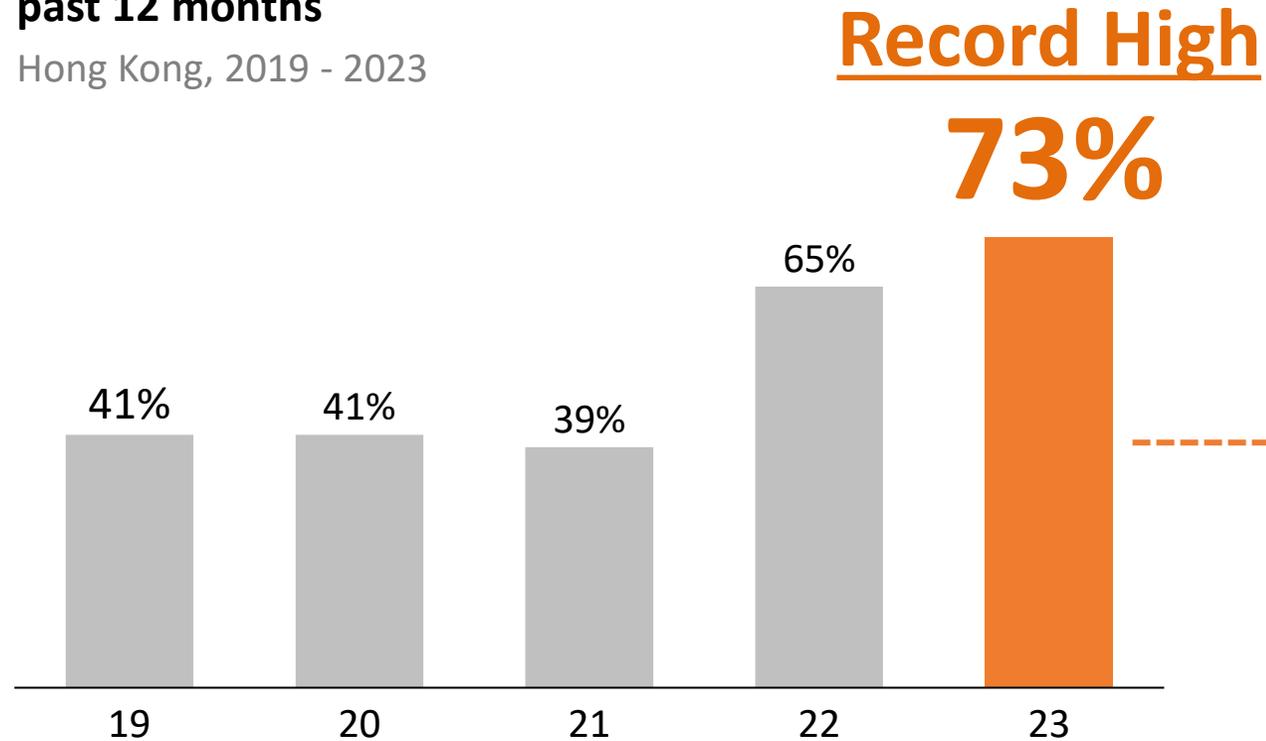
# Local Cyber Security Attacks

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

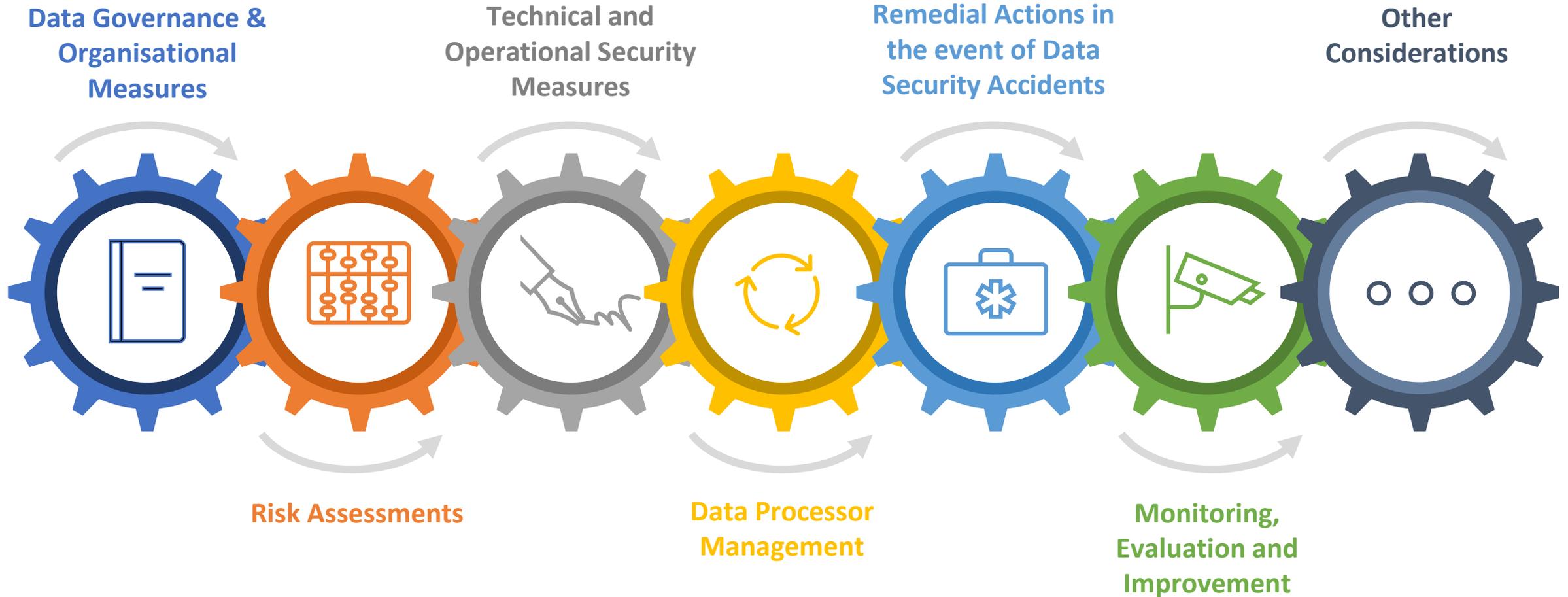
Hong Kong, 2019 - 2023



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

# 7 Recommended Measures

Taking the below measures enhances data security of your organisation



# Inspections and Compliance Checks

PCPD takes proactive actions

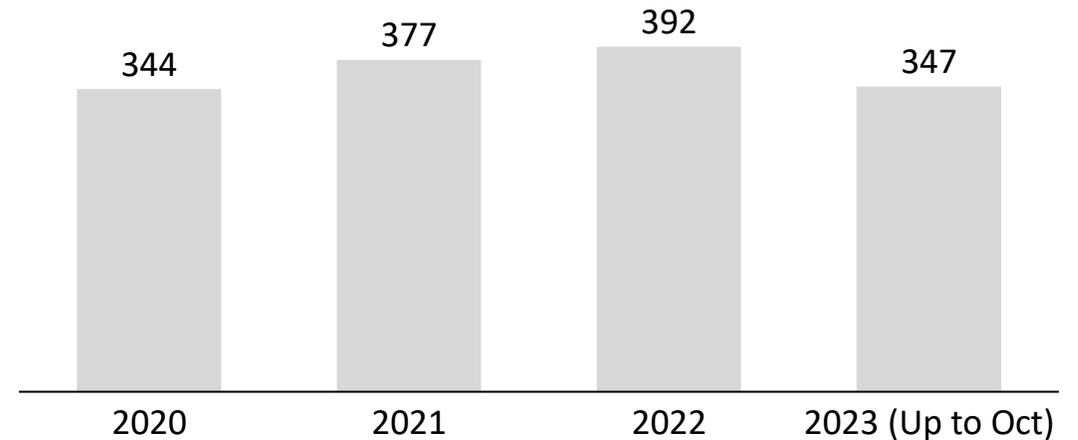
## Inspections

### Inspections by PCPD in the past three years

Report Date	Companies Inspected
9 Oct 23	ZA Bank Limited
20 Sep 23	The Registration and Electoral Office
20 Dec 22	TransUnion Limited
18 Aug 21	(1) CLP Power Hong Kong Limited and (2) The Hongkong Electric Company, Limited

## Compliance checks

### Compliance checks initiated by PCPD



### Selected compliance checks launched in 2023

- All **credit reference agencies**
- Selected **organisations that process personal data** in the development or use of **AI systems**

# Data Breach Response Plan

Putting a plan in place can help minimise impact of a data breach

## What?



A document setting out **how** an organisation should **respond in a data breach**



The plan should outline:

- a **set of procedures** to be followed in a data breach
- **strategy for identifying, containing, assessing and managing** the impact brought about by the incident from start to finish

## Why?



Help ensure a **quick response** to and **effective management** of a data breach

## Elements



Description of what makes a data breach



Internal incident notification procedure



Contact details of response team members



Risk assessment workflow



Containment strategy



Communication plan



Investigation procedure



Record keeping policy



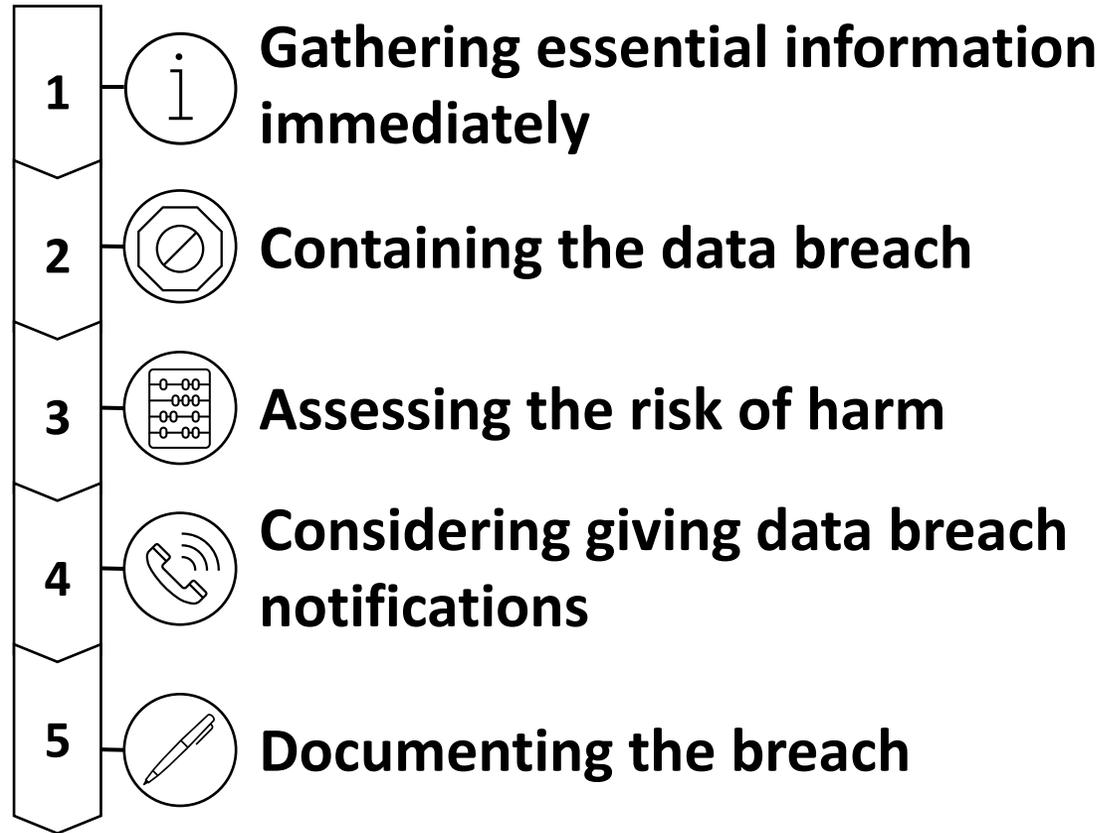
Post-incident review mechanism



Training or drill plan

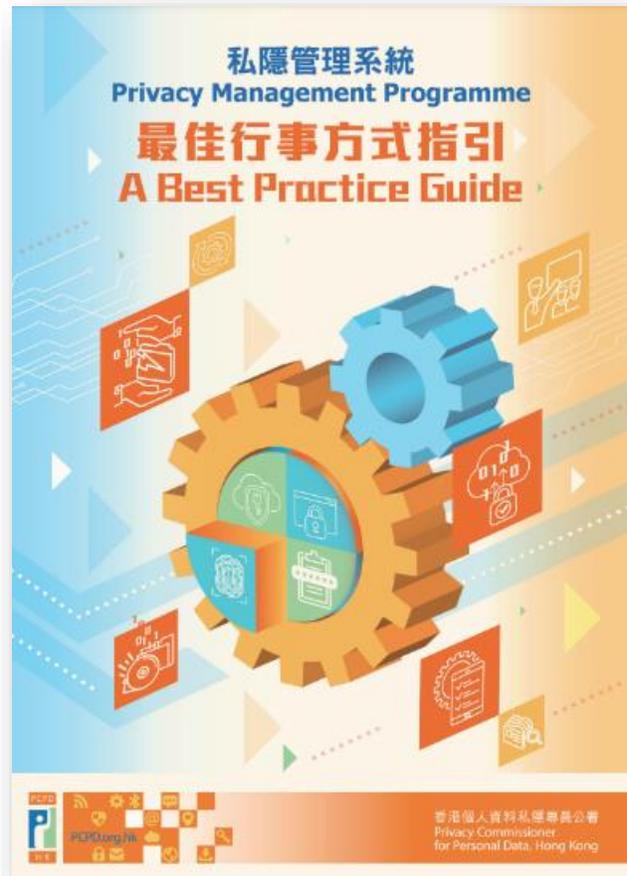
# 5 Steps for Handling Data Breaches

Proper data breach handling and management shows data users' commitment



# Privacy Management Programme (PMP)

## Definition and benefits of adoption



### What's PMP?

A **management framework**

- For the **responsible collection, holding, processing & use of personal data** by the organisation
- To **ensure compliance with Personal Data (Privacy) Ordinance (PDPO)**

### Why PMP?



**Minimise risk of data security incidents**



**Handle data breaches effectively** to minimise damage



**Ensure compliance** with PDPO



**Build trust** with employees and customers, and enhance corporate reputation and competitiveness

**“Guide for Independent Non-Executive Directors” published by HKIoD recommends use of PMP as part of ESG management!**

# 1 Privacy Management Programme: A Best Practice Guide (revised in Mar 2019)



# 3 Guidance on Data Breach Handling and Data Breach Notifications (revised in Jun 2023)



# 2 Guidance Note on Data Security Measures for Information and Communications Technology (Aug 2022)



# 4 Guidance on the Ethical Development and Use of Artificial Intelligence (Aug 2021)



# Thank you



2827 2827



[www.pcpd.org.hk](http://www.pcpd.org.hk)



[communications@pcpd.org.hk](mailto:communications@pcpd.org.hk)

