



MSc Computer Science
RMPP_PCOM7E January 2025

A Framework for Mitigating Data Breach Risk – A Case Study and Solution for SMEs in Hong Kong

Student Name: SIU, Oi Lam Helen
Student ID: 12694914

7 April 2025

Agenda

Significance and Research Problem

Research Question

Aims and Objectives

Key Literature

Methodology

Ethical Considerations

Description of Artefact

Project Timeline

Conclusion and Expected Outcomes

Reference

Project Title: A Framework for Mitigating Data Breach Risk – A Case Study and Solution for SMEs in Hong Kong

Significance and Research Problem

- The rise of cyber risks (HKCERT, 2025) and increasing data breaches (PCPD, 2025) in Hong Kong.
- Small and medium-sized enterprises (SMEs) are increasingly adopting technology but remain unaware of cyber risks (QBE, 2025; Yeung, 2020).
- Increased compliance requirements under the Personal Data (Privacy) Ordinance (PDPO) (DLA Piper, 2025; Lau, 2025; Legislative Council, 2024).

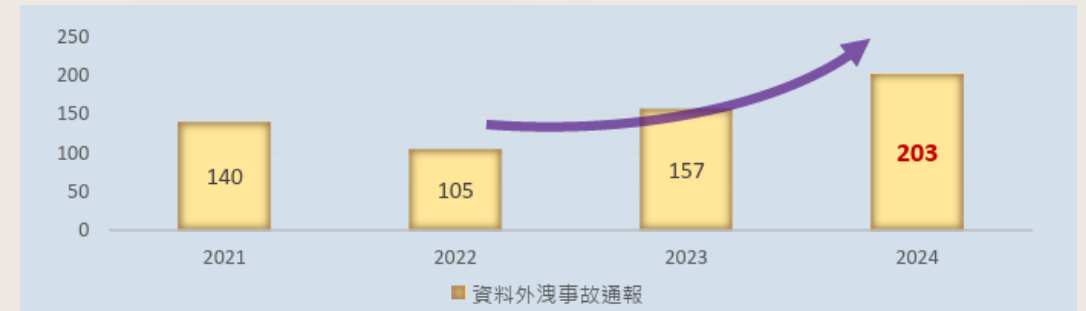


Figure 1: Number of Data Breach Notifications Received (PCPD, 2025)

Research Question

Central Research Question

How can a practical, resource-efficient data breach mitigation framework be designed, implemented, and evaluated to meet the security needs of SMEs in Hong Kong?

Sub-Questions

1. What are the most common vulnerabilities and risk factors leading to data breaches in SMEs?
2. Which recognised standards or frameworks can be suitably adapted for smaller organisations?
3. How can an artefact be developed with minimal technical overhead while still effectively mitigating data breach risks?



Aims and Objectives

Aim

To propose and assess a tailored framework for SMEs.

Objectives

1. Conduct a case study on data breaches in Hong Kong.
2. Adapt existing standards.
3. Design and evaluate a cost-effective solution or toolkit.

Key Literature

Vulnerabilities and Mitigation

- Research on data breach mitigation focused on GDPR compliance (Ashraf, 2021; Brodin, 2019; Kapoor et al., 2018; Mutalib et al., 2021).
- Data breach reports (IBM, 2024; Verizon Business, 2024).

Hong Kong Regulatory Context

- The PDPO, issued by the PCPD in Hong Kong (PCPD, 2022).
- Further reviews of the PDPO (DLA Piper, 2025; Lau, 2025; Legislative Council, 2024).
- Investigation reports published by the PCPD (PCPD, n.d.).

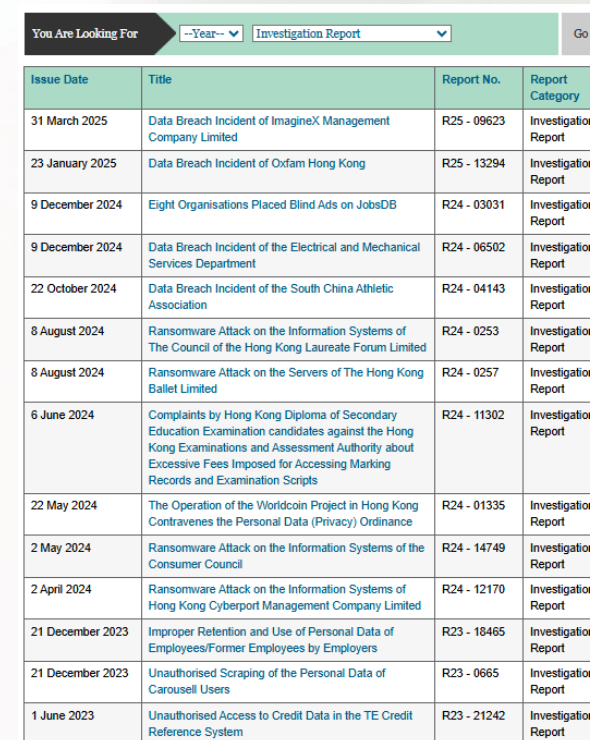
Existing Standards, Guidelines, and Frameworks

- ISO 27001 and ISO 27701 (ISO, 2019; ISO, 2022).
- Local guidelines and programmes on cybersecurity (HKCERT, 2022; HKMA, 2020).

Methodology

Mixed-methods approach

- Case studies of data breaches in Hong Kong (PCPD, n.d.).
- Surveys and interviews with SMEs.
- Adaptation of existing frameworks, such as ISO 27001 and ISO 27701 (ISO, 2019; ISO, 2022).



The screenshot shows the PCPD Investigation Reports website. At the top, there is a search bar with the text "You Are Looking For" and a dropdown menu set to "--Year--". To the right of the search bar is a "Go" button. Below the search bar is a table with four columns: "Issue Date", "Title", "Report No.", and "Report Category". The table lists 15 investigation reports, with the most recent at the top.

Issue Date	Title	Report No.	Report Category
31 March 2025	Data Breach Incident of ImagineX Management Company Limited	R25 - 09623	Investigation Report
23 January 2025	Data Breach Incident of Oxfam Hong Kong	R25 - 13294	Investigation Report
9 December 2024	Eight Organisations Placed Blind Ads on JobsDB	R24 - 03031	Investigation Report
9 December 2024	Data Breach Incident of the Electrical and Mechanical Services Department	R24 - 06502	Investigation Report
22 October 2024	Data Breach Incident of the South China Athletic Association	R24 - 04143	Investigation Report
8 August 2024	Ransomware Attack on the Information Systems of The Council of the Hong Kong Laureate Forum Limited	R24 - 0253	Investigation Report
8 August 2024	Ransomware Attack on the Servers of The Hong Kong Ballet Limited	R24 - 0257	Investigation Report
6 June 2024	Complaints by Hong Kong Diploma of Secondary Education Examination candidates against the Hong Kong Examinations and Assessment Authority about Excessive Fees Imposed for Accessing Marking Records and Examination Scripts	R24 - 11302	Investigation Report
22 May 2024	The Operation of the Worldcoin Project in Hong Kong Contravenes the Personal Data (Privacy) Ordinance	R24 - 01335	Investigation Report
2 May 2024	Ransomware Attack on the Information Systems of the Consumer Council	R24 - 14749	Investigation Report
2 April 2024	Ransomware Attack on the Information Systems of Hong Kong Cyberport Management Company Limited	R24 - 12170	Investigation Report
21 December 2023	Improper Retention and Use of Personal Data of Employees/Former Employees by Employers	R23 - 18465	Investigation Report
21 December 2023	Unauthorised Scraping of the Personal Data of Carousel Users	R23 - 0665	Investigation Report
1 June 2023	Unauthorised Access to Credit Data in the TE Credit Reference System	R23 - 21242	Investigation Report

Figure 2: Investigation Reports published by PCPD (PCPD, n.d.)

Ethical Considerations

- Informed consent and PDPO compliance (UOE, 2018; PCPD, 2022).
- Ensuring confidentiality and the sensitivity of data.
- Anonymised case studies.



Description of Artefact



SME Data Breach Mitigation Toolkit

- Self-assessment checklists.
- Risk scoring spreadsheets.
- PDPO compliance guidance.

Project Timeline

Activity	Weeks 1-4	Weeks 5-8	Weeks 9-12	Weeks 13-16	Weeks 17-20	Week 21-24	Weeks 25-30
Research design finalisation & ethics	X						
Literature review & framework analysis	X	X					
Case study data collection		X	X				
Surveys & interviews		X	X				
Data analysis (qualitative & quantitative)			X	X			
Artefact development (Toolkit creation)				X	X	X	
Feedback & refinement					X	X	
Final write-up and dissemination						X	X

Conclusion and Expected Outcomes

- A practical framework for SME data security.
- Empirical findings on vulnerabilities specific to SMEs in Hong Kong.
- Contribution towards addressing a critical gap in SME cybersecurity.



Reference

Ashraf, S. (2021) GDPR Implementation Framework for SMEs. Available from: <https://www.theseus.fi/handle/10024/493722> [Accessed 30 March 2025].

Brodin, M. (2019) A framework for GDPR compliance for small-and medium-sized enterprises. *European Journal for Security Research* 4: 243-264.

DLA Piper. (2025) Transfer in Hong Kong, SAR. Available form: <https://www.dlapiperdataprotection.com/index.html?t=transfer&c=HK> [Accessed 15 March 2025].

HKCERT. (2022) *Incident Response Guideline for SMEs*. Available from: <https://www.hkcert.org/security-guideline/incident-response-guideline-for-smes> [Accessed 17 February 2025].

HKCERT. (2025) Statistics. Available from: <https://www.hkcert.org/statistic> [Accessed 15 March 2025].

HKMA. (2020) HKMA launches Cybersecurity Fortification Initiative 2.0. Available from: <https://www.hkma.gov.hk/eng/news-and-media/press-releases/2020/11/20201103-4/> [Accessed 13 March 2025].

IBM. (2024) Cost of a Data Breach Report. Available from: <https://www.ibm.com/reports/data-breach> [Accessed 17 February 2025].

ISO. (2019) ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Available from: <https://www.iso.org/standard/71670.html> [Accessed 20 March 2025]

ISO. (2022) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Available from: <https://www.iso.org/standard/27001> [Accessed 20 March 2025]

Kapoor, K., Renaud, K., & Archibald, J. (2018). 'Preparing for GDPR: helping EU SMEs to manage data breaches', *2018 AISB Convention: Symposium on Digital Behaviour Intervention for Cyber Security*. 5 April 2018. Liverpool, United Kingdom: AISB. 13-20.

Lau, C. (2025) Hong Kong alert to data protection challenges as technology evolves: a 2025 update on privacy laws. Available from: <https://www.rs-lawyers.com.hk/post/hong-kong-privacy-laws-update> [Accessed 13 March 2025].

Legislative Council. (2024) Panel on Constitutional Affairs - Meeting on 19 February 2024: Background brief on the work of the Office of the Privacy Commissioner for Personal Data. LC Paper No. CB(2)157/2024(03)

Mutalib, M. M. A., Zainol, Z., & Halip, M. H. M. (2021). 'Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework', *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*. 1-3 December 2021. Kedah, Malaysia: IEEE. 1-6

Thank you

MSc Computer Science
RMPP_PCOM7E January 2025

Student Name: SIU, Oi Lam Helen
Student ID: 12694914