Research Proposal Outline

(Word count: 509)

Project Title

A Framework for Mitigating Data Breach Risks: A Case Study and Solution for SMEs in Hong Kong.

Background

During a recent literature review on "Financial Impact of Ransomware and Malware in Hong Kong," an alarming rise in data breaches affecting small and medium-sized enterprises (SMEs), including smaller non-governmental organisations (NGOs), was highlighted. Owing to limited resources and expertise, SMEs often struggle to implement effective data security protocols, making them prime targets for cyberattacks. Although ample research examines large-scale breaches in other regions, fewer studies focus on smaller local entities in Hong Kong, which must comply with the Personal Data (Privacy) Ordinance (PDPO). Many existing guidelines likewise cater primarily to large corporations with extensive IT infrastructures and often rely on frameworks design for other jurisdictions. Consequently, there is a clear need for a bespoke, accessible risk mitigation framework that addresses the specific requirements of SMEs in Hong Kong.

Research Question

<u>**Central Research Question**</u>

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. Which vulnerability and risk factors most frequently lead 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

Overall Aim

To propose and assess a tailored, cost-effective framework that strengthens data breach resilience in SMEs in Hong Kong.

Objectives

1. Conduct a detailed case study of an Hong Kong data breach incident to determine key vulnerabilities and root causes.

2. Examine and adapt existing data protection standards (e.g., ISO 27001, ISO 27701, etc.) for an SME context, ensuring that proposed controls remain feasible and affordable.

3. Design and evaluate a practical solution or toolkit for risk assessment and breach prevention, aligned with recognised security guidelines.

Methodology / Development Strategy / Research Design

A qualitative or mixed-methods approach will be employed. This may include a case study analysis of SMEs data breach in Hong Kong, supplemented by interviews or surveys with SME stakeholders where feasible. Relevant documents—such as industry reports and prevailing security guidelines—will also be critically reviewed. The research will examine how current frameworks (ISO 27001, ISO 27701) can be adjusted to suit SMEs in terms of technical complexity, financial costs, and ease of adoption.

Description of artefacts

To support SMEs in enhancing their security posture, a prototype "SME Data Breach Mitigation Toolkit" will be created. This artefact is intended to help businesses systematically assess risks, prioritise actions, and track compliance. The toolkit will incorporate self-assessment checklists targeting common SME vulnerabilities, a spreadsheet-based risk scoring model for evaluating overall exposure, and clear guidance linking recommended controls to well-established cybersecurity standards. Real-world examples and scenarios will be included to illustrate how each proposed measure can be applied with minimal technical overhead. This structured solution aims to empower SMEs by providing an accessible, cost-effective avenue for ongoing risk assessment and data breach prevention, thus fulfilling both academic and practical needs.

Bibliography

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. (2024) Ransomware's New Front: Uncovering the Latest Threats Facing Hong Kong. Available from: https://www.hkcert.org/blog/ransomware-s-new-front-uncovering-the-latest-threats-facing-hong-kong [Accessed 15 March 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]

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].

PCPD. (2022) *The Ordinance: Personal Data (Privacy) Ordinance (Cap. 486). Government of the Hong Kong Special Administrative Region.* Available from: https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html [Accessed 2 March 2025].

PCPD. (n.d.) Enforcement Reports. Available from: https://www.pcpd.org.hk/english/enforcement_reports/report.html [Accessed 2 March 2025].

QBE. (2025) Hong Kong SMEs face rising business costs and rapidly evolving cyber risks, while AI is thought to significantly impact business productivity, finds QBE Hong Kong annual SME survey. Available from: https://www.qbe.com/hk/en/newsroom/press-releases/qbe-hong-kong-sme-survey-results-business-outlook-2025 [Accessed 13 March 2025].

Verizon Business. (2024) *Data Breach Investigations Report.* Available from: https://www.verizon.com/business/resources/reports/dbir/ [Accessed 3 March 2025].