Literature Review Outline

(Word count: 481)

Topic

Financial Impact of Ransomware and Malware in Hong Kong**.**

Focus and Aim

This literature review investigates the short- and long-term financial implications of ransomware and malware attacks on organisations in Hong Kong. It aims to consolidate current academic research, industry findings, and case studies to reveal the nature of these costs and evaluate the effectiveness of mitigation measures. The primary audience includes academic researchers, lecturers, cybersecurity professionals, and risk managers seeking a thorough understanding of local cyber threat repercussions.

Rationale and Significance

Hong Kong's status as a major economic centre in Asia highlights the urgency of comprehending how ransomware and malware incidents affect businesses. By examining direct and indirect losses, this review intends to guide policy decisions and resource planning at both institutional and governmental levels, thereby promoting stronger cybersecurity practices in the region (Dupont et al, 2023).

Context, Perspective, and Analytical Framework

Owing to its digitally advanced and globally linked financial systems, Hong Kong remains particularly susceptible to cyberattacks (FSDC, 2021). From a socio-economic viewpoint, ransomware and malware are not solely technical issues but also present extensive business challenges. Their financial repercussions surpass initial ransom and system recovery costs, extending to reputational damage, regulatory fines, and operational delays (August et al, 2022; IBM, 2024).

A thematic structure underpins the literature search (George, 2023), covering:

- Direct costs: negotiation, restoration
- Indirect costs: reputational damage, cyber insurance premiums
- Mitigation strategies: continuity planning, technical solutions
- Ongoing debates: ethics of ransom payment (Everett, 2016), reliance on insurance (Shackelford, 2012)

Source Location and Selection Criteria

Sources are drawn mainly from academic databases such as UoE Library, IEEE Xplore and Google Scholar, supplemented by key Hong Kong specific organisations, such as the Hong Kong Computer Emergency Response Team (HKCERT, n.d.), the Hong Kong Monetary Authority (HKMA, n.d.) , and other governmental sources. Search terms include “ransomware”, “malware”, “financial impact”, “Hong Kong”, “cybersecurity”, “cyber insurance” and “economic loss”. Preference is given to studies from the past decade to capture the evolving nature of threats and defences; works containing empirical evidence or explicit cost data are prioritised.

Structure of the Review

1. **Introduction** – States the rationale and main aims
2. **Context and Scope** – Outlines Hong Kong's digital environment and regulations
3. **Direct Financial Impacts** – Examines ransom payments, restoration costs, and legal liabilities
4. **Indirect Financial Consequences** – Reviews reputational damage, rising insurance costs, and staff training
5. **Mitigation Measures** – Discusses security frameworks, continuity planning, and cyber insurance (Marsh & McLennan, n.d.)
6. **Critical Perspectives** – Addresses debates about paying ransoms and reliance on insurance
7. **Gaps and Future Directions** – Emphasises SME concerns and the necessity of longitudinal studies (Paavilainen & Raukko, 2008)
8. **Conclusion** – Summarises key outcomes and suggests further exploration or policy changes

Strengths and Limitations

Emerging empirical case studies increasingly shed light on the financial ramifications of cyberattacks. Nonetheless, reputational fears often lead to underreporting, hindering accurate cost estimations and highlighting the need for more transparent, up-to-date data.

Reference

August, T., Dao, D. & Niculescu, MF. (2022) Economics of Ransomware: Risk Interdependence and Large-Scale Attacks. *Management Science.* 68(12):8979-9002. DOI: https://doi.org/10.1287/mnsc.2022.4300

Dupont, B., Shearing, C., Bernier, M. & Leukfeldt R. (2023) The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security*. 132(103372): 1-17. DOI: https://doi.org/10.1016/j.cose.2023.103372.

Everett, C. (2016) Ransomware: to pay or not to pay? *Computer Fraud & Security*. 2016(4): 8-12. DOI: https://doi.org/10.1016/S1361-3723(16)30036-7.

FSDC. (2021) *Cybersecurity Strategy for Hong Kong's Financial Services Industry*. Available from: https://www.fsdc.org.hk/en/insights/cybersecurity-strategy-for-hong-kong-s-financial-services-industry [Accessed 16 February 2025].

George, E. (2023) How to Write a Thematic Literature Review: A Beginner's Guide. Available from: https://researcher.life/blog/article/how-to-write-a-thematic-literature-review-a-beginners-guide/ [Accessed 20 February 2025 2025].

HKCERT. (n.d.) Hong Kong Computer Emergency Response Team Coordination Centre. Available form: https://www.hkcert.org/ [Accessed 16 February 2025].

HKMA. (n.d.) Welcome to Hong Kong Monetary Authority. Available form: https://www.hkma.gov.hk/eng [Accessed 16 February 2025].

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

Marsh & McLennan. (n.d.) Cyber Insurance – Innovative insurance brokerage services and tools can help companies effectively transfer cyber risk. Available at: https://www.marsh.com/en/services/cyber-risk/expertise/cyber-insurance.html [Accessed 17 Feb. 2025].

Paavilainen, E. & Raukko, M. (2008) 'Longitudinal Research Methods Approaches in International Business - A Typology', *7th European Conference on Research Methodology for Business and Management Studies.* Regent's College, London, 19-20 June 2008. UK: Academic Publishing Limited. 237-244.

Shackelford, SJ. (2012) Should your firm invest in cyber risk insurance? *Business Horizons.* 55(4): 349-356. DOI: https://doi.org/10.1016/j.bushor.2012.02.004.

Bibliography

Healey, M., Matthews, K., & Cook-Sather, A. (2020) *Writing about learning and teaching in higher education: Creating and contributing to scholarly conversations across a range of genres*. Center for Engaged Learning Open-Access Books, Elon University. 142-152.

HKCERT. (2024) *Hong Kong Security Watch Report 2024 Q3*. Available from: https://www.hkcert.org/watch-report/hong-kong-security-watch-report-q3-2024

[Accessed 17 February 2025]