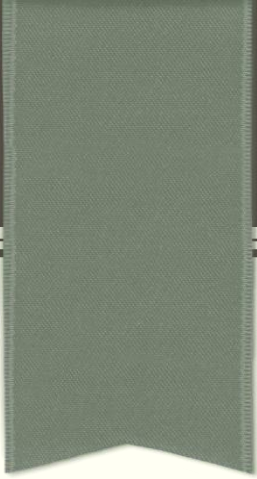


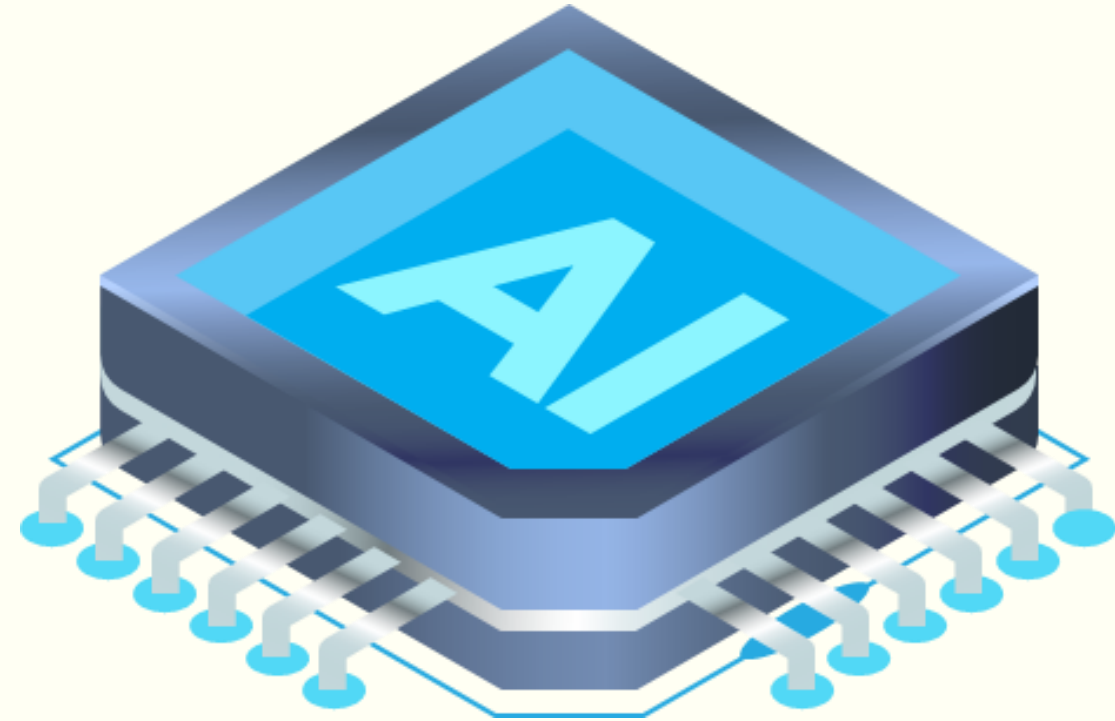
LEVEL 7 ASSESSMENT SPECIFICATION

Student name:	Chiang Chun Wah	Student ID number:	2119645
Programme:	DBA		
Module:	Advancing to Doctoral Research Stage		
Module code:	HKBM7022	Contribution to Overall Module Assessment (%):	40%
Lecturer:	Prof Peter Fong	Internal Verifier:	Dr Andrew Chan
Assignment Title:	Impact of Machine Learning on Cybersecurity Operational Efficiency in Hong Kong Banking Sector	Word count (or equivalent):	18 minutes
Submission deadline:	13 March 2025 (Submission of PPT) 15 March 2025 (Presentation)	Return date of provisional marks & written feedback:	15 April 2025 (Tentative)
Submission method:	All written assessments, where practical and possible, must be submitted via Turnitin unless otherwise instructed by the Lecturer. (Please DO NOT put this assessment specification into Turnitin or it will match many similarities with other students' submissions.) Alternative submission method (if applicable): Late submission of the assessment will result in a late penalty mark. Work which is submitted up to 1 week late will be capped at 50% for the first attempt and will be awarded a mark of 0% for re-assessment. Late submission penalties may be lifted only if there is an approved extenuating circumstances claim. Work submitted more than 1 week late will be considered as a non-submission and will not be marked. The work may be considered as a submission for reassessment if offered by an Examining Board or if there is an approved extenuating circumstances claim.		
Academic honesty / referencing:	Academic honesty is required. In the main body of your submission you must give credit to authors on whose research and ideas your work is based. Append to your submission a reference list that indicates the books, articles, etc. that you have used, cited or quoted in order to complete this assessment.		



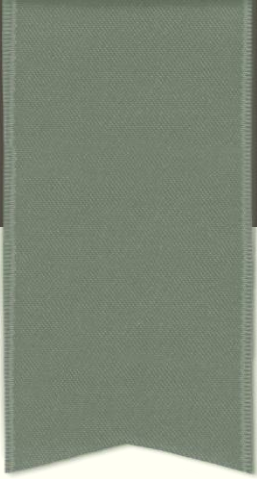
IMPACT OF MACHINE LEARNING ON CYBERSECURITY OPERATIONAL EFFICIENCY IN HONG KONG BANKING SECTOR

Student Name: Chiang Chun Wah (2119645)
Module: HKBM7022
Lecturer: Prof. Peter Fong



Agenda

- Research Proposal Summary
- Critical Evaluation of the Research Proposal
- Alternative Research Methods
- Expected Findings and Contributions



RESEARCH PROPOSAL SUMMARY

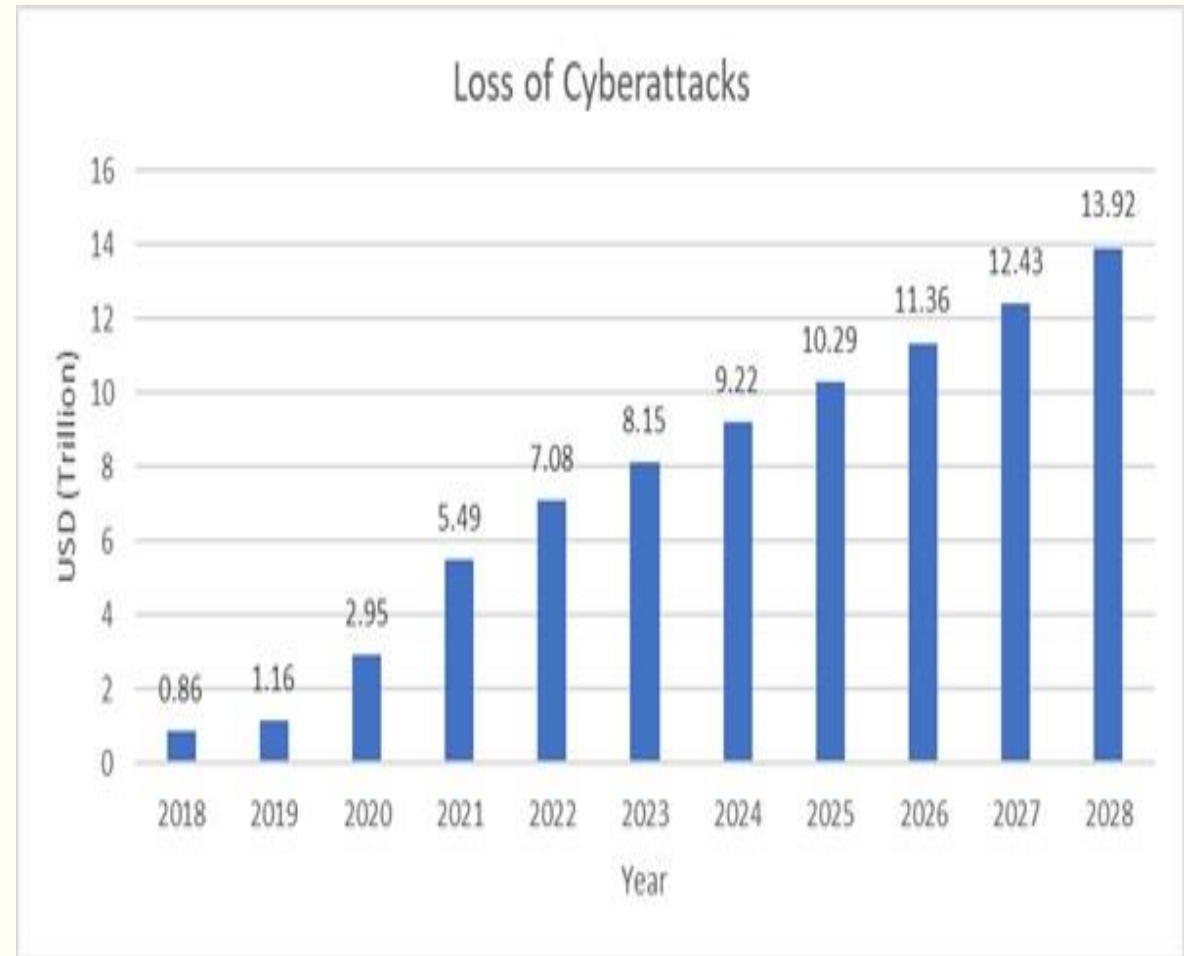
Research Background

- AI is becoming a powerful technology that will greatly impact the future (Kelly, Kaye and Oviedo-Trespalacios, 2023).
- Tools such as ChatGPT, Copilot, and DeepSeek are examples of this innovative progress.
- However, AI is like a two-sided sword.
 - One side: It increased the organization's proactivity.
 - On the other side: Hacker uses it to launch cyberattacks.

Research Background

External Environment:

- Refer to the Statista report (Statista, 2024), the financial loss due to cyberattacks will increase significantly in the next four years.
- Losses forecasted to grow from around USD 9 to 14 trillion.
- Cyberattack frequency and severity are increasing each year (Charlton, 2024).
- It is a significant global challenge.
- It is a wake-up bell for cybersecurity professionals and organizations.



Research Background

Problems in the Organization:

- Many organizations rely on legacy security systems and methods to analyze the threats (Shwede, Malaka and Rwashdeh, 2023).
- These legacy methods are inadequate against modern cyberattacks.
- At the same time, there is a lack of skilled cybersecurity professionals in the job market (Meineke, 2024).

This problem needs to be solved quickly, and immediate action is necessary.

Research Objectives

Research Aim:

To assess the impact of machine learning (ML) on cybersecurity operational efficiency, focusing on the banking sector in Hong Kong.

Significance:

As technological innovation accelerates, ML offers opportunities for enhanced cybersecurity, which is critical for protecting banking assets.

Research Objectives

Research Objectives:

- Understanding of ML applications that can be applied in banking information systems.
- Utilizing machine learning improves the operational effectiveness of cybersecurity for the bank.
- Identifying the role of ML in cybersecurity's operations, and demonstrate how ML reduces human involvement while speeding up the detection and shortening response times.

Research Questions

Research Questions:

- RQ1: What ML features can be used in cybersecurity work?
- RQ2: How does ML improve the efficiency of cybersecurity in the banking sector?
- RQ3: What is the position of ML in cybersecurity operations?

Literature Review Summary

Key Themes:

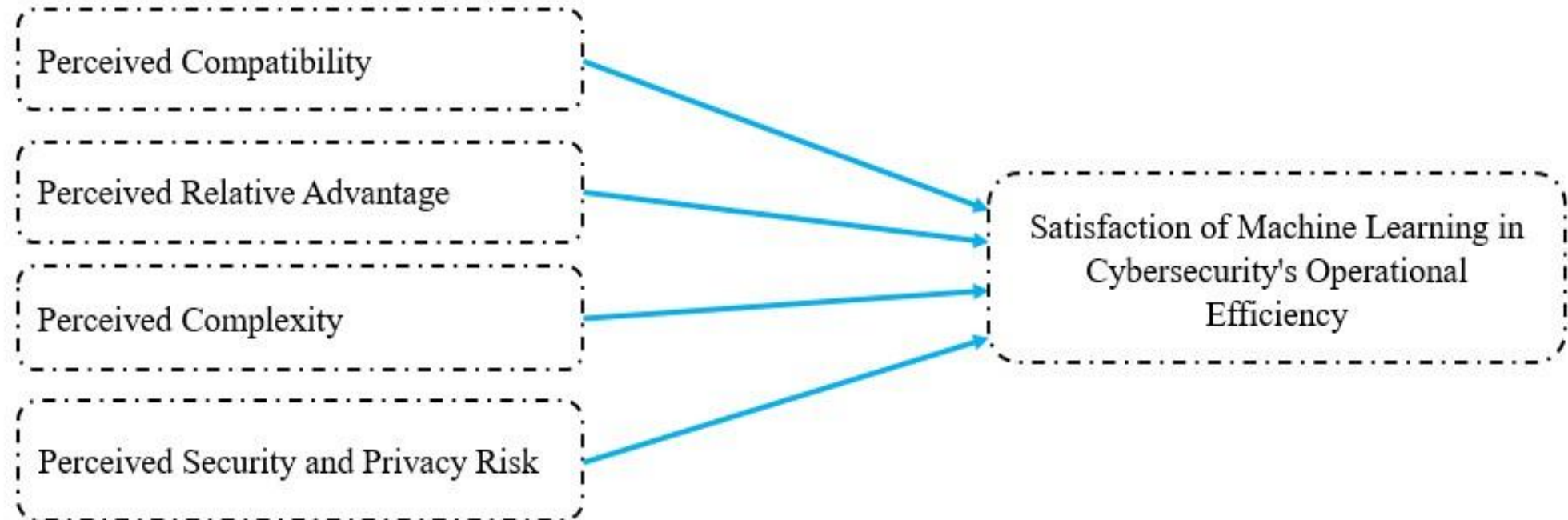
- Machine Learning Model
 1. Supervised (Sarker, 2021)
 2. Unsupervised (Taha, 2023)
 3. Semi-supervised (Sarker, 2021)
- Machine Learning Techniques in Cybersecurity
 1. Threat prevention (Li et al., 2019)
 2. Threat detection (Apruzzese et al., 2023)

Literature Review Summary

Key Themes:

■ Theoretical Framework

Based on Diffusion of Innovations (DOI) theory, which explains the adoption of new technologies (Shaikh et al., 2023).



Literature Review Summary

Research Gap:

- Previous studies are focus on static threat analysis.
- Limited studies analyzing the intersection of ML and cybersecurity in the Hong Kong banking sector.

Research Design and Methodology

Approach:

Combining existing theoretical and practical experiments.

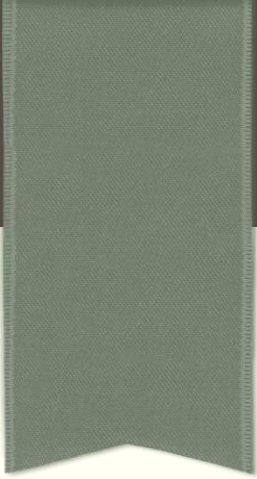
Methods:

Mixed-methods approach

1. Qualitative: Interviews and focus groups for insights and recommendations (Abraham et al., 2022).
2. Quantitative: Surveys and statistical analysis for measurable outcomes (Apuke, 2017).

Data Sources:

Combination of primary data (interviews, focus group and survey) and secondary data (literature review from textbook, journal, article, etc.)



CRITICAL EVALUATION OF THE RESEARCH PROPOSAL

Critical Evaluation of the Research Proposal

Strengths:

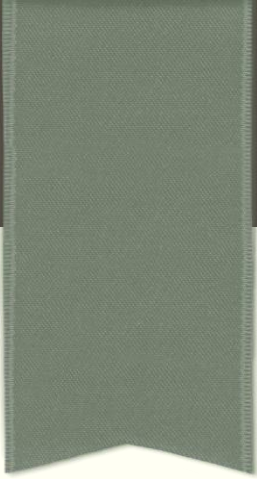
- Use of mixed-methods enhances result validity (Ijadi Maghsoodi et al., 2024).
- Focus on the high-priority area of cybersecurity in banking.
- Established effectiveness of ML in cybersecurity applications.

Weaknesses:

- Reliance on existing DOI theory to form a framework.
- General feedback from the respondents in survey.

Limitations:

- Compatibility challenges between new and legacy banking systems.



ALTERNATIVE RESEARCH METHODS

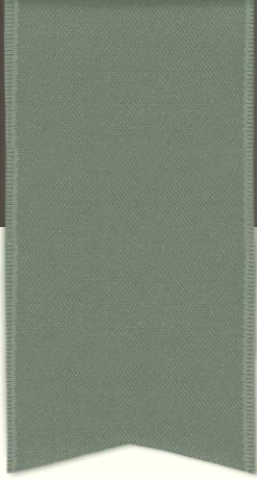
Alternative Research Methods

Proposed Alternative: Case Study Approach

- In-depth analysis of specific banks in Hong Kong.
- Detailed examination of practical challenges and successes in implementing machine learning.

Addressing Shortcomings:

- Overcomes theoretical limitations by focusing on practical implementation.
- Reduces data collection barriers by involving participants in the process.



EXPECTED FINDINGS AND CONTRIBUTIONS

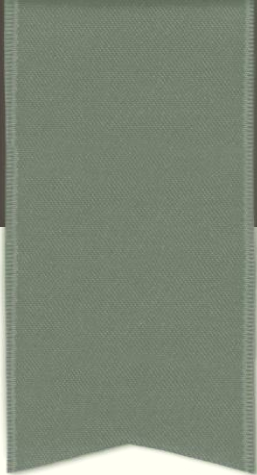
Expected Findings and Contributions

Expected Findings:

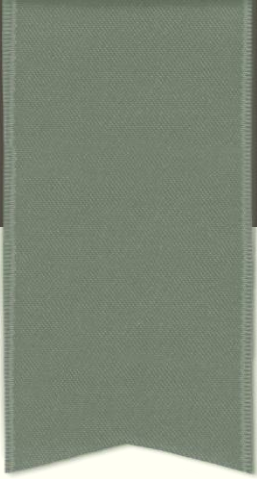
- Determining the position of ML in cyber-defense operations.
- ML significantly enhances cybersecurity operational efficiency by detecting and preventing threats more effectively.

Contributions:

- Provide invaluable insight for banking institutions' executives, Chief Information Officer (CIO), the Chief Information Security Officer (CISO), and other security stakeholders. Guidance they decide on introducing ML in their organization cybersecurity strategies.
- Provides actionable insights for cybersecurity professionals to integrate ML.



THANK YOU!!



Q&A

Reference

Abraham, M. *et al.* (2022) 'Implications of XR on Privacy, Security and Behaviour: Insights from Experts', *ACM International Conference Proceeding Series* [Preprint]. Available at: <https://doi.org/10.1145/3546155.3546691>.

Apruzzese, G. *et al.* (2023) 'The Role of Machine Learning in Cybersecurity', *Digital Threats: Research and Practice*, 4(1). Available at: <https://doi.org/10.1145/3545574/ASSET/C4586A69-4437-435A-9DE6-E5F12828847D/ASSETS/GRAPHIC/DTRAP-2021-0064-F15.JPG>.

Apuke, O.D. (2017) 'Quantitative Research Methods : A Synopsis Approach', *Kuwait Chapter of Arabian Journal of Business and Management Review*, 6(11), pp. 40–47. Available at: <https://doi.org/10.12816/0040336>.

Charlton, E. (2024) *2023 was a big year for cybercrime – here's how we can make our systems safer* | *World Economic Forum*. Available at: <https://www.weforum.org/stories/2024/01/cybersecurity-cybercrime-system-safety/> (Accessed: 26 January 2025).

Ijadi Maghsoodi, A. *et al.* (2024) 'What Makes Effective Acute Geriatric Care? - A mixed Methods Study From Aotearoa New Zealand', *Ageing International*, 49(3), pp. 660–683. Available at: <https://doi.org/10.1007/S12126-024-09568-7/FIGURES/1>.

Kelly, S., Kaye, S.A. and Oviedo-Trespalacios, O. (2023) 'What factors contribute to the acceptance of artificial intelligence? A systematic review', *Telematics and Informatics*, 77, p. 101925. Available at: <https://doi.org/10.1016/J.TELE.2022.101925>.

Li, J. *et al.* (2019) 'The Approaches of Prevention, Detection, and Response for Cybersecurity of I&C Systems in NPPs', *Lecture Notes in Electrical Engineering*, 507, pp. 283–290. Available at: https://doi.org/10.1007/978-981-13-3113-8_33.

Reference

Meineke, M. (2024) *Tackling cybersecurity's global talent shortage: Report | World Economic Forum*. Available at: <https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/> (Accessed: 26 January 2025).

Sarker, I.H. (2021) 'Machine Learning: Algorithms, Real-World Applications and Research Directions', *SN Computer Science*, 2(3), pp. 1–21. Available at: <https://doi.org/10.1007/S42979-021-00592-X/FIGURES/11>.

Shaikh, I.M. *et al.* (2023) 'ISLAMIC BANK CUSTOMERS' ADOPTION OF DIGITAL BANKING SERVICES: EXTENDING DIFFUSION THEORY OF INNOVATION', *Journal of Islamic Monetary Economics and Finance*, 9(1), pp. 57–70. Available at: <https://doi.org/10.21098/JIMF.V9I1.1545>.

Shwede, F., Malaka, S. and Rwasheh, B. (2023) 'The Moderation Effect of Artificial Intelligent Hackers on the Relationship between Cyber Security Conducts and the Sustainability of Software Protection: A Comprehensive Review', *Migration Letters*, 20. Available at: <https://doi.org/10.59670/ML.V20IS9.4947>.

Statista (2024) *Cybersecurity - Worldwide | Statista Market Forecast*. Available at: <https://www.statista.com/outlook/tmo/cybersecurity/worldwide> (Accessed: 26 January 2025).

Taha, K. (2023) 'Semi-supervised and un-supervised clustering: A review and experimental evaluation', *Information Systems*, 114, p. 102178. Available at: <https://doi.org/10.1016/j.is.2023.102178>.