PAPER NAME	AUTHOR
Proposal for Final Project.docx	132789212 607877401
WORD COUNT	CHARACTER COUNT
424 Words	2811 Characters
PAGE COUNT	FILE SIZE
4 Pages	18.8KB
SUBMISSION DATE	REPORT DATE
Oct 27, 2025 6:52 PM UTC	Oct 27, 2025 6:53 PM UTC

● 4% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 3% Internet database
- Crossref database
- 3% Submitted Works database
- 0% Publications database
- Crossref Posted Content database

● Excluded from Similarity Report

- Bibliographic material
- Quoted material

Proposal for Final Project: Future Trends in Cyber Risk

Student's Name

Institution Name

Course Name

Instructor's Name

Due Date

Proposal for Final Project: Future Trends in Cyber Risk

Thesis Statement and Question: The paper will focus on the following question: What does the incorporation of artificial intelligence (AI) and quantum computing into the present-day realm of cyber risk change the existing situation by exposing organizations to more vulnerabilities in the form of AI-driven attacks and encryption breaches, and what strategic reaction should organizations take, based on course concepts such as risk quantification and executive leadership, to help mitigate these developing threats?

Overview

It will be premised on Course Units 4 (Quantifying Cyber Risk) and 14 (Emerging Trends and Technologies), discussing how AI enables more advanced threats, such as deepfakes and automated phishing, and questions traditional encryption with the implementation of quantum computing (Poremba, 2025). The companies must take a more proactive stance and combine risk modeling, as presented in "How to Measure Anything in Cyber Risk," with buy-in from the board of directors, as outlined in "A Leader's Guide to Cybersecurity" (Cybersecurity Considerations 2025, 2025). The paper argues that in half or more of the financial and operational effects of cyber-attacks, without adaptive controls such as zero-trust design and AI-based defenses, cyber threats can significantly influence the financial and operational impacts in high-stakes sectors like finance and healthcare (Ejjami, 2024).

Research Plan

To facilitate this analysis, I will summarize the course materials, including case studies, Study.net, and lectures on building risk programs (Units 2-3). In order to consider future trends, I will continue researching one of the reputable reports and industry forecasts. This includes the screening predictions on the two-sidedness of AI in attacks and defenses, as well as trolling cyber tensions between geopolitics and quantum hazards. It has enough content that selected publications of trends, implications, leading indicators, and organizational reactions can confirm. This literature will also be the basis for estimating the cost of valuable resources, with some examples being training budgets and technology investments (Jurgens & Dal Cin, 2025). The other stipulation will also include an equal treatment of gaps, advantages, and tactful moves for advantage as the implementation plan begins in 2026.

References

Cybersecurity considerations 2025. (2025). KPMG. https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2025.html

Ejjami, R. (2024). Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives. *Journal of Next-Generation Research 5.0*. https://doi.org/10.70792/jngr5.0.v1i1.5

Jurgens, J., & Dal Cin, P. (2025). Global Cybersecurity Outlook 2025. In the *World Economic Forum*. World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Poremba, S. (2025, January 9). *Cybersecurity trends ibm predictions 2025*. Ibm.com. https://www.ibm.com/think/insights/cybersecurity-trends-ibm-predictions-2025

● 4% Overall Similarity

Top sources found in the following databases:

- 3% Internet database
- Crossref database
- 3% Submitted Works database
- 0% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	coursehero.com Internet	3%
2	University of North Texas on 2025-09-04 Submitted works	1%