132789212 607877401

Proposal for Final Project.docx

Turnitin

Document Details

Submission ID

trn:oid:::22779:118722450

Submission Date

Oct 28, 2025, 1:22 AM GMT+6:30

Download Date

Oct 28, 2025, 1:23 AM GMT+6:30

File Name

Proposal_for_Final_Project.docx

File Size

18.8 KB

4 Pages

424 Words

2,811 Characters

0% detected as AI

The percentage indicates the combined amount of likely AI-generated text as well as likely AI-generated text that was also likely AI-paraphrased.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Detection Groups

0 AI-generated only 0%
Likely AI-generated text from a large-language model.

0 AI-generated text that was AI-paraphrased 0%
Likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

Disclaimer
Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

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