MTFC Project Proposal 2024-25

Team Name	Ctrl+ Alt + Predict
Team ID #	191718

MTFC Project Proposal Template Use Notes:

- *Refer to the official MTFC Project Proposal Prompts 2024-25 for the 15 prompts and scoring instructions.*
- *The use of this template is OPTIONAL.*
    - *It is provided as an optional resource for teams to keep their Project Proposal response organized. Teams who wish to use this template should make a copy in order to edit.*
- *The final version of the team's MTFC Project Proposal should be downloaded as a PDF or Word document to submit on the ICS Dashboard. A single file will be submitted.*
- *Additional resources (including the Actuarial Process Guide) can be found on the Modeling the Future Challenge website: https://www.mtfchallenge.org/resources/*
- *Please direct any questions to challenge@mtfchallenge.org.*

Part 1: Project Definition *(Team's Topic)*

These prompts can be found on page 3 of the MTFC Project Proposal Prompts 2024-25. Additional information on Project Definition can be found in ***Step 1: Project Definition*** in the Actuarial Process Guide.

Team Responses:

#1: Identify the topic

- Response: Cyberattacks are unwelcome attempts to steal or destroy data through computers. Such attacks can be intensely disruptive to systems that require near 24/7 uptime – which can include governments, hospitals, businesses, and regular consumers –

and to systems that hold sensitive data. Cyberattacks are conducted by cybercriminals who exploit vulnerabilities in computer systems for their own personal gain, and they very often come from foreign countries.

#2: Identify potential risks

- Response: Businesses can lose access to important and valuable data, which can lead to direct loss of money, disruption in ordinary business, and loss of communications. For example, a cyberattack could mean hospitals would receive a disruption in their normal affairs, even though they need to be running 24/7. This can lead to a direct loss of life, or destruction or damage to equipment. Other businesses could have credentials or passwords stolen, facilitating theft and thus a loss of money.

#3: Identify a behavior change risk mitigation strategy

- Response: Enforcing a higher awareness of security standards at these businesses/organizations will lead to a lower risk for cyberattacks. For example, these places can institute training programs that explain the risks of trusting random emails, opening potentially harmful links, and using weak passwords. Furthermore, decreasing reliance on digital systems will decrease the potential for severe loss of data or money.

#4: Identify a modifying outcomes risk mitigation strategy

- Response: Businesses can implement preventative strategies in their digital framework to lower the chances of a cybercriminal gaining access to private data or disrupting normal operations. A simple way to modify the outcome of this is to keep backups of the data so service is harder to disrupt. They can also distribute their data and systems among multiple computers so there is not just one point of failure.

#5: Identify an insurance risk mitigation strategy

- Response: Insurance companies can serve as an effective risk mitigator for organizations or individuals with a propensity for loss due to malware or cyberattacks. The insurance policy can pay out if data is stolen, based on the value of this data, or based on the money that the company would have made during a period of disruption. They can also recuperate the losses if a business cannot function properly for a long period of time. Of course, these organizations must pay a premium to ensure the insurance company is solvent. In cases where the attacker demands money, an alternative insurance policy can be one that always pays the attackers in the case of a hack. A maximum payout will most

likely be needed– however, this is likely not a good policy since it encourages attackers, and it may lead to upward pressure in the ransoms that attackers charge.

#6: Identify driving research questions for your topic

- Response: What programs and features could be implemented to lower the risk of cybercriminals gaining access to business data or operations? How is the data that a company lost related to the monetary value of this loss? What are reasonable premiums and claim rates that the insurance company can issue?

Part 2: Data Identification & Assessment *(Team's Topic)*

These prompts can be found on page 4 of the MTFC Project Proposal Prompts 2024-25. Additional information on Data Identification and Assessment can be found in ***Step 2: Data Identification & Assessment*** in the Actuarial Process Guide.

Team Responses:

#7: Identifying the type of data you hope to find

- Response: Important data for us would be finding out how frequently businesses suffer cyberattacks. Additionally, it would be vital to determine how much money companies lose with cyberattacks and the indirect effects of these losses. We also hope to find data on the effectiveness of defensive measures against cyberattacks. Lastly, we would also want to find data on which methods these cyberattacks use to exploit vulnerabilities.

#8: Identify potential data sources for your topic

- Response:
  https://cissm.umd.edu/cyber-events-database - This dataset details many cyber incidents since 2014. It contains information about each attack such as dates, actor, target organization, motive, and an event description.
  https://eurepoc.eu/ - Dataset that provides various info about recent cyberattacks, such as cyber intensity, political response, and legal responses.
  https://jamcyber.com/discover/cyber-attacks/ - This website provides general information about recent cybersecurity attacks

Part 3: Mathematical Modeling *(Team's Topic)*

These prompts can be found on page 5 of the MTFC Project Proposal Prompts 2024-25. Additional information on Mathematical Modeling can be found in ***Step 3: Mathematical Modeling*** in the Actuarial Process Guide.

Team Responses:

#9: Modeling research on your topic

- Response:

The existing research on mitigating cybercrime is mostly focused on qualitative things that people can change within their systems, however, there exist mathematical models. These usual work by using a measure of susceptibility to attack by subjecting a system to cyberattacks over time and measuring the average functionality. Some research uses game theory and machine learning, and some adapts models' ideas used to model epidemics of diseases. These ideas helped determine what different approaches can be used to create our model. A lot of the research is more focused on computer science than math, which means it discusses topics we were not aware of – there is also higher-level math, like differential equations.

Useful links:
https://www.mdpi.com/2078-2489/15/5/273
https://www.mdpi.com/2076-3417/13/11/6508
https://ieeexplore.ieee.org/abstract/document/10380585
https://arxiv.org/pdf/2302.04413

#10: Goals of a mathematical model in the project phase

- Response:

A mathematical model for cybercrime ought to be able to quantify the resilience of a system to being hacked. It should also be able to model the effects of a mitigation strategy in preventing this hacking by using historical data and guessing emerging trends. The model should detect changes in threat levels over time and predict future risks – it should also consider variables like system vulnerabilities, attack frequency, and mitigation strategies to measure this risk. Probabilistic modeling, such as Bayesian analysis or Monte Carlo simulations would help with the uncertainty of this risk while network analysis could tell us how these cyber-attacks can spread rapidly across interconnected systems.

#11: Assumption development

- Response: The model should be able to last for the next ten years, as it is currently unpredictable how servers and cybercriminals will evolve after that. Criminals may use tools that leverage machine learning for faster and more automated attacks, and the current power of these tools is unknown.

Part 4: Risk Analysis *(Team's Topic)*

These prompts can be found on page 6 of the MTFC Project Proposal Prompts 2024-25. Additional information on conducting a Risk Analysis can be found in ***Step 4: Risk Analysis*** in the Actuarial Process Guide.

Team Responses:

#12: Goals for mitigation strategy

- Response: Currently, if no mitigation strategy was developed, companies would lose important data and money to hackers, lose clients and gain lawsuits, and hurt their reputations. This risk mitigation strategy aims to prevent companies from ending up in this position and retain their money and data.

Part 5: Recommendations *(Team's Topic)*

These prompts can be found on page 7 of the MTFC Project Proposal Prompts 2024-25. Additional information on making Recommendations can be found in ***Step 5: Recommendations*** in the Actuarial Process Guide.

Team Responses:

#13: Recommendation differences between mitigation strategies

- Response: The timeframe for implementation will be one of the most important metrics to consider when pursuing mitigation strategies. Cyberattacks can lead to down time for companies, that would then result in a large loss of money and services. Cost must also be considered as the clients who would use this model will mostly be businesses who would like to maximize profit and minimize loss, which would be impeded by disruption in affairs or theft of key data. Lastly, effectiveness of the mitigation strategies must be

heavily considered, as many strategies for improving digital safety are cumbersome to enact but only lead to marginal improvements in safety.

#14: Audience for recommendations

- Response: The most important group that could consider our recommendations is the head of the security department of a company. This group will be the deciding factor in implementing our cybersecurity strategies into their security framework.

#15: Goals for situation improvement

- Response: Our recommendations would aim to improve the security of a company's services, preventing their susceptibility to harmful cybersecurity attacks. In this way, we will decrease monetary losses and the downtime that their services cannot be used. We can therefore improve the success and stability of our clients.