




Milestone 2 Report: Insider Threat Risk Modeling for BillyBank

Team 3: Akhil Harikumar, Paul Hitchcox, Shyon Ghahghahi, Vy Tran

What is planned to be delivered?

1. Synthetic dataset  billybank_activity_updated.xlsx (modeled after CERT's insider threat dataset^{1 2} and JPMC real life case studies) & code file used for generation
2. Monte Carlo simulation model and output
3. Heatmap based on employee role and geographical region and their probability of being a malicious insider & code used for creation
4. Interactive front-end for the model we made for the above items, which shows how impact and likelihood may change depending on the course(s) of action the client choose
5. Courses of action/recommendations, basing off of real security solutions' costs, and JPMC-like banks' budgets, tying back to potential monetary losses demonstrated in Monte Carlo simulation. If there turns out to be too much here to deliver well in the final presentation (item below), we plan to include the details of these options for the "client" in a supplementary report.
6. Final in-person presentation to (imaginary) client, aimed to have some interactive component
7. Internal deliverables as evidence of the team's process (would not be submitted to "client"), such as  CRM Project Timeline / Meeting Agendas

Are all actively engaged?

Yes. The team has been meeting for check-ins on a weekly cadence. The  CRM RACI Matrix outlines each member's level of involvement in each task, aligning with each of our strengths.

Are things on track?

Yes, mostly. Currently, we are putting together ranges for losses/impact to build up to the Monte Carlo simulation. Once that has been done, the interactive front-end (which we currently have a simple rough copy of in a Jupyter Notebook) can be fleshed out. That notebook also includes our rough idea of how to make the heatmap, which still needs to be finalized. We have ideas of industry solutions for the courses of action, backed by some real cases, but only after everything else is done can we finalize these. The final presentation will be built last, and hopefully we will know soon on which of the three possible dates our group is presenting. Ideally, we want to share our project with Doc Rock and our TA a bit before the deadline for preliminary feedback, but the feasibility here will be reassessed after the team syncs up later this week.

¹ <https://www.kaggle.com/datasets/nitishabharathi/cert-insider-threat>

² <https://www.sei.cmu.edu/library/insider-threat-test-dataset/>