CyberKillChain Notes

This paper describes an intelligence-driven,
threat-focused approach to study intrusions from the adversaries' perspective.

Each discrete phase of the
intrusion is mapped to courses of action for detection, mitigation and response. The phrase "kill chain"
describes the structure of the intrusion, and the corresponding model guides analysis to inform actionable
security intelligence. Through this model, defenders can develop resilient mitigations against intruders
and intelligently prioritize investments in new technology or processes.

Advanced Persistent Threat - emergent threat that is the current largest risk element.

Conventional cyber responses - anti-virus, firewalls.

Conventional fail because it assumes

- response should happen after the point of compromise
- compromise was the result of a fixable flaw

Trojan - Users have to allow it into the system. Its a payload that requires user interaction. The malicious program masks itself as a benign program, misleading users of its true intent.

- In rose, gtst, accord, can they store documents by case? and isit easy to manage?

Presentation notes - Intern case study

- The hours that we have spent working on the Network Case Study and the regulation engagement projects have convinced us that what we need in JP Morgan is not more applications that are tailor made to the needs of a single business unit. Because these development efforts do not leverage the scale that JPMC possesses. This behaviour results in duplication of effort.
- The first thing we need to do in JPMorgan is to try to leverage our scale. We as a firm need to move away from developing applications without customizability in mind.
- Also talk abit about why legacy is important.

- We created Bank.OS because we wanted to give business units more control over their business process management software. Focus on 4 key areas
    - integrate Legacy systems. (Capitalize on the strong points of legacy systems, Not alienate staff who are familiar)
    - provide an intuitive user interface.

    - provide configurability. (Makes business units more AGILE)
    - simplify communication, (effective and transparent document tracking)

- The first thing you need to know is that Bank.OS is not an operating system. Instead,
- Bank.OS is a business process management portal built as a sugar layer on top of a sharepoint site. And while it has many useful functionalities, individuals who are more comfortable with interacting directly with the sharepoint site can still choose to do so. Bank.OS comprises of three components. All targeted towards providing configurability, simplifying communications, and offering an intuitive user interface.
    - The first component I will present is Bank.OS Forms (An easily configurable drag-and-drop form builder)
        - We realized that most business process management processes boil down to collecting, sending and reviewing information. By providing a flexible and easily configurable form builder, we give business functions more control over their business process management software.
    - Next, we have Bank.OS Visio (A software that makes your visio diagrams come to life)
        - Everyone understands visio diagrams. It is an intuitive way to view and review the current state of a business process. By making visio diagrams interactive, we breathe business logic into the already familiar flowcharts.
    - Lastly, we have Bank.OS Share (A way to synchronize communications and documents across emails and SharePoint)
        - We learned that business functions often send important information or documents over email, but oftentimes forget to CC all related parties and update their sharepoint site accordingly. By synchronizing communications and documents, we organise communications on a project level and provide transparency into the communication process without overloading the mailbox.
- Now that you are familiar with the three solutions offered by Bank.OS, let me demonstrate how Bank.OS can be used to simplify your business process. In particular, I will be presenting how Bank.OS can be used to empower the network team.
- The network team has three different business roles. Project Manager, Resource Manager, and Engineer. I will begin by explaining how the Project Manager interacts with Bank.OS. (click)
- Over here, we have the Project manager's dashboard.
- Project Managers are only concerned with two interactions with the network team. Firstly, they are concerned with submitting a new work request to the network team. (Click)
    - Here, we see Bank.OS forms at work. The site admin is able to configure the fields that a project manager has to fill in in order to submit a project request.
- Secondly, project managers are concerned with tracking project timelines.
    - So here the site admin has configured a calendar on the project manager's dashboard to track the network team's availability.
    - The project manager can also access the project view to track the exact stage that each

project is at.
    - I will explain all functions related to the project view shortly when examining the Resource Manager's view
- Since network Resource Managers require fine-grained control over all aspects of the project. The site admin has configured various charts on the dashboard that display important information for the RM.
    - The resource manager is able to view the different type of network projects that the network team is currently undertaking,
    - See the forecast of engineering hours, and view other useful statistics.
    - When the resource manager wishes to view a project in detail, he simply clicks into the timeline chart to pull out the project view.
    - Now, let us first examine the project's visio diagram.
        - Over here, the project's current state is highlighted in turquoise. We can click on arrows downstream from the current state to trigger preconfigured visio events.
        - For instance, when the resource manager sends a project to the build team, he would want to notify the build team through an email.
        - When triggering a business critical state transition, the state transition may require a confirmation dialog.
        - Some state transitions require information gathering and Bank.OS form allows us to configure forms that can be used as part of the information gathering process.
    - The Project Q&A button allows us to contact parties involved in the project for information without flooding mailboxes. We are also able to view all previously submitted Q&As within the scope of the project.
    - The Project Email button allows us to view all email communications sent through the Bank.OS portal. All communications and documents sent over the emails will be synchronized with the sharepoint site as well.
    - The project Forms button allows us to view all forms filled from triggering the project's visio diagrams.
    - The project Documents button allows us to view all documents uploaded onto the project and also provide a way for us to upload new documents onto the project.
- Now that we have completed explaining all of the functions the resource managers have access to, let us round up by reviewing the Network Engineer's view.
- Network engineers are mainly concerned with completing their BAU, and their view has been configured to allow them access to the tools and information that they need in order to complete their BAU.
    - Over in the notifications centre, the network Engineer is notified of all the tasks that he has at hand.
    - Similar to the PM and RM, the network Engineer is also able to access the project level view. However, since the task at hand is not currently in his swimlane, he is not able to

trigger any downstream events.
    - This rounds up the Bank.OS demo, Daniel will now conclude our presentation.

- Engineer wants to able to complete their BAU easily. Provide the minimum set of tools required for them to complete their BAU.
    - Engineer
        - Answer Q&A
            - Configurations will be complete by Wednesday, July 19.
        - Show Answer recorded in Engineer Q&A
        - Go to flow but cant trigger because not admin

- While our original intention was to develop seperate solutions for each case study, we realized that the pain points uncovered in both cases converge from a technology viewpoint.
- Hence, we have decided to develop a tool to provide 4 core functionalities. (we briefly mentioned b4 now we go in depth)
    - Legacy system compatibility. (Capitalize on the strong points of legacy systems, Not alienate staff who are familiar)
    - An intuitive user interface.
    - A BPMS that is simple and intuitive to configure. (Makes business units more AGILE)
    - A Centralize document and communications manager, (effective and transparent document tracking)
- Today, we introduce Glide, a new way to manage business processes. Glide seeks to achieve four main objectives.
    - Legacy system compatibility. (Capitalize on the strong points of legacy systems, Not alienate staff who are familiar)
    - An intuitive user interface.
    - A BPMS that is simple and intuitive to configure. (Makes business units more AGILE)
    - A Centralize document and communications manager, (effective and transparent document tracking)
- Glide is a toolkit comprising of three components.
    - Glide Forms (An easily configurable drag-and-drop form builder)
    - Glide Flow (A software that makes your visio diagrams come to life)
    - Glide Share (A way to manage/synchronize your communications/documents across emails and SharePoint)
-
- High level
    - Reiterate both case studies (purpose, and blockers)
        - Show the problems that technology can solve
    - Want a way to manage communications and documents effectively. (transparently)

    - Want a user interface that is intuitive and easy to use
    - Want a configurable portal to manage different types of projects/engagement
    - Want a legacy compatible system
    - There are already tools available to solve these issues.
    - Highlight that both are business process management issues and that there are already tools available to solve these issues. Like PEGA 7
    - But no one uses these tools cuz it is difficult to use. And configuring these things are far from our mental map.
- (Centralized document storage, communications manager, business process visualization system)
    - Today we introduce (glide, sail, flow which??) a new way to manage business processes. That is intuitive, configurable, easy-to-use.

```
- Glide consists of three different components. (Roles, forms, flows)
  - Glide Forms, Glide Flows, and Glide Share.
- Task view (Engineer view, PM view also)
  - View tasks you have to complete from all your different projects (Engineer)
  - Trigger requests, tasks for other ppl.
- Dashboard view (All view)
  - Charts to track all ongoing projects
  - For Engineers and PM, less charts
- Project view (All view)
  - View all communications (emails)
  - Submit QnA to different business roles (track)
  - View all documents (store attachments from email as well) (only ppl involved in email can see)
  - View flow
```

    - Walk them through setting up a projects (might put in)
        - Trigger one form
        - Set up visio diagram
    - Walk them through working on a project
        - display form fill (pm request) - PM Dashboard View
            - PM submits form to trigger a new work request (PM form1)
        - display flow chart (rm sees new request) - RM task to dashboard to flow view
            - RM goes into his task view and approves new work request to trigger new project (Also pm form 1)

        - RM goes into dashboard and clicks on the newest item on the gantt chart to trigger flow view (last item on gantt chart)
        - RM clicks around the flow view. Nothing happens.
    - display email (rm send it down to next stage) - RM flow view feature
        - RM clicks on active state. Triggers email dialog.
    - display triggering task (fill up the engineer task board) - RM flow view feature
        - 2 or 3 clicks down (eventless states), RM triggers to next swimlane. (engineer)
    - display task list - Engineer task view
        - Engineer checks out task view, clicks on task to fill form. (Acknowledge and sign off form)
        - But enginner requires clarification.
    - display q&a (engineer ask question to pm)
        - Engineer goes into project(flow) view to trigger Q&A to PM
    - display answer q&a (PM task view)
        - PM goes into portal to fill form to answer Q&A
    - display task view - Engineer task view
        - Engineer reads Q&A reply
        - Engineer completes task.
    - display comms tracking (Pull out all emails) - PM Project level comms view
        - PM Pulls out all the comms in project - in one click.
            - Can see email thread and all Q&A
    - display document management (pull out all document) -PM Project level doc view
        - PM pulls out all docs.
-
- Conclude both cases, high level.
    - The reg eng study - Figure out a way to provide consistent engagements with regulators globally. figure out where the global process diverge, try to streamline global process.
        - Blockers: Globally not using the same tool
            - UI/UX problem.
        - Difficult to gather/retrieve information, responses, and documents using email
            - Manual labour intensives
        - Exam manager want oversight.
    - The Network portal study - Find a way to better track and manage network projects.
        - Projects lack structured ways of tracking
        - Projects

- In both cases, there is a business process to manage. There is also a tool available, however, both teams do not like the tool that they are using.
    - Reg eng, too many different tools… (No visibility)
-