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

- 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)
-