James Chad Ballay

Week 1 Module 1 Written Assignment

*Provide at least three examples of how people act as vulnerabilities, defenses, or threats to an information system.*

I’ll be using the Equifax breach of 2017 for this assignment. (<https://www.gao.gov/assets/700/694158.pdf>)[[1]](#footnote-19997)

**Vulnerabilities**

*Equifax IT administrators circulate this advisory on an internal mailing list. Unbeknownst to its IT administrators, the mailing list was out-of-date and did not include all its systems administrators, indirectly leading to an incomplete patch of Equifax's servers. [[2]](#footnote-31185)*

Short term thinking lead to long term culture problems. A manually created or maintained email distribution list for communicating with system stakeholders about must take action items is a weakness of process due to people. Making some assumptions but you can see a chain of small right decisions being made that led to this. Creating an email distribution list one time vs identifying all servers and their owners and then creating a mechanism to auto communicate to them. Making the task coming across this channel as a note of warning instead of tracked and assigned work items in a project tracking software. Finally, showing trust in your coworkers to heed the note at their chosen time versus a top down deadline given on patching. In a perfect world much of the human element would be removed.

**Defenses**

*Equifax officials stated that, on July 29, 2017— approximately 2.5 months after the attackers began extracting sensitive information on May 13, 2017—security personnel conducting routine checks of the operating status and configuration of IT systems detected the intrusion on the online dispute portal.[[3]](#footnote-20522)*

Routine checks of systems that should be secure within the internal topology are some of the least glamourous roles. Red Team penetration testing, Blue Team external defense, etc... Those have the focus and glory due to the variance of problems faced and immediate feedback. The routine scanning of systems that are usually still safe requires you to focus on process and automation. Automation so that very infrequent anomalies don’t get missed. Process since every system has to be treated as compromised until proven otherwise and they often do prove themselves secure.

**Threats**

*As a result of Equifax storing usernames and passwords unencrypted on the network, the attackers were easily able to extend their attack beyond the three databases supporting the dispute resolution portal to 48 other unrelated databases.[[4]](#footnote-31784)*

There never is a reason to collect and store usernames and unencrypted passwords in an accessible location unless it is for convenience. The systems we secure need to be useful and available but often times the threats from within are worse than the threats from without. External threat actors have clearly defined goals and reasons. Blocking them is the end goal and improves the system. The ambiguity is removed due the lack of middle ground. Internal threats become much more hazy. Often we patch over hard to implement technical solutions with simple memos and procedures that we trust employees to diligently follow. No major IT organization is ok with credentials being left around but if this policy is only enforced internally by trust then people will ignore and circumvent it.

1. GAO-18-559 “DATA PROTECTION Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach” August 2018 [↑](#footnote-ref-19997)
2. <https://www.zdnet.com/article/us-government-releases-post-mortem-report-on-equifax-hack/> [↑](#footnote-ref-31185)
3. <https://www.bankinfosecurity.com/postmortem-behind-equifax-breach-multiple-failures-a-11480> [↑](#footnote-ref-20522)
4. <https://www.theinquirer.net/inquirer/news/3062853/equifax-hack-report-sheds-light-on-firms-dysfunctional-it-department> [↑](#footnote-ref-31784)