James Otis

IS428 Koulopoulos

Readings for Feb 27th

**Cybersecurity’s Human Factor: Lessons from the Pentagon**

* Unifying Cyber Command put what was an infrastructure of 100,000 admins into a smaller body that is able to detect threats faster
* Unifying Protocols and Data Analytics have allowed for quick detection of threats.
* Instant Reconfig/Central monitoring/easy updating/standardized defenses
* Benefits outweigh the risks of having all of the information in a centralized location.
* Security Structure:
  + Integrity: Making sure that mistakes that are made are brought forth and that none are made on purpose
  + Depth of knowledge: Have people become totally proficient in their tasks and make sure that they know how everything works so that they are more likely to spot vulnerabilities
  + Procedural Compliance: Ensure that every worker knows the proper procedures and follows them. Enforced by random checks.
  + Forceful Backups: No one is alone in their tasks, and often surrounded by more senior experienced personnel.
  + Question Attitude: have members always double check their work, and go over results and question why the results turned out the way they did if they deviated from the norm.
  + Formality in communication: Make sure that directions are clear, and have them reiterated back to make sure that they were conveyed properly.
* \*Crown Jewels of a company are often not what most companies think that they are.
* Can’t just protect the crown jewels, as hackers often start at low levels and then work their way around.

**The Flaws in Obama’s Cybersecurity Initiative:**

* Goals:
  + Eliminate the sale of Bot Nets and Security Vulnerabilities
  + Give the courts authorization to prosecute/shut down networks involved in DDOS attacks
  + Protect companies that choose to share their information with the government about security vulnerabilities and attacks.
* Problems:
  + Over the past few years the cybercriminals within the US has decreased by 10%, whilst the newer threats have been coming from other nations such as Russia and Brazil. Essentially not doing anything for America today.
  + Really nothing new in this article.
* Solution:
  + Essentially Interpol (A global organization with the funds and the authority to fight cybercrime)

**The Vulnerability Economy: Zero-Days**

**Cybersecurity and Public Policy Epilogue:**

* We already read this article. The dude that set out to find zero-day vulnerabilities in the Siemens systems.

**Your Company Needs a Communication Plan for Data Breaches:**

* The first thing that every company should do is to prepare an impact test
* Second is to create a communication team of a group of individuals able to communicate live.
* Turn to outside resources and maintain good connections with Security Experts and Media Officials to make sure that when a breach does occur, these people can be allies rather than enemies. (Assets)
* Continue to function with normal efficiency so as to not take a further hit to your industry.