James Otis

IS428 Reading notes

Cybersecurity Does not try to prevent Every Attack:

* Risk is often associated with more or less the individual who have personal access to data outside of the company or the realm of work.
* In this day in age it is almost inevitable that there will be some sort of a breach. In this case it is important to be fiscally responsible and have a plan for when such intrusions occur.
* Employee education and regular trains are more likely to reduce the risk of cybersecurity issues and allow a level of reassurance for the clients.

Security Breach at TJX:

* Downplayed the breach (46 million was 94 million in reality).
* Multiple points of entry (USB-Drives / Wireless Attacks / Compliance and encryption attacks)
* WEP encryption (Can be broken in under a minute on an average computer) Which is a 40 bit key and a 24 bit IV initialization Vector (Stream Cipher) and only ASCII characters. So the greatest amount of keys you can have would be which means that the amount of limited characters for a 152bit key (for enterprise) is 16 ASCII characters or 128^16 broken on a microprocessor in under 50-60 seconds.
* Exhibit 2: PCI/DSS standards
* Note of talking: They seem vague and some of them don’t seem like wise practices to begin with. You should never send secure information over public channels.

Sony Playstation, a security Breach:

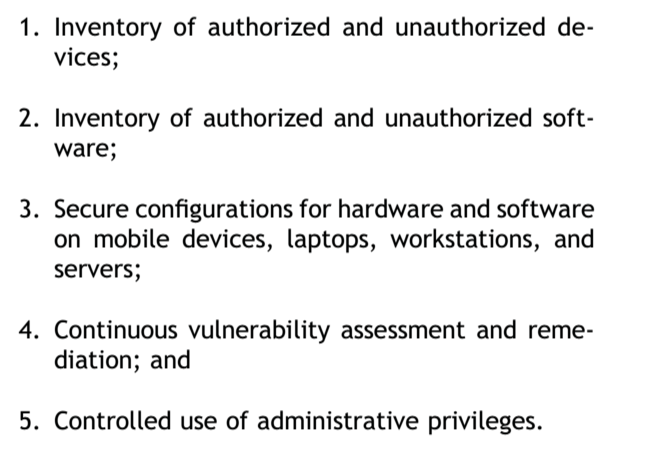
* Nothing new

Why Cybersecurity is so hard to get Right?:

* Stealing data is often used not directly, it can be used to leverage a more sophisticated attack.
* Best Practices for preventing attacks:
  + Encryption of important data, and further encryption of data that is more important
  + Employee Trainings (Fake Phishing Emails as in the article)
  + Good analytics to know what was stolen and how and be able to identify a breach quickly.
  + Have a response team that is able to react quickly.

The Case of the emerging role of CISO:

* The CISO would be a position right next to the VIO.
* The CISO requirements at this day in age are pretty inclusive. Most businesses want both 5+ years in IT and Risk often with a MBA.
* Positions require familiarity with multiple languages as well as tools for network and software scanning and monitoring.
* The job of the CISO is mainly to always have an idea of the amount of metrics of malicious devices and software



Manage Operating System and Hardware/Software versions to make sure that everything is properly up to date as “Patch” applications always present a risk.

The Vulnerability Economy: Zero-Days, Cybersecurity, and Public Policy:

* Stuxnet used what were coin 0-Day vulnerabilities in windows software that monitored and controlled the Logic Gates that operated the Nuclear Centrifuges. By doing this Stuxnet was able to break the centrifuges (Causing physical damage).