IS428 Notes:

Koloupolos

Minimize the likelihood of Lawsuit and cost:

-No 100% solution ever.

-Human element is the greatest risk to devices and to cybersecurity

-Cybercrime: 500Billion Approx industry

-Change in Management can cause for lack of knowledge base.

-Version Control Management:

-**Scenario Based Planning**

-Inconceivable situations for worse case management

-Allows for easy management of minute issues.

-Good Culture is aware and prepared.

Guest Speaker:

* Authentication:
  + “Process of proving or showing that something is real”
  + Verifying the identity of the user or process
  + Biometric/Password/Token
  + IP address / Location
  + Two Factor Authentication
* Authorization:
  + Principle of least Privilege or Need to Know\* “Above my Paygrade”
  + Authorization levels/grades/classes should be universal
* RansomWare:
  + Encrypt data and make you pay to decrypt it.
* Usability vs Security:
  + Generally the more usable the lower the security
* Cost
  + No Return on Investment for Security
  + Target lost 291million lost in 2016 as a result of attack
  + “Just good enough” not that great
* Downsides:
  + Biometrics when they are obtained are unchangeable
  + Computer administrators have access to everything (One person is easier to break than two or more).
* Value of Protection:
  + Not worth it to protect small amount of money
  + Protect from the inside out: Maintain greater security and access to more important resources.

All companies are vulnerable (Internet or not)

Turing Test: If a machine can pose as a human it passes the turing test.

\*\*\*Things that we have learned to trust, are no longer trustworthy\*\*\*

-With every piece of tech there is a consequence: We just need to measure the gains versus the losses.

-APT advanced persistent threat: Nation State Threats, little tiny threats that infiltrate constantly.

-CCTV closed circuit television. 1 camera for every 14-35 people in the UK.

-Deterrent, not a preventative measure.

-FBI/CIA/NSA:

-In essence: National Police Force and manner of defense.

-CIA: Outside the Nation, not within the nation

-NSA: Unclear role: Super Secretive without jurisdiction.

-DDOS: Distributed Denial of Service Attack:

-Growing to a size that is exponential.

-IoT to distribute attacks and embed software.

-PII: Personal Identifiable Information

-PKI/CA : Public Key Infrastructure. Private and public keys.

-SCADA: System Control and Data Acquisition

-Control the flood gates of a sewage plants, succeeded and flooded sewage….. RIP.

-SSL/VPN: Secure Socket Layer / Virtual Private Network

-Harry Stimson – Edward Snowden:

- Secretary of State 1920s: “Gentlemen don’t read other gentlemen’s mail”

-

Class February 6th:

* When presenting:
  + Vocabulary and language to explain the issue and define
  + Conveying of Concepts and Frameworks
  + Explain Tactics and Mechanics to craft a solution and/or develop a strategy.
* A **zero-day** (also known as **zero-hour** or **0-day** or **day zero**) vulnerability is an undisclosed [computer-software](https://en.wikipedia.org/wiki/Computer_software) [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)) that hackers can [exploit](https://en.wikipedia.org/wiki/Exploit_(computer_security)) to adversely affect computer programs, data, additional computers or a network.[[1]](https://en.wikipedia.org/wiki/Zero-day_(computing)#cite_note-1) It is known as a "zero-day" because it is not publicly reported or announced before becoming active, leaving the software's author with zero days in which to create [patches](https://en.wikipedia.org/wiki/Patch_(computing)) or advise [workarounds](https://en.wikipedia.org/wiki/Workaround) to mitigate its actions
* Half of threats are internal threats:
  + Often inadvertent: yet still a substantial issue.
  + Quis custodies ipsos custodies?
  + Degree to which monetary composition motivates. (Money motivates less than 2%)
* The more that you secure things the tougher it is to innovate
  + American Made Supply: Locality allows for quicker innovation if there is no outsourcing.
  + Lower cost for innovation as it is easier to trial products
* CISO and CSO should be aligned with the business model.
* Dark Territory: Some generals didn’t understand the benefits of cyberwarfare, would have been must more precise and effective.
* Accept responsibility! \*\*\*
  + Must accept the loss and do the best to survive it
* Demon dialing: Call someone on a landline and find a modem signal.