



Cyber Security Putting a human face on a technical threat

The Origins of Hacking – Counting Coup

- Points for how many systems you got into
- You needed to copy something to prove you were there
- Don't leave a trace



1998 – Law & Order Episode

- Hospital system hacked
- Penetration was unknown for an extended period of time
- Hacker changed patient prescriptions
- Diabetic patients went into insulin shock, many died
- Discovered accidentally by nurse looking at a display when the prescription changed



Hacking – The Big Bang

Blatant Attack

- Crash a computer
- Denial of Service
- Crash the network
- Plant upset – Brown's Ferry engineer incident

Result

- Inconvenience a bunch of overworked plant workers
- Maybe some lost generation dollars
- Bad PR



Counting Coup

- Make subtle changes to R*TIME ini files over a period of time resulting in a large cumulative effect
- Data injection directly into the R*TIME database using one of the database utilities

Result

- Extended overpower condition
- Potential fuel damage
- Potential equipment damage
- Possible Regulatory Action
- Significant PR issues



Suggestions

- Don't just plan for the full frontal assault
- Know the usual operating characteristics of your systems
- Baseline your systems, and verify the baseline periodically
- Design file permissions on the critical disk folders
- Set up passwords wisely, even if it is inconvenient
- Insider threats can be very real