Cyber Security

...AND OTHER REAL-WORLD THREATS
Threat Management

- Prevention
- Detection
- Reaction
Threat Landscape

- Physical Threats
- Cyber Threats
Physical Threats

- Electricity
- Water
- Fire
- Environmental
- People
Physical Threats - Electricity

- Electricity
  - Surges
  - Brownouts
  - Loss of Power
  - Extended Loss of Power
  - Surge Suppression
  - UPS (Uninterruptable Power Supply)
  - Generator
  - Redundant Power Sources
Physical Threats - Water

- Water
  - Flooding / Flash Flooding
  - Fire Suppression (Sprinklers)
  - CRAC (Water Chiller)
Physical Threats - Fire

- Fire
  - Fire Detection
  - Fire Suppression
    - Pre-action Sprinklers (dry pipes and water)
    - Clean Agent
      - FM-200 (ANSUL)
      - Novec 1230 (3M)
  - Fire Recovery
Physical Threats - Environmental

- Lightning
- Flooding
- Tornado / Straight Line Winds
- Earthquake
Physical Threats - Environmental

- Lightning
- Flooding
- Tornado / Straight Line Winds
- Earthquake
Physical Threats - People

- Theft
- Vandalism
- Errors
  - Accidental
  - Intentional
- Weaponized Information Requests
Cyber Threats
Cyber Threats – Penetration (Outside In)

- Firewall
  - Layered Defense
  - Inbound Ports
  - Utilize a DMZ
  - Deep Packet Inspection
  - GAV (Gateway Anti-Virus)
  - Geolocation
Cyber Threats – Malware (Inside)

- Virus
- Trojan
- Bot (CNC)
  - DOS
  - DDOS
  - Probing
  - Penetration
Cyber Threats – Crypto / Ransomware

- Encrypts Your Data
- Rampant
- Used to Hide Other Attacks
Cyber Threats – CPU Theft

- Computationally Intense Applications
- Cryptojacking
- Gaming
Cyber Threats – Data Theft

• Identify Theft
• Confidential Information
• Reportable Data Breaches
Cyber Threats – Attack Profiles

- Phishing
- USB Drop
- Tailgating
- Open Firewall Ports (RDP)
- ADFS
Good (Simple) Security Tips

• Improve Password Security
  • Create a strong password
  • Consider using a password manager
  • Use two-factor / multi-factor authentication (where available)
  • Use security questions properly
  • Create unique accounts for each user per device

• Choose Secure Networks

• Keep All Personal Electronic Device Software Current

• Be Suspicious of Unexpected Emails
Security Assessment – Get a second opinion

- FISASCORE Assessment
Summary

BAD NEWS

• This is really, really important.
• It can be costly – doing nothing is worse.
• You’re not alone.
• Assume that you’re already infected.

GOOD NEWS

• You’re not alone.
• You can improve.
• Training works.
Cyber Crime in Minnesota Government

• Minnesota Judicial Branch, Hennepin County (Hack)
• Minnesota Department of Human Services (Phishing, Data Breach)
• City of Albert Lea, Freeborn County (Phishing, Data Breach)
• Hennepin County Government Employees (Phishing, Data Breach)
• Becker County (Ransomware)
• Sterns County (Hack)
• Crow Wing County (Ransomware)
• City of Wadena (Ransomware)
• City of Prior Lake (Hack)