INSIDER THREAT MITIGATION

Cyber Insider Training for Radiological Sources

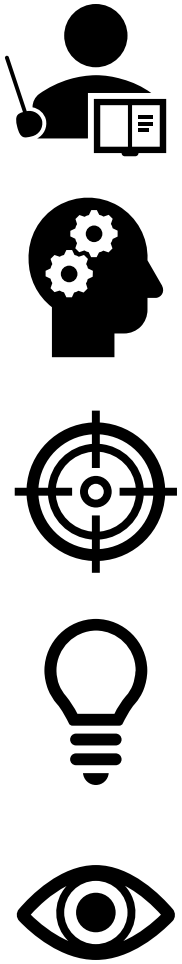
Greg White

Lawrence Livermore National Laboratory

for U.S. NNSA Office of Radiological Security

LLNL-PRES-831032

Topics



- Quick Cyber Insider Information
- Anshar and Gula Regional Hospital Overview
- Scenario Steps and Polls / Discussion
- Post-Incident Discussion

INSIDER THREAT MITIGATION

Background - Cyber Insiders

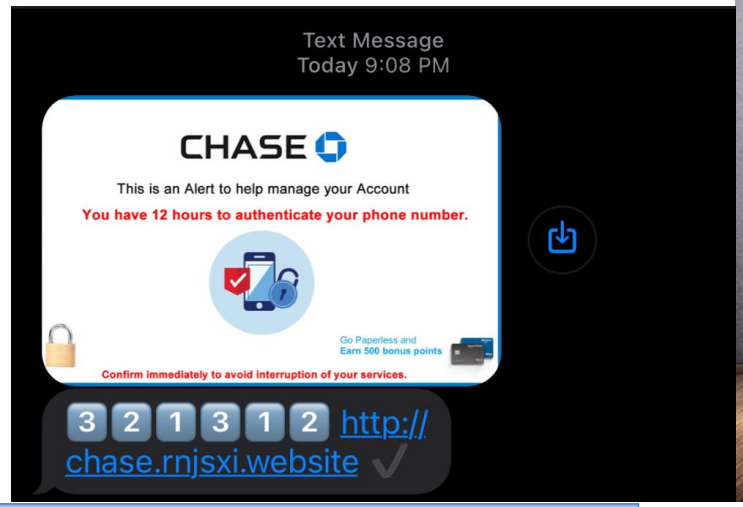
INSIDER THREAT MITIGATION

Like all other insiders, cyber insiders have similar characteristics

- They have varying **motivation(s)** to carry out their attack
  - Ideology, Coercion, Financial, Revenge
- They are utilizing their **knowledge**, **access**, and **authority** to compromise systems
- Their **end goals** also vary

The Unwitting Insider

- Opening a malicious email attachment
- Plugging-in an unknown thumb drive
- Visiting a malicious website
- Following instructions of a social engineer



We have all been the unwitting insider,
but it probably didn't result in a successful attack

Country of Anshar Overview

State Organizations

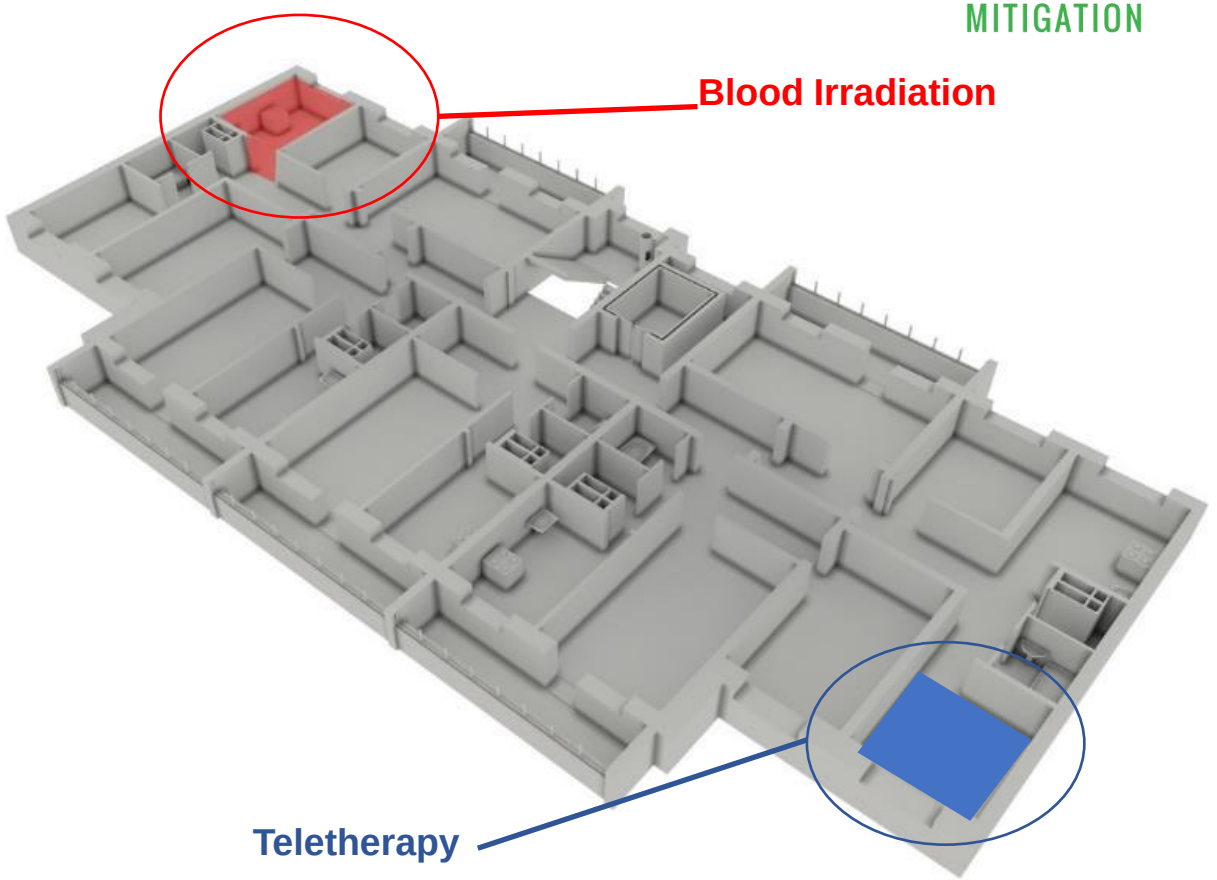
- Anshar Atomic Energy Agency
- Anshar Computer Emergency Response Team (CERT)
- Anshar Republic Federal Police
- State Intelligence Services

Licensees

- Gula Regional Hospital
- Asherah Nuclear Power Plant
- Shapash Nuclear Research Institute

Gula Hospital Physical Security

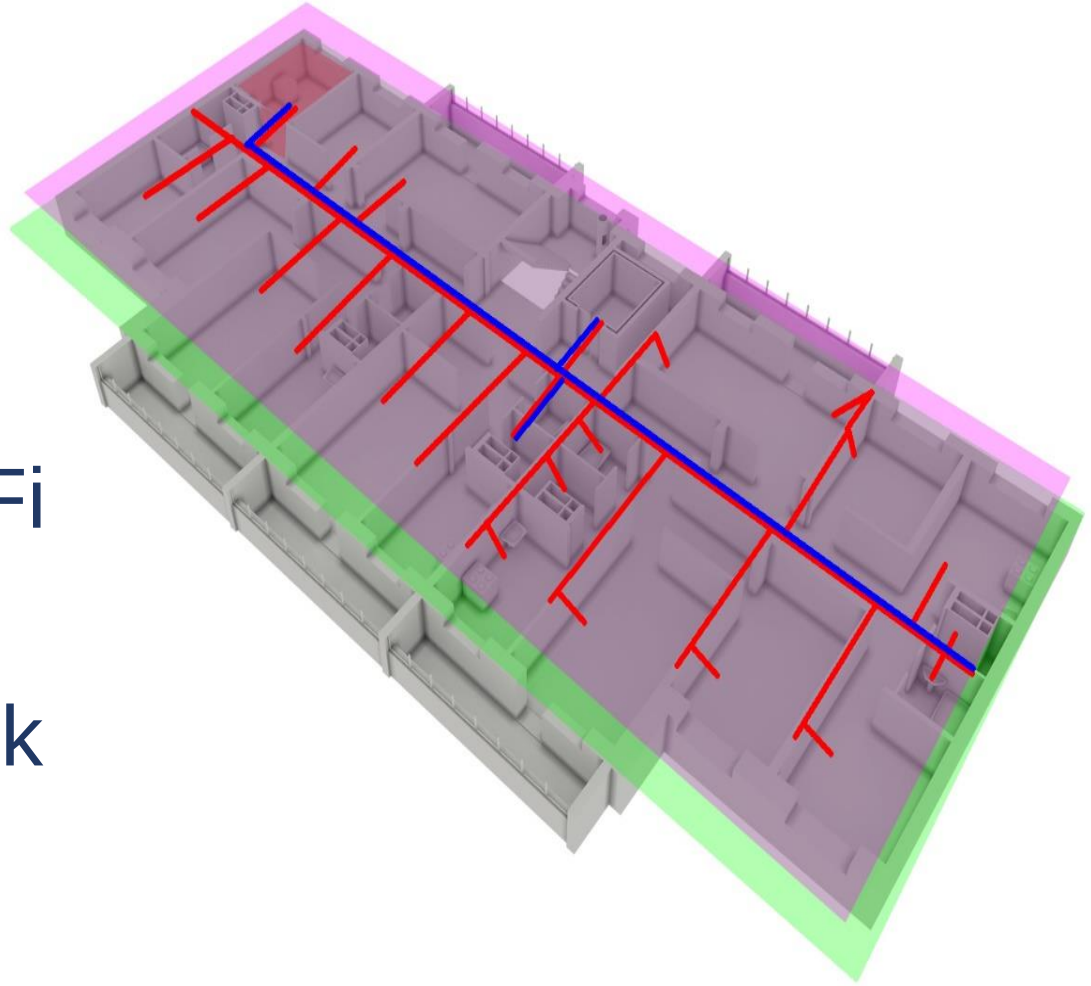
- One law enforcement officer on premises 24/7
- One unarmed security contractors is on premises 24/7 to assist law enforcement
- The blood irradiator and the teletherapy unit are in the basement
- Access to basement is unrestricted, but access to blood irradiator and teletherapy rooms is controlled



Hospital Basement

Gula Hospital Networks

INSIDER THREAT MITIGATION

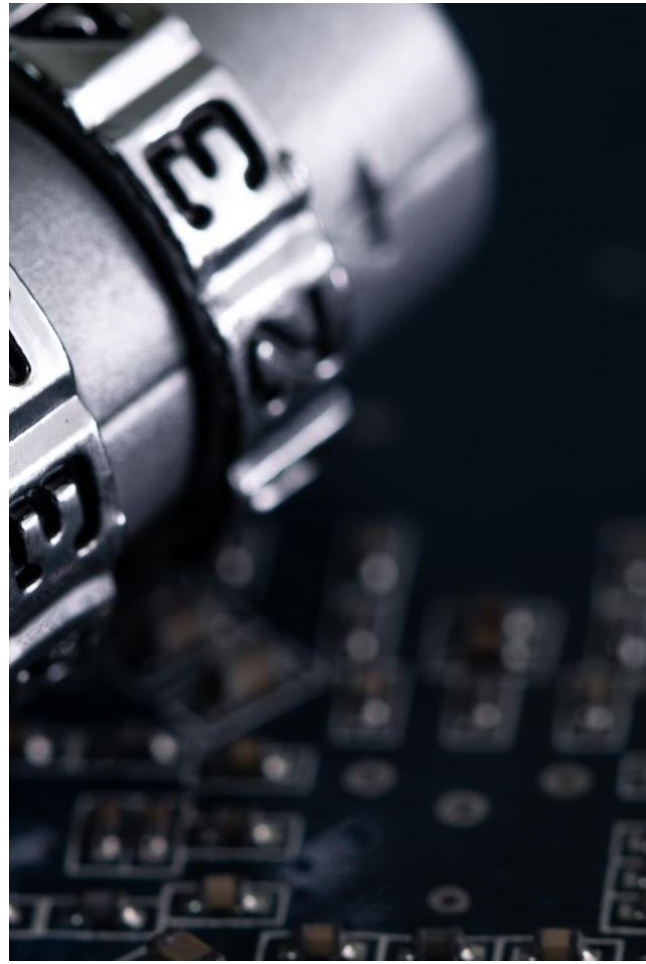


- **Green** – Complimentary Guest Wi-Fi
- **Purple** – Hospital staff Wi-Fi
- **Red** – Fire and Safety wired network
- **Blue** – Physical Protection System (PPS) wired network

Gula Hospital Cybersecurity Program

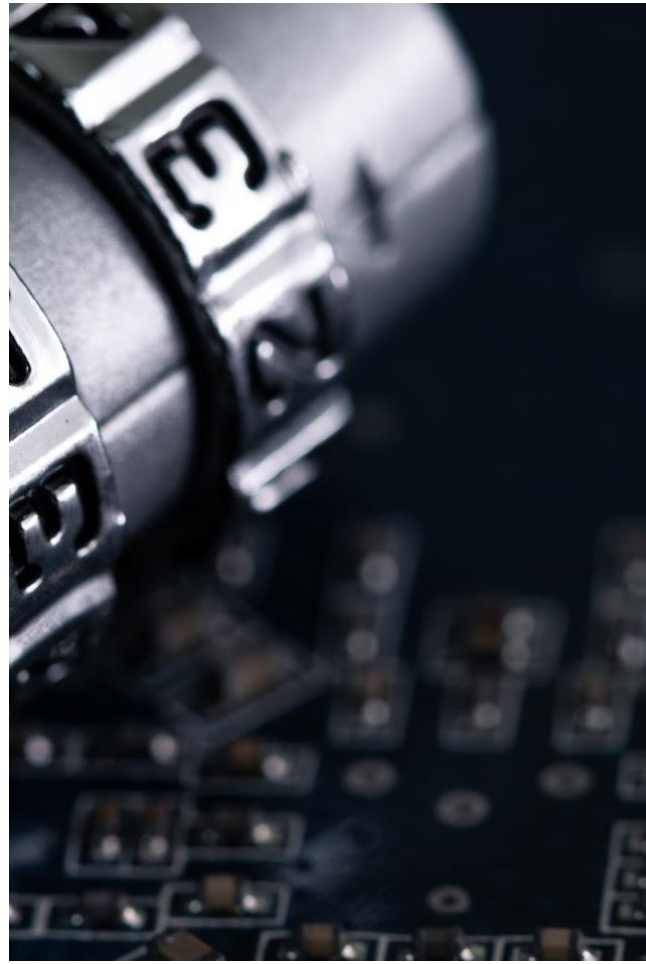
INSIDER THREAT MITIGATION

- Gula has implemented a basic cybersecurity program
- Head of Security is the person responsible for the cybersecurity program
- Computer inventory and risk assessment documents have not been updated
- The hospital does not have cybersecurity incident response team or any response or recovery procedures
- All hospital staff must undergo cybersecurity awareness training.



Gula Hospital Computer Support

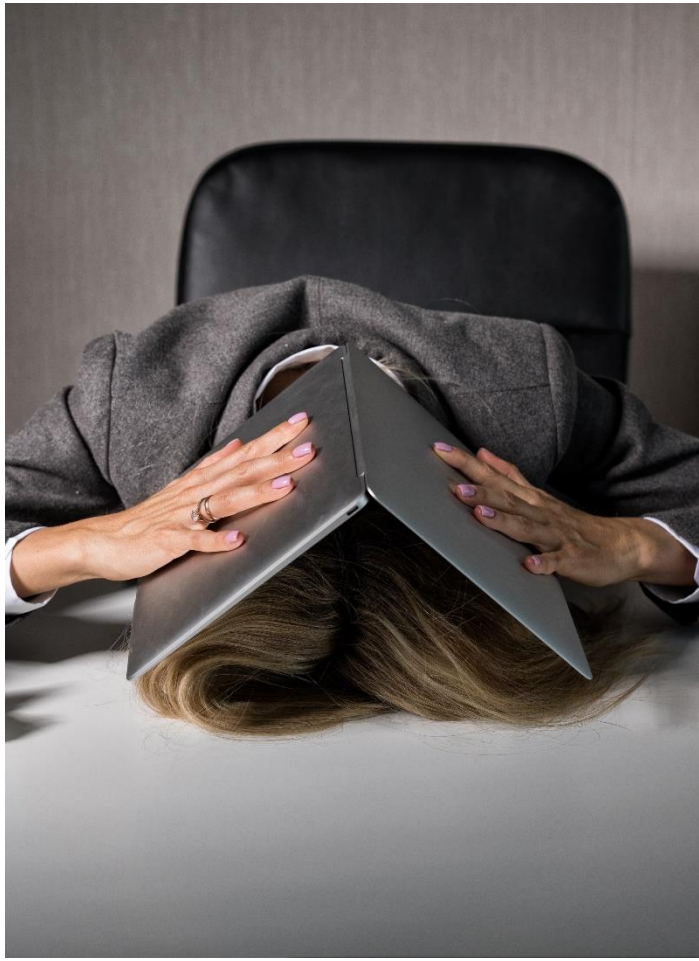
- Basic Tasks are performed by Gula staff
  - Cybersecurity hygiene and administration tasks
- Intermediate Tasks are performed by on-site contractors
  - Troubleshooting, Repairs, Backup, Log monitoring
- Advanced Tasks are performed by external contractors
  - Forensics



9am Monday

INSIDER THREAT MITIGATION

- A cloud provider in Anshar notifies the head of security of a cyber-attack campaign targeting key organizations in Anshar
  - Encrypted data was sent to one of their machines from an IP address registered to the Gula Hospital
- Cloud provider sends an email detailing the:
  - Suspect IP address
  - IP address of the hospital system on the Guest network Dates and times of transmissions for past 30 days
  - Size of transmissions are 5KB – 10MB each, about 100MB total



10am Monday

- The Head of Security has determined that immediate response is necessary
- An incident response team and recovery plan must be developed to fill the existing gap

Who should be on this team?

11am Monday

- The incident response team of internal staff is assembled
- The Head of Security leads the first meeting to set up roles and responsibilities for the team members
- The Cloud Provider did not provide:
  - What type of information was exfiltrated
  - The specific assets that were compromised
    - Only externally exposed IPs from Gula's network were provided
  - The target of the adversary or the intent of the campaign
- Hospital records needed to perform key incident response tasks are:
  - Missing
  - Need to be acquired
  - Incomplete
  - Lack sufficient detail

9am Tuesday

INSIDER THREAT MITIGATION

- The incident response team assembles for a second meeting
- Information sources that are available, acquirable, and valuable are:
  - List of network drawings; including defensive architecture specification
  - Risk registry/scenarios associated with consequences
  - List of most valuable assets
  - Network logs (30 days)
  - IT system logs (variable periods)
  - Physical Protection System host logs (90 days)

Which source should be prioritized?

9am Thursday

- The Network Logs have been analyzed and the findings are discussed
- The Network Analysis Report indicates:
  - Unencrypted web traffic includes transfer of sensitive PPS information and passwords via guest wireless network

But there is an air gap between PPS and guest networks (i.e., no authorized wired or wireless connection exists)

1pm Thursday

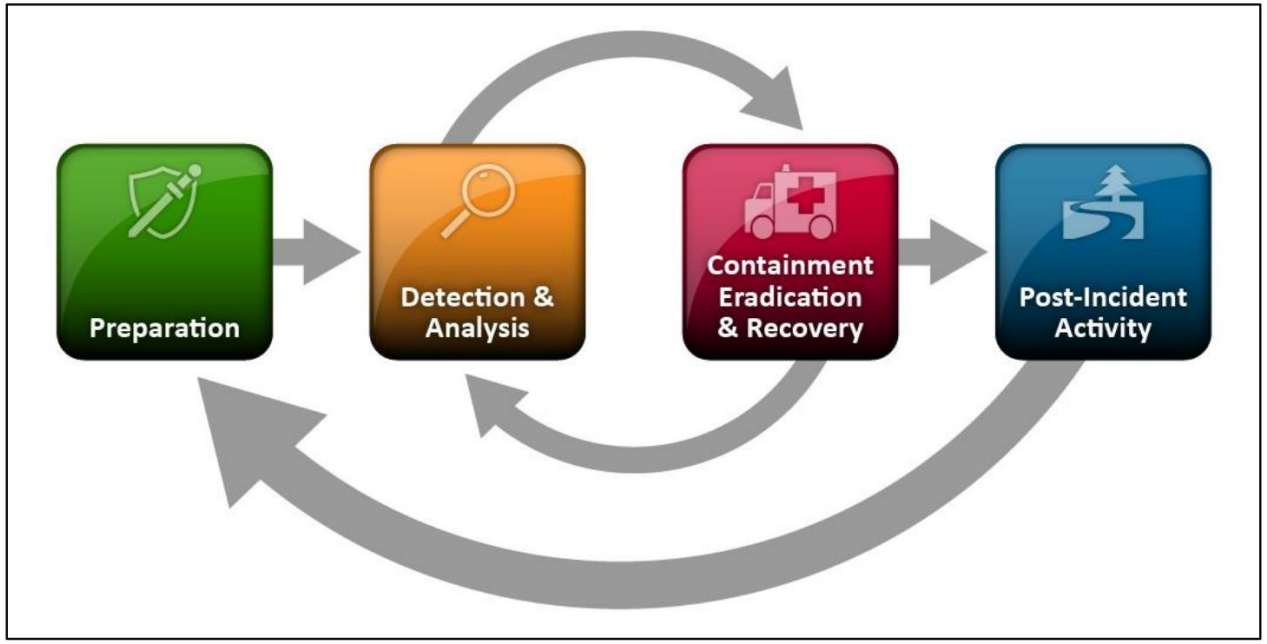
- An unauthorized device found connected to PPS wired network in a locked panel within the Central Alarm Station
  - Access to area is restricted to only authorized staff and contractors
- Urgent incident response meeting is held

Discussion Next Steps

What should then be prioritized?

a) Investigate to determine who placed the device in the Central Alarm Station panel.

b) Contain, eradicate, and recover the Physical Protection System



Poll / Discussion

INSIDER THREAT MITIGATION

What order would you do the following steps? (First to Last)

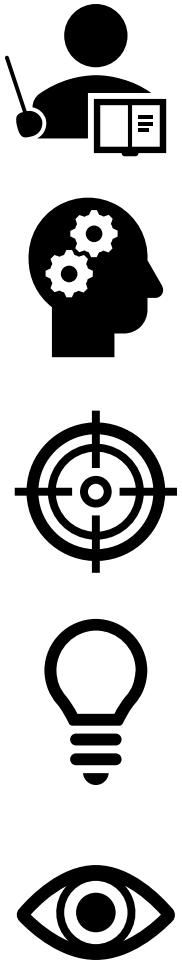
1. Quarantine the network/devices
2. Deploy Guards
3. Alert Anshar Regulator/Police Force/NCSC/Vendor
4. Change Passwords and other configurable security parameters/attributes
5. Take Forensic Images
6. Apply compensatory countermeasures
7. Replace devices with available Spares and Repair / Re-image equipment where no spares are available
8. Power down Raspberry Pi and remove the SD card
9. Place system back into service

There are no wrong answers, but this was mine

INSIDER THREAT MITIGATION

1. Power down Rasp Pi and remove the SD card
2. Deploy Guards
3. Alert Anshar Regulator/Police Force/NCSC/Vendor
4. Quarantine the network/devices
5. Take Forensic Images
6. Replace devices with available Spares and Repair/Re-image equipment where no spares are available
7. Change Passwords and other configurable security parameters/attributes
8. Apply compensatory countermeasures
9. Place system back into service

From the Attacker's Perspective



- How did the incident play out from the attacker's perspective
- What were their next steps

Background

- Bob is an unarmed security guard at Gula Hospital
- Bob has a large amount of personal debt

- John is a member of a terrorist group Anshar Dawn, who operates against the government.
- He knows about Bob's job at Gula Hospital and his debts.

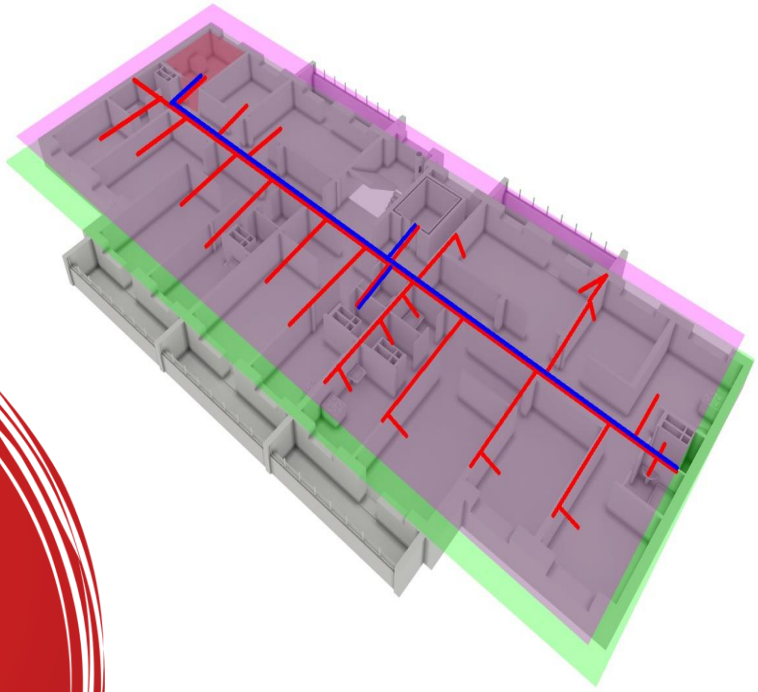
Discussion

What is the most likely motivation for this insider? (select one)

1. Ideological – fanatical conviction
2. Financial – wants/needs money
3. Revenge – disgruntled employee or customer
4. Ego – “look what I am smart enough to do”
5. Coercion – family or self threatened
6. Psychological– based on predisposition or stress

Information Gathering

- John gathers information about the Gula Hospital and finds they have
  - a guest network
  - wired and wireless network for staff
  - an isolated network for the physical protection system



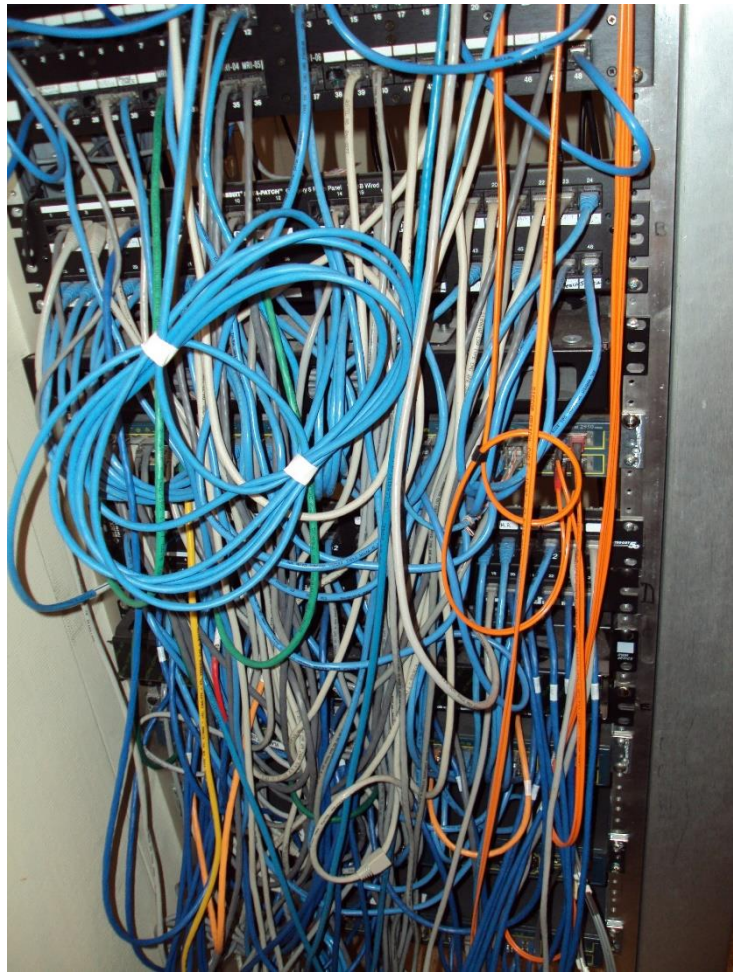
Negotiations

John offers Bob money to help with his debts in exchange for Bob putting a credit card size computer in a physical security equipment closet

Bridging Gula Hospital's Networks

INSIDER THREAT MITIGATION

- Bob uses his security keys to open the equipment closet and install the credit card size computer and hook it up to the physical security network and power
- John has pre-configured it to bridge the Guest and Physical Protection System network, and provide clandestine command and control connections from anywhere on internet



Network Access

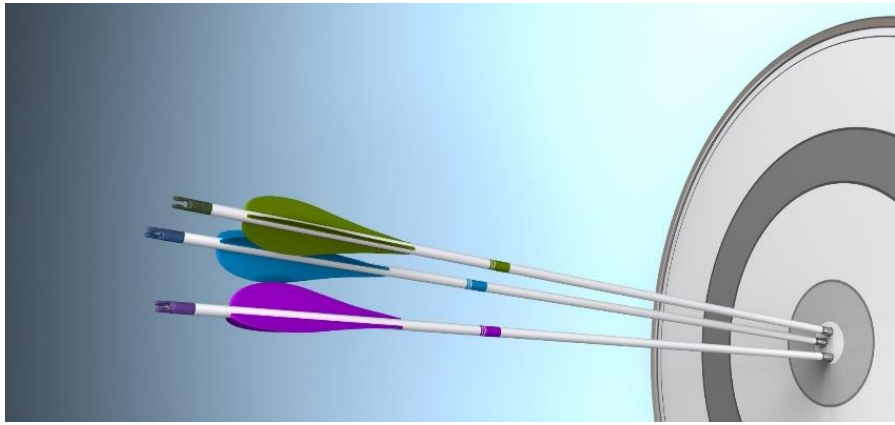
- John uses his new access to look for vulnerabilities in devices on the Physical Protection System networks
- He exfiltrates sensitive information about physical security at the Gula Hospital
- Anshar Dawn is preparing to disable the Physical Protection System, then have a group break into the Gula Hospital and steal the Cesium-137 source

Result of the PPS Network Attack

INSIDER THREAT MITIGATION

The Adversary has acquired the following information

1. Identified key PPS hosts, cameras, and alarm equipment that protect the blood irradiator
2. Identified key personnel, contractors, and service providers that have access to the secure room
3. Exfiltrated Site Security Plan that details measures, procedures, and response



Contacts

INSIDER THREAT MITIGATION

Greg Herdes (gregory.herdes@nnsa.doe.gov)

Greg White (white6@llnl.gov)

Mike Rowland (mtrowla@sandia.gov)