



ADVANCING INFCIRC/908 INTERNATIONAL

— WORKING GROUP —

Cyber Insider Training for Radiological Sources
Instructor Guide

This page intentionally left blank

Time Allotted:	3 hours
Instructional Methods:	Presentation, Discussion
Information Release No.	LLNL-PRES-831032

Module Overview and Instructor Guidance

- | | |
|------------------------------|--|
| Instructor responsibilities: | <ul style="list-style-type: none"> • This module is delivered in a <i>classroom setting</i>. • Instructors are responsible for obtaining site/country specific information including what equipment is being deployed/used and coming prepared to train on that equipment. • Verify that participants have received all necessary supplies and equipment needed to complete this training as listed below. • Instructor-led facilitation is scheduled for 3 hours. • Activity: <i>N/A</i> |
|------------------------------|--|

Evaluation opportunities:	Evaluate participants through discussion, knowledge checks, and observations during the activities.
---------------------------	---

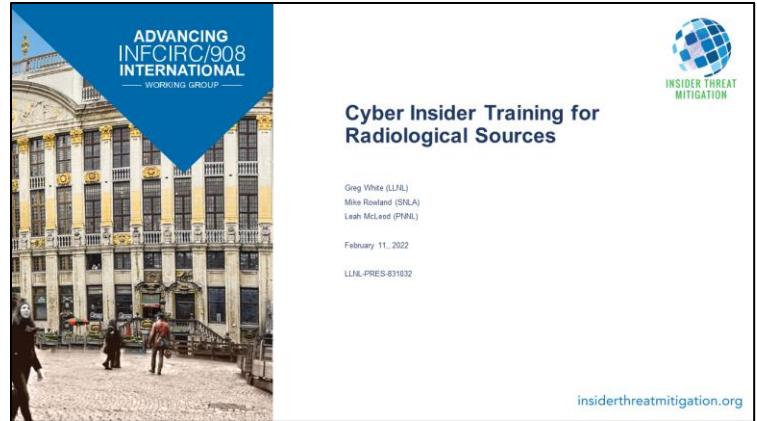
Safety briefing:	Remind participants of the general safety, emergency egress information, and any other safety related information required by the site.
------------------	---

- | | |
|--|--|
| Course materials, training aids, and supplemental materials: | <ul style="list-style-type: none"> • <i>Instructor Guide</i> • <i>Participant Guide</i> • PowerPoint file • Instructor laptop, tablet, or desktop computer |
|--|--|

Cyber Insider Training for Radiological Sources

Good afternoon, everyone and thank you for joining me in this training session. Today, we are going to be gaining some Cyber Insider Training for Radiological Sources.






Introduce instructors and students.




Modules

Let's talk about how cyber security is affected by an insider attack and how we can protect against it. We will also discuss several real-world examples of cyber insiders and their effect on their organizations. We will then walkthrough how a hypothetical organization can deal with an incident. Then we will walkthrough the incident from the attacker's perspective. Finally, we will discuss how an organization can prevent and protect against the insider.

Modules



1. Basics and Incidents
2. Cyber Incident Response Walkthrough
3. Cyber Insider Attacker Actions
4. Prevention and Protection

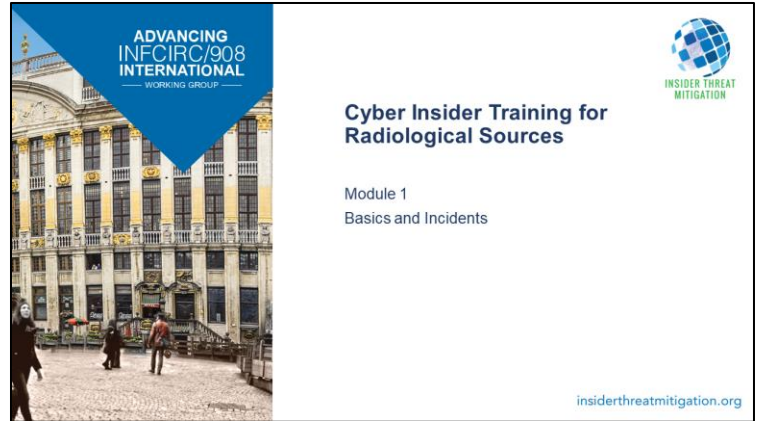

INSIDER THREAT
MITIGATION

insidethreatmitigation.org

Module 1

Basics and Incidents


Let's talk about the basics of the insider threat and several examples of insiders and their effect on the organizations.




Topics

Let's talk about how cyber security is affected by the insider attack and how we can protect against it. We will also discuss several real-world examples of cyber insiders and their effect on their organizations.

Topics



- Basics of cyber insider
- Real-world, industry-adjacent examples
- Learn how an insider with cyber capabilities can affect the operations of your facility



insidethreatmitigation.org


4

Computers are everywhere!

Every nuclear and radiological facility is filled with computers. These computers run every facet of your organization's business. This makes an insider with cyber capabilities especially dangerous and effective. The cyber insider compromises the confidentiality, availability, and integrity of the computer systems.

Computers are everywhere!

- Every operational or security system is computerized
 - Physical Security
 - Nuclear Material Control and Accounting
 - Industrial Control Systems
 - etc.
- All of them can be compromised by an insider with cyber capabilities
- Computer attacks compromise confidentiality, availability and integrity




insidertreatmitigation.org

Cyber Insiders

- Motives were often highly personal and were related to problems that the employees were facing when they decided to exploit or sabotage the organization's information systems.
- Some insiders were under financial stress and used the information systems to embezzle funds or access proprietary information that they then sold to competitors.
- Other insiders felt unappreciated for their work and wanted to prove their expertise by creating a cyber breach that they then solved.
- And in other cases, the employee was facing discipline or termination and wanted to embarrass the organization or ruin its brand reputation.

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

insidethreatmitigation.org

The Insider Threat and Malicious Code

Ron Harris worked for the Nevada Gaming Control Board. They regulate gambling establishments in the US state of Nevada which includes Las Vegas. Part of their job is to ensure the fairness of slot machines. Just like nuclear and radiological facilities, slot machines have transitioned from mechanical systems to computerized systems with software. Ron Harris was part of the process of ensuring that the software installed on these slot machines worked as described by the manufacturer and was fair to both the player and the facility.

Ron used his position to install a modified version of the software into 30 slot machines before they were put in casinos. This allowed him to initiate an input sequence that put the slot machine into winning mode where it paid out the maximum amount. The sequence was:

- 3 coins, pull level once
- 1 coin, pull lever twice
- 1 coin, max payout


Since he worked for the gaming board, he was not allowed to gamble in Nevada. So he hired accomplices to gamble for him and split the profits. This continued for about 2 years.

One of his friends Reid McNeal got caught. In friend's hotel room was a police scanner, computer equipment, software and Ron Harris. Ron was found guilty and was sentenced to 7 years in prison. He has since been released and is prohibited from entering casinos in the state of Nevada.


Reference:

<http://www.cnn.com/2006/TECH/07/13/popsci.gambling/>

The Insider Threat and Malicious Code



- Ron Harris case: slot machines
 - He worked for the Gaming Control Board in the Electronic Services Division in Las Vegas testing slot machines
- He installed malicious code in a testing unit
 - He downloaded an altered version of the software to 30 slot machines when he checked the machines as part of his job
 - A special sequence of coins activated "winning mode"
 - His change was never detected
 - He and his accomplices made hundreds of thousands of dollars
- Caught when winnings of an accomplice sparked an investigation



What could the gaming board have done to detect, prevent or mitigate this damage?

insidethreatmitigation.org

Jonathan Toebbe

Jonathan Tobbe was a nuclear engineer working for the US Navy. He started his disclosure and sending an unsolicited letter by regular mail and includes a memory card to a foreign government. That government passed that information to the US FBI who then posed as representatives of the foreign government. Jonathan tried to hide his actions by using two encrypted email accounts (Proton mail), exchanged asymmetric keys, used public Wi-Fi and TOR, and asked for \$100k payments in cryptocurrency (Monero). For that, he gave the FBI agents and SD card which contained critical information about the design of submarine nuclear reactors and design information about the Virginia fast-attack submarine.

Background Information:





<https://www.secureworld.io/industry-news/navy-insider-threat-case-court-documents>

Jonathan Toebbe

- 42 years old, worked as a nuclear engineer in the US Navy
- Sent a letter by mail with an SD card to a foreign government in April 2020
- The foreign government passed the information to the US Federal Bureau of Investigation (FBI), who posed as the foreign government
- Used encrypted email and files, public Wi-Fi and TOR, received payments in cryptocurrency (\$100K)
- SD cards contained design information for submarine nuclear reactors and schematic designs for the Virginia fast-attack submarine

What could the US Government have done to detect or prevent this damage?

insidertreatmitigation.org

Jonathan Toebbe (continued)

Jonathan was concerned that he wasn't dealing with the foreign government. He asked for a particular signal at their embassy. Through the FBI, the foreign government replied.

After that confirmation, they convinced him to switch to dead drops with encrypted SD memory cards. During these dead drops, his wife acted as a lookout. He hid the SD memory card inside a wide range of items.

Him and his wife were arrested by the FBI and US Naval Criminal Investigative Service in October 2021. 13 months later and after both having a plea agreement, Jonathan was sentenced to 18 years and the wife was sentenced to 21 years. The judge felt that the wife was driving the crime and tried to pass Jonathan a message in jail for him to lie, by sticking to the plan and absolve her of wrongdoing.

Background Information:

Criminal Complaint: <https://www.justice.gov/opa/press-release/file/1440946/download>

Conviction: <https://www.justice.gov/opa/pr/maryland-nuclear-engineer-and-wife-sentenced-espionage-relatedoffenses#:~:text=A%20Maryland%20man%20and%20his,over%2019%20years%2C%20of%200incarceration.>

Plea agreement: <https://lawandcrime.com/crime/after-rejection-by-federal-judge-couple-reaches-new-plea-deals-in-nuclear-submarine-secrets-case/>

Sentencing: <https://www.bbc.com/news/world-us-canada-63578924>

Jonathan Toebbe (continued)

- Jonathan asked foreign government (FBI) for a signal on their property (embassy) that he was dealing with them directly
 - Foreign government complied
- FBI convinced him to switch to dead drops to leave encrypted SD cards
 - Located inside bandages, chewing gum wrapper and a peanut butter sandwich. Wife was the lookout
- Jonathan and his wife were arrested by FBI and NCIS (Naval Criminal Investigative Service) on October 9, 2021
- In November 2022, Couple accepted plea agreements and where convicted for sentences of 18 and 21 years

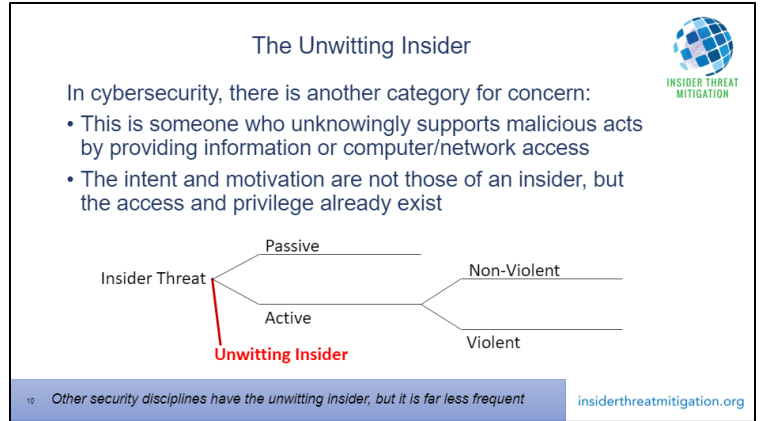
» What could the US Government have done to detect or prevent this damage?

The Unwitting Insider

In most cases, the insider knows that his actions are causing damage to the facility and is deliberate. However, with cyber there is the unwitting insider. They support the malicious act without knowing the potential damage of their actions. They don't intend to cause damage to the facility, but the result is the same.

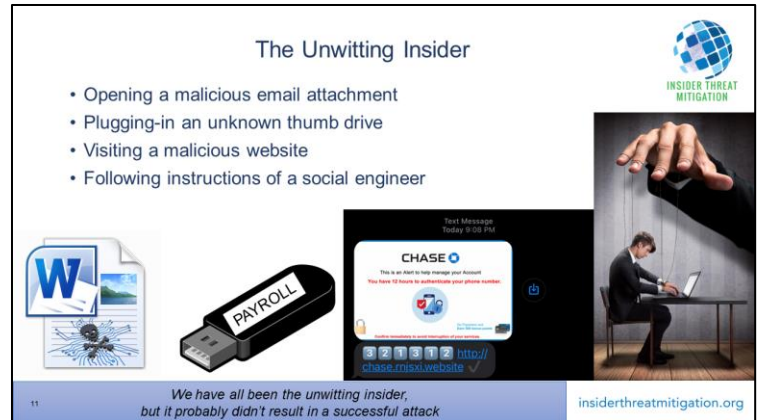
Background Information:

IAEA Nuclear Security Series No. 8, Preventive and Protective Measures Against Insider Threats: Implementing Guide. Figure. 1. Categories of insiders [Color graphic], adapted and recreated in PowerPoint by LLNL and modified to show Unwitting Insider and reflect current thinking that no longer considers rationality when classifying insider threats



The Unwitting Insider

- In most cases, the insider knows that his actions is causing damage to the facility and is deliberate.
- However, with cyber there is the unwitting insider. They support the malicious act without knowing the potential damage of their actions.
- The user may open a document attached to their email, visit a malicious website, or insert a USB thumb drive into their computer that they found dropped into the parking lot. Any of these may install malicious software on their system. They don't intend to cause damage to the facility, but the result is the same.



Unwitting Insider Example


In 2012 a power company in the US found that there was a computer virus infecting 10 computers which controlled a turbine. Investigators found that a 3rd party technician has inserted a USB thumb drive into one of these computers to install software updates during a maintenance period. The USB drive was infected with a virus, which spread to the other computers on the network. Removing the virus took time and delayed the plant restart by 3 weeks.

Reference:

http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf

https://en.wikipedia.org/wiki/Mariposa_botnet

Unwitting Insider Example





INSIDER THREAT
MITIGATION

Virus infection at an electric utility

- In 2012, a power company reported a virus infection in a turbine control system that impacted approximately ten computers on its control system network
- Analysis of the incident revealed that a third-party technician had used a USB drive to upload software updates during a scheduled outage for equipment upgrades
- Unknown to the technician, the USB drive was infected with a variant of the Mariposa botnet virus, which moved from machine to machine on the local network
- The infection resulted in downtime for the impacted systems and delayed the plant restart by approximately three weeks

12 What could the company have done to detect, prevent or mitigate this damage?

insidertreatmitigation.org

Computer Roles and Functions


Everyone that operates a computer is given some level of access and authority with that computer and the network it runs on. But system administrators, network managers, and software developers are given a higher level of access and authority on these systems as part of their job. We must consider that with this increased access and authority gives them the ability to cause more damage if they become an insider. We must provide more oversight for personnel that have more access and authority.

This is also why we do cyber threat education for the entire staff. Everyone should be aware of social engineering that specifically targets your staff.


Computer Roles and Functions

What roles and access potentially support insider activity?

- System administrator (Sysadmin)
Sysadmins are usually charged with installing, supporting, and maintaining servers or other computer systems and planning for and responding to service outages and other problems.
- Maintenance, technical operations, integrators
- Network Managers
- Software Developers
- Operators
- Employees



13 All have a level of authority over the system they manage and operate.
What is the level of oversight for these personnel?



insidethreatmitigation.org

Large Defense Manufacturing Company


System administrators, by their job function, have the highest level of access and authority over the computers they manage. They can often do the most damage to your facilities computer systems. Let's consider the case of a large defense manufacturing company. They had a system administrator that felt he wasn't being appreciated for the work he had done for the company. As the company dropped his level of responsibility, he became angry and bitter. He consolidated all of the manufacturing processes to a single computer and acquired the only backup tapes. Later, he was fired for inappropriate conduct and abusing his coworkers.

Reference:

Keeney, Michelle, J.D., Ph.D., *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, U.S Secret Service and CERT Coordination Center/SEI May 2005.

Large Defense Manufacturing Company

- A system administrator worked for a large defense manufacturing company
 - By himself, he had created and managed the computer network
 - The company had diminished his role which made him angry
 - He moved all the critical software that ran the company's manufacturing processes to a single server
 - He then intimidated a coworker to give him the only backup tapes for that software
- He was then fired for inappropriate and abusive treatment of his coworkers



INSIDER THREAT
MITIGATION

insidethreatmitigation.org

14

Large Defense Manufacturing Company (continued)


Unfortunately, he had installed custom software to run if he was ever fired. This software is called a dead man's switch. The software deleted the only copy of the company's critical software. The damage to the company was \$10 million and led to the layoff of about 80 employees.

Reference:

Keeney, Michelle, J.D., Ph.D., *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, U.S Secret Service and CERT Coordination Center/SEI May 2005.

Large Defense Manufacturing Company (continued)

- Before he was fired, the system administrator had installed a software script (sometimes called a dead man's switch) on the single critical server
- Later, the script ran and deleted the only remaining copy of the critical software from the company's server
- The company estimated the cost of the damage to be in excess of \$10 million, which led to the layoff of about 80 employees



15 What could the company have done to detect, prevent or mitigate this damage? insidertreatmitigation.org

Maroochy Australia Sewage Treatment

Let's look at another example. Vitek Boden worked for a contractor that installed and operated a sewage system in an area of about 70 cities in Australia. He had a disagreement with his company and quit. He then tried to get the local government to hire him directly to perform the same job. When they didn't hire him, their sewage system started malfunctioning. Sewage was spilled, causing large amounts of environmental damage. Experts were hired and initially thought the problems were just equipment failures. They replaced equipment, but the system kept failing.

References:


<https://malicious.life/episode/episode-7-stuxnet-part-1/> [The Maroochy Incident]


https://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

<https://cams.mit.edu/wp-content/uploads/2017-09.pdf>

Maroochy Australia Sewage Treatment

- Maroochy Australia (an area of about 70 cities) has a sewage system with 142 pumps
- Vitek Boden worked for a company that installed the control system
- He resigned from his company (after a disagreement with his bosses), then he tried to convince the local government to have him work directly for them, but they declined
- The sewer system started breaking regularly
 - 200,000 gallons of sewage leaked into the environment
 - This turned the river black, killed fish and wildlife, and destroyed nature reserves
- Experts looking at the problems and initially thought it was normal equipment failures
- Despite new equipment, failures continued





insidethreatmitigation.org

Maroochy Australia Sewage Treatment (continued)

Then, late one night, one of the experts reconfigured a pump, but another pump changed the configuration back. This seemed odd. He renumbered the pump that had changed the configuration, but the network traffic indicated the bad pump was still reconfiguring other pumps. This indicated some kind of network breach. Vitek Boden was identified as a suspect and they hired someone to follow him. He was found near one of the pumping stations with a laptop and a wireless radio. The laptop had a pirated version of the control software installed on it. They found he had made at least 46 attempts to take control of the sewage system. He was convicted and sentenced for his crimes.

References:

<https://malicious.life/episode/episode-7-stuxnet-part-1/> [The Maroochy Incident]

https://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/



<https://cams.mit.edu/wp-content/uploads/2017-09.pdf>

Maroochy Australia Sewage Treatment (continued)

- One of the experts who was working late at night put a new configuration in a pump, but another pump (#14) changed it back
- The expert renumbered the #14 pump to be #3, but the command again came from pump #14 (which now didn't exist), which implied it was a network breach
- Vitek Boden was identified as a suspect and was followed
- He was found near one of the pumping stations with a laptop, a wireless radio, and a pirated version of the control software
- He had made at least 46 attempts to take control of the sewage system
- He received a two-year prison sentence and fined \$13,000

17

What could the government or company have done to detect, prevent or mitigate this damage?

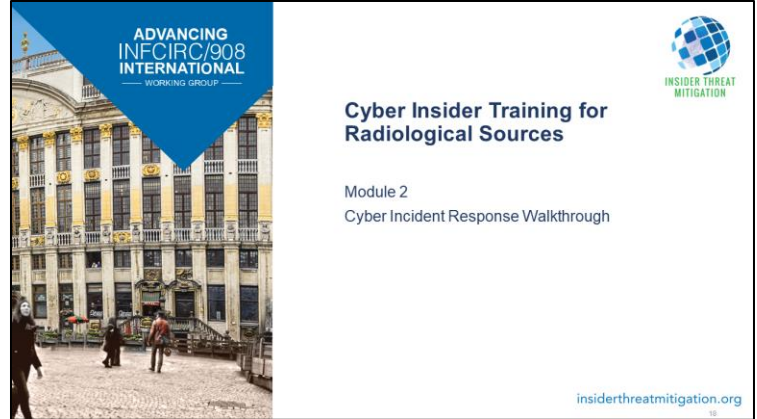



insidertreatmitigation.org

Module 2

Cyber Incident Response Walkthrough


In the next module, we'll walk through a cybersecurity incident from the perspective of the hypothetical facility being attacked.




Topics

Here is a list of the major topics we are going to discuss in this module. We start with familiarizing you with the hypothetical facility. We'll then walk through the incident, discussing each step along the way. Finally, we'll then discuss the overall incident.

Topics



- Anshar and Gula Regional Hospital Overview
- Scenario Steps and Polls / Discussion
- Post-Incident Discussion




insidertreatmitigation.org

19


Country of Anshar Overview

Anshar is a hypothetical country. They have a full set of state organizations, from a nuclear regulator, a cybersecurity organization, a federal law enforcement organization, and an intelligence service. There are three primary facilities. A regional hospital with radiation sources, a nuclear power plant, and a nuclear research institute.

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



insidertreatmitigation.org


Gula Regional Hospital

This incident will happen at the Gula Regional Hospital. It serves about a thousand patients per week. It includes two high-activity radioactive sources: a blood irradiator with a cesium source, and a teletherapy device with a cobalt source.

Reference: IAEA Hypothetical State Facility

Gula Regional Hospital

- 1000 patients per week
- Radioactive Material Devices
 - Blood Irradiator – Cesium-137
 - Teletherapy Device – Cobalt-60

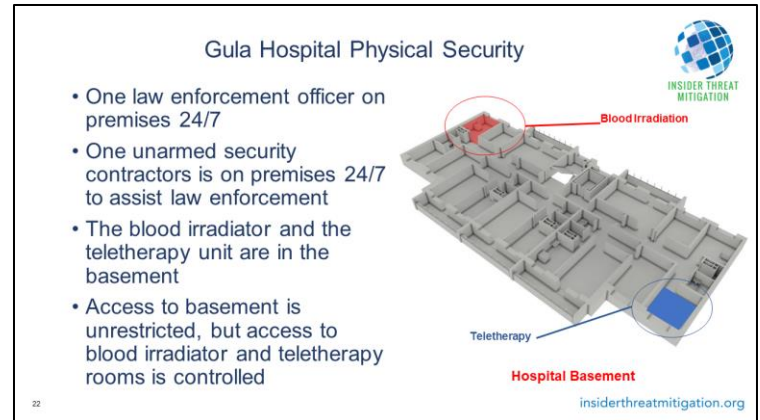


insidethreatmitigation.org

21

Gula Hospital Physical Security

- Arrangement with local law enforcement has one police officer on premises 24/7
- Also, one unarmed security contractor is on premises 24/7 to assist law enforcement
- Rooms that contain 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



Reference: IAEA Hypothetical State Facility

Gula Hospital Networks

There are four networks at Gula

Green – Complimentary Guest Wi-Fi to be used by patients and staff. No password required.

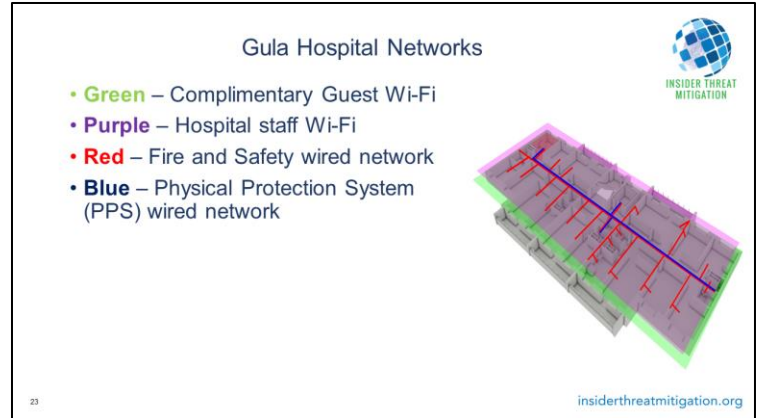
Purple – Hospital staff Wi-Fi for Gula personnel to conduct communications throughout the hospital. Password required

Green and Purple are supported by the same network infrastructure (routers/switches) separated by VLANs.

Red – Fire and Safety wired network. Enables fire sensors and life monitoring devices to communicate with nurse station.

Blue – Physical Protection System (PPS) wired network. Blue network runs throughout Gula. Endpoints are cameras, sensors, door controls, etc. and report to Central Alarm Station

Reference: IAEA Hypothetical State Facility




Gula Hospital Cybersecurity Program

Gula has a basic Cybersecurity Program. The head of security is responsible for the cybersecurity program. An initial inventory and risk assessment has been completed but hasn't been updated. There is no incident response team and there are no response and recovery procedures. There is a staff cybersecurity awareness training program.

Gula Hospital Cybersecurity Program

- 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.



insidertreatmitigation.org


24

Gula Hospital Computer Support

Gula staff do basic computer administration and cybersecurity hygiene, but anything more complicated than that are done by on-site contractors or external contractors.

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



insidertreatmitigation.org


25

9am Monday

- A cloud provider in Anshar calls Head of Security
 - One of the machines hosted by the cloud provider has been used in the conduct of a cyber-attack campaign targeting key organizations significant to Anshar's national security
 - Encrypted data was sent to this machine from an IP address registered to Gula's guest network
- Cloud provider sends an email detailing the:
 - Suspect IP address at the cloud provider
 - Hospital IP address (from the Guest Network)
 - Dates and times of transmissions for past 30 days
 - Size of transmissions are 5KB – 10MB each, about 100MB total
 - Further information will be provided later

9am Monday

- 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



insidethreatmitigation.org


26

Poll / Discussion

So, what should we do first?


The desired answer is (3) Set Up an incident response team

Poll / Discussion



What should be the first action by the head of security?
(Select one)

1. Power Down the IT and/or PPS Network
2. Ask Cloud Provider for additional information
3. Set up an incident response team
4. Review IT Network Logs (past 30 days)
5. Review PPS Network Logs (if available)



insidethreatmitigation.org


10am Monday

The head of security decides this is a critical problem and he should convene an incident response team. But he doesn't have one already setup, so this will have to be ad hoc, for now.


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?



insidethreatmitigation.org



Poll / Discussion

Let's think about what kind of expert our head of security might want on his cyber security incident response team? He wants a multidiscipline team.



The desired answers are:

1. Physical Security Personnel
2. Radiation Protection Personnel
3. Internal IT Staff
4. Service Providers (includes contractors for Advanced IT tasks)

Poll / Discussion

What types of experts/personnel should be included?
(Select one or more)

1. Physical Security Personnel
2. Radiation Protection Personnel
3. Internal IT Staff
4. Vendors
5. Service Providers
6. Contractors for Advanced IT tasks
7. Legal Department (lawyers)
8. Anshar State Organizations (CERT, Regulator)



insidethreatmitigation.org


11am Monday

The head of security assembles the incident response team, made up of hospital staff. He leads the meeting and talks about each member's roles and responsibilities.


There are lots of things we don't know right now. The cloud provider can't tell us what kind of information was exfiltrated since it was encrypted. It's on the guest wireless network, so we aren't sure if one of our devices was compromised. We also don't know what the attacker was trying to accomplish.

We also don't have information about our networks and devices that would help the investigation. Some of the information we have lacks the details we need.

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



insidertreatmitigation.org

30

Poll / Discussion

What actions should we prioritize?


The desired answer is:

2. Identify potential information sources

Poll / Discussion

What action should the incident response team prioritize? (Select one)

1. Ask cloud provider for more information
2. Identify potential information sources
3. Power down wired and wireless networks
4. Deny all access (i.e., lock out) all areas secured by PPS.
5. Run Anti-virus on everything
6. Walk down of all assets



insidethreatmitigation.org

31


9am Tuesday

The incident response team has gone off and found out what information sources they could acquire.

We have network diagrams that include our defensive architecture, risk scenarios with consequences, and a list of our most important assets.


We also have several logs. We have network logs for 30 days, IT system logs for different time periods and physical protection system host logs for 90 days.

9am Tuesday



- 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)
 - PPS host logs (90 days)

Which source should be prioritized?



insidertreatmitigation.org

32

Poll / Discussion


Of the information sources we have, what should we prioritize?

The desired answer is:

4. Network logs


Rationale: The initial discover was exfiltration from the network.

Poll / Discussion


INSIDER THREAT
MITIGATION

Which of these information source should the incident response team prioritize acquiring and analyzing? (Select one)

1. List of network drawings; including defensive architecture specification
2. Risk registry/scenarios associated with consequences
3. List of most valuable assets
4. Network logs (30 days)
5. IT system logs (variable periods)
6. PPS host logs (90 days)


insidethreatmitigation.org

33

9am Thursday


By looking at the logs, we've found some interesting traffic. This was early in the attack and isn't the encrypted data that the cloud provider found. Basically, the attackers weren't as careful as they should have been this early in the attack. They sent some unencrypted web/http traffic which implies the transfer of sensitive information and passwords from the physical protection system (PPS) via the guest wireless network.

But the two networks aren't connected to each other. This is called an air gap.

So how did this data from the PPS network get to the guest wireless network?

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)



insidethreatmitigation.org

34

Poll / Discussion

With this new information, what should the incident response team do next?


The desired answer is:

5. Walk down PPS hosts and networks

Poll / Discussion

What action should the incident response team perform next? (Select one)

1. Shut down PPS network
2. Shut down all networks
3. Turn of Wi-Fi for all systems and networks
4. Walk down all computer assets
5. Walk down PPS devices and networks
6. Ask Cloud Provider for additional information



insidethreatmitigation.org


35

1pm Thursday

- The team has found an unauthorized raspberry pi connected to the physical security wired network. A raspberry pi is a credit card sized standalone computer. It has a Wi-Fi device.
- The device was found in a locked panel within the central alarm station. Access to this area is strictly controlled and only authorized staff and contractors are allowed.
- The head of security calls an urgent incident response meeting.

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



insidethreatmitigation.org

36

Discussion Next Steps

We've solved the immediate problem, but how do we deal with the larger problem? We seem to have an insider or an access control issue. We also need to figure out what the attacker did to devices on our physical security network?

Discussion Next Steps

INSIDER THREAT MITIGATION

What should then be prioritized?

- Investigate to determine who placed the device in the Central Alarm Station panel.
- Quarantine and eradicate the physical protection security environment

```
graph LR; A[Preparation] --> B[Detection & Analysis]; B --> C[Containment, Eradication & Recovery]; C --> D[Post-Incident Activity]; D --> A;
```

insidertreatmitigation.org

37

Poll / Discussion

What order would you do the following steps?



This is the correct order.

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

Poll / Discussion

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

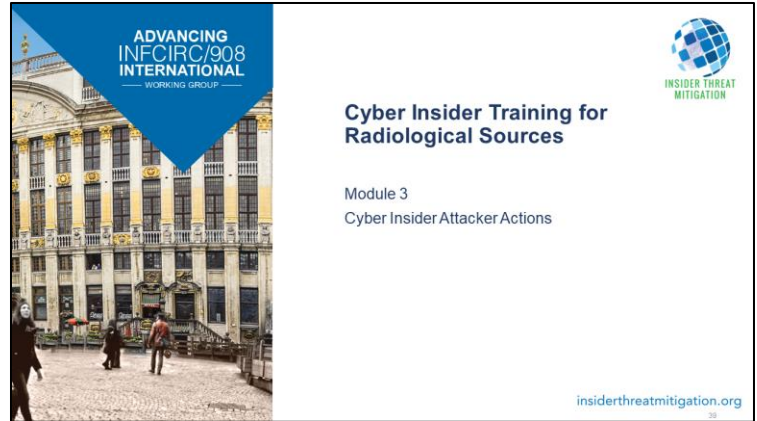


insidethreatmitigation.org

Module 3

Cyber Insider Attacker Actions


In the next module, we'll discuss the same incident from the attacker's perspective.




Topics

We are going to look at both the steps they took before the devices was discovered, but the next steps they intended to take.

Topics



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



insidethreatmitigation.org

40



Introduction

Bob is an unarmed security guard at the Gula Hospital. He has a large amount of personal debt and is struggling.



John is a member of the group Anshar Dawn, a terrorist group who operates against the government of Anshar. John knows about Bob's work at Gula and his crippling debt.


Introduction

- 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.



insidethreatmitigation.org

Information Gathering


What is the most likely motivation for the insider in this description?


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**

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




insidethreatmitigation.org

42


Information Gathering

John the Terrorist gathers information about the Gula Hospital, some of it by walking around and inside the facility, some open-source intelligence, and talking with Bob the guard.


He learns that Gula has a:

- Guest Network
- Wired and wireless networks for hospital staff
- An isolated network for the physical protection system.

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



insidertreatmitigation.org

43

Negotiations

John offers help for Bob's financial problems. John will give Bob money in exchange for Bob putting a small, credit card sized computer in a physical security equipment closet. Bob decides he can do it with a low probability of getting caught. Bob and John talk about the details of their plan, both logistical and technical.

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




insidethreatmitigation.org


44

Bridging Gula Hospital's Networks

Some time when he's alone, Bob goes to the central alarm station, and uses his keys to open the equipment closet and uses his keys to open the equipment closet and installs the small, credit card sized computer and hooks it up to the physical security network and power.




John has pre-configured the device to connect wirelessly to the Guest network and bridge it and the wired physical protection system network. It provides a clandestine command and control path from anywhere on the internet to the physical security network.

Bridging Gula Hospital's Networks



INSIDER THREAT
MITIGATION

- Bob uses his security keys to open the equipment closet and install the credit card sized 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

insidertreatmitigation.org

45

Network Access





John uses this access to look for what kind of devices are used on the physical protection network at Gula. He then looks for vulnerabilities in those devices.

Those vulnerabilities give him additional access and allows him to exfiltrate sensitive information about physical security at Gula. He can also control many of the devices.

His plan is to at the right time disable to physical protection system and simultaneously have a group break into Gula and steal the large Cesium-137 source in a blood irradiator.

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

insidertreatmitigation.org


Result of the PPS Network Attack

Before the attack, John new a lot of information about the physical security at Gula. He identified key devices and computers on the physical security network, like cameras and alarm equipment. He also knows firmware and software versions.

He was able to identify key personnel, contractors and service providers that have access to the secure room and regularly perform work on-site.


He was able to exfiltrate the site security plan, which included security measures, procedures, and response plans.

Result of the PPS Network Attack



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



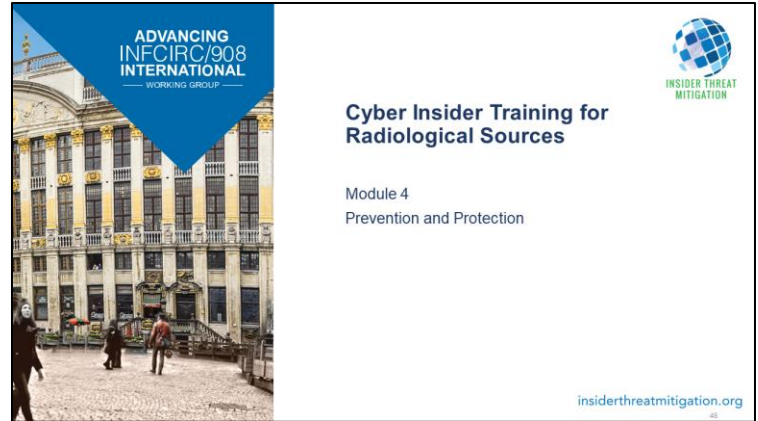
insidethreatmitigation.org

47

Module 4

Prevention and Protection


In this module we will discuss how to prevent and protect against an insider attack.




Topics

We'll start this module with talking about the differences between preventative and protective measures. We will then discuss the different types of controls we can implement. This includes technical, administrative, and physical controls.





Topics



- Difference between Preventive and Protective Measures



- Controls
 - Technical
 - Administrative
 - Physical



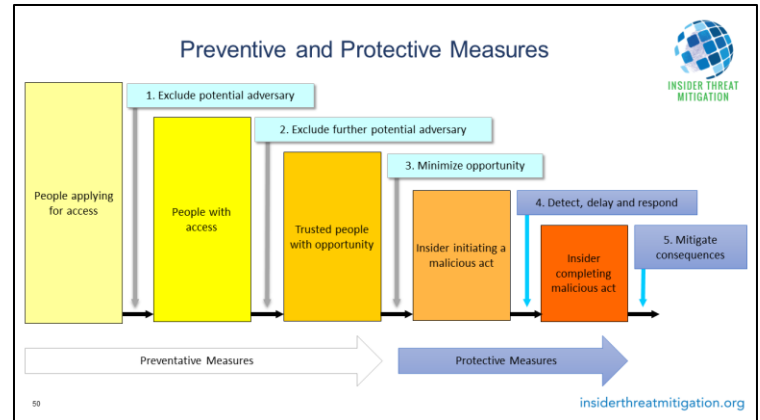
insidethreatmitigation.org

49

Preventative and Protective Measures

This is IAEA's preventative and protective measures for the insider.

Findings from the cyber sabotage closely parallel pre-attack behavior in cases of workplace violence, thus the need for disciplines to work together: cyber, physical security, HR and employee assistance or mental health.



Insiders who sabotage or exploit information systems don't just snap. Before major incidents, they follow a pathway of planning and research. They engage in troubling behavior that is observable – online and in person – and that alarms co-workers and friends. In some cases, they tell others explicitly about the malicious insider activity they are planning. This finding illustrates that information about potential insider threats may be known to physical security personnel, or cybersecurity personnel, or both before harm occurs – thus underscoring the need for these departments to share information to prevent insider sabotage.

Across these cases, some pre-incident information was observable within the insiders' online behavior, while other pre-incident behavior was observable in the insiders' offline or in-person behavior.

When security professionals determine that someone is on a “pathway to violence” or is planning cyber damage to the organization, they can try to determine what is driving that behavior.

Sometimes connecting a stressed employee to mental counselling, financial counselling, or changing supervisors or departments, can be all that is needed to defuse hostilities and mitigate risk.


Resource:

SEI/US Secret Service report: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7227>


Technical Controls

The key with any technical controls is have well defined roles and responsibilities and looking at the data you are generating. For instance, we need to limit access and administrator privileges to only what each employee needs to do their assignment. We need to implement robust identification and authentication of users on our systems. We should also implement encryption and network switches to keep network traffic safe from snooping. We should also install firewalls and data diodes to enforce network separation and boundary protection. Finally, we need to collect computer events and auditing to flag suspicious activity. We should also implement intrusion detection tools to look for anomalous behaviour. Of course, if we don't regularly look at these events, audits, and intrusions, they aren't effective.

Technical Controls



- Preventive:
 - Implement **access control** and **least privilege**: limit all employees to only the access and privilege needed to perform their job
 - Require **identification** and **authentication** of individuals operating on computing systems
 - Use **encryption** and **network switches** to prevent unauthorized network monitoring
 - Enforce **boundary protection**, including the creation of zones to limit both internal and external system access
- Protective:
 - Use **event logging** and **auditing** to track and flag suspicious activity
 - Use **intrusion detection** tools to detect anomalous behaviour patterns



insidethreatmitigation.org





51

Administrative Controls

We can also implement administrative controls. Vetting worker's background is critical, especially those with elevated access. We can segregate duties to ensure that one person can't compromise the system by himself. We need clear policies on what actions are allowed or disallowed with clear consequences. Clear guidance on how access is removed when employees leave an organization, both under good and bad situations. Finally, we need proper training of all employees on the cyber insider threat, company policies, detecting abnormal behaviour and to respond to cyber events.

Administrative Controls

- Preventive:
 - Detailed **vetting of workers**, especially those with elevated network and computing system access
 - **Segregation of duties** to ensure no single person can compromise the security of the computer system
 - Clear **policies detailing unapproved actions** on computing systems and the consequences of such actions
 - Clear **policies on the removal of access** to employees that have exited the organization
- Protective:
 - **Training** should include an understanding of expected employee behaviours, recognition of abnormal behaviours, and the proper response to such events

See something ... Say something


insidethreatmitigation.org

Physical Controls

Finally, physical security can enhance our ability to combat the cyber insider. Only employees with an appropriate job function should be allowed physical access to computer systems. This may be controls at the site level (like badges and access control systems) and at lower levels (access control for computer rooms or individual racks of equipment). We should prevent employees from making covert changes to the networks or computer systems.

Physical Controls

- Preventive:
 - **Physical access control** to computing systems based on job function
- Protective:
 - Create a **secure computing environment** to minimize the potential of covert computer activities



insidethreatmitigation.org

53

Assumptions

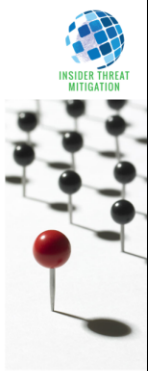
It is important to remember some things about insiders.

- Every organization can have an insider threat. They can be minor or very serious.
- We can't solve the problem with just background checks. These checks need to be done both pre-employment and periodically. Some indicators of an insider threat can't be detected by a background check or can happen between periodic checks.
- Red flags of an insider will sometimes be missed or downplayed.
- Security rules and procedures won't always be followed. This makes the insider's job easier.
- It is possible for insiders to conspire with each other.
- The culture of an organization and the relative happiness of the employees is an important factor.
- Remember that insiders often know the facility's security measures, so they can work around them.
- We need to use multiple layers of defense to prevent and protect against an insider threat.
- Finally, we need to also mitigate the insider threat.

Assumptions

- Unwitting insiders will happen
- Serious insider problems are possible in your organization
- Background checks are not the only solution
- Red flags will be missed or not acted on
- Security rules aren't always followed
- Insider conspiracies are possible
- Organizational culture and employee disgruntlement matters
- Insiders will know about security measures and how to work around them
- You will need multiple protection measures

54 Don't focus on just Prevention and miss opportunities for Mitigation insidertreatmitigation.org



Resource:

A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes, Matthew Bunn and Scott D. Sagan, <https://www.amacad.org/publication/worst-practices-guide-insider-threats-lessons-past-mistakes/section/2>

Conclusions


There are many similarities between insiders and cyber insiders, but there are also key differences. The differences include the ability to affect multiple disciplines with computer access, and the idea of the Unwitting Insider. We have shown several examples of the cyber insider and described several preventative and protective measures that can assist us. We need a layered defense strategy. Preventative measures can exclude or remove potential insiders, minimize their opportunity to act. Protective measures are used to detect, delay, respond to, and mitigate malicious acts.

Reference:

IAEA Nuclear Security Series No. 8, Implementing Guide: Preventive and Protective Measures against Insider Threats


Keeney, Michelle, J.D., Ph.D., Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, U.S Secret Service and CERT Coordination Center/SEI May 2005

Conclusions



INSIDER THREAT
MITIGATION

- Insiders with cyber capabilities have **access**, **authorization**, **knowledge**, and some level of **motivation** to perform an attack
- Personnel can be an unwitting insider
 - For instance, someone who inserts an infected USB flash drives into their computer
- The cyber insider threat should be part of security training
- Insider attacks can only be prevented through a layered defense strategy consisting of policies, procedures, and technical controls
 - Preventative measures can be used to exclude or remove potential insiders, or minimize their opportunity to act
 - Protective measures can be used to detect, delay, respond to, and mitigate malicious acts



insidertreatmitigation.org

55

Discussion

Have an open floor for discussion asking:

- Did your perception of insider threats and how to handle them change?
- What can we do in this environment to do our part?
- What questions do you have?

Discussion

INSIDER THREAT MITIGATION

- Did your perception of insider threats and how to handle them change?
- What can we do in this environment to do our part?
- What questions do you have?

OPEN

insidethreatmitigation.org

56

The slide features a large, semi-transparent circular graphic with the word "OPEN" in bold, capital letters. The background of the slide is a blurred image of a server room with blue and green lights. The text "Discussion" is at the top center, and the "INSIDER THREAT MITIGATION" logo is in the top right corner. The website URL "insidethreatmitigation.org" is at the bottom right, and the number "56" is at the bottom left.

Contacts

Here we've listed our email addresses.

Contacts





Greg Herdes (gregory.herdes@nnsa.doe.gov)
Greg White (white6@llnl.gov)
Mike Rowland (mtrowla@sandia.gov)
Leah McLeod (leah.mcleod@pnnl.gov)



insidethreatmitigation.org

57

Auspices



Lawrence Livermore National Laboratory is operated by Lawrence Livermore National Security, LLC, for the U.S. Department of Energy, National Nuclear Security Administration under Contract DE-AC52-07NA27344. This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

LNL-PRES-631032

58

insidethreatmitigation.org