



Cybersecurity and the Insider Threat Nuclear Facilities

Risk Management Exercise, Instructor Guide

2023

PNNL-SA-183134

VERSION CONTROL

Version	Description	Approval Date

1. RISK MANAGEMENT EXERCISE

Risk Management Exercise

Slide 1:

Instructor Notes:

- You may consider changing the dates on the slides starting on slide 10.
- You can break the students up into groups, ask the questions and then debrief each decision slide as a whole class.
- Each group selects a provided option or produces their own decision. Then they present their case to the class. Debate occurs.
- Let the students answer the questions on each slide before continuing to the next.



Slide 2:

Instructor Notes:

1. The whole point of the presentation is to lead the participant to understand that a structured and systematic approach to cybersecurity is not only needed but critical if they want to protect their nuclear and radiological assets.
2. While there are many methodologies and frameworks for building cyber security, this workshop will introduce the 5 core tenets of the NIST Cybersecurity Framework:
 - Identify
 - Detect
 - Protect
 - Respond
 - Recover



Risk Management Exercise

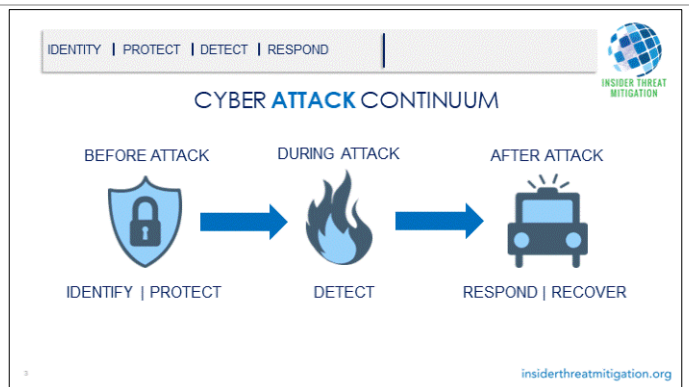
3. All slides are led to lead the participant to this conclusion. Each attack described for adversary TTP leads to the need for one of these tenants.

Slide 3:

Instructor Notes:

Highlight the continuum of a cyber attack.

1. We seek to identify potential attack points (vulnerabilities)
2. We seek to protect potential pathways into our environment
3. We put detection points in our environment to trigger response and recovery activities
4. Once detected we move into incident response mode with the goal of containing and remediating any issues
5. Finally we recover the system to a trusted and reliable state.



Risk Management Exercise

Slide 4:

Instructor Notes:

This is a build up to the basis of the exercise. A cyber security assessment team will have a diverse set of skills across multiple people.

Building a Cybersecurity Assessment Team

Overview of Exercise

NUREG 6847 Describes a CSAT Team of 3 to 7 Individuals with Broad Technical Knowledge in:

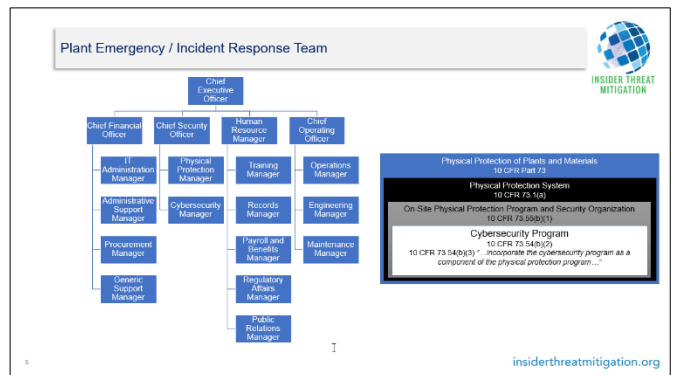
- **Information and Digital System Technology**
Areas of cybersecurity, software development and application, computer system administration, and computer networking. Knowledge is required of the digital systems involved in plant operations, including digital instrumentation and control systems, and those involved in plant business systems.
- **Nuclear Power Plant Operations, Engineering and Safety**
Knowledge of overall facility operations and plant technical specifications. Staff representing this technical area must be able to trace the impact of a vulnerability or series of vulnerabilities in connected digital asset outward through plant subsystems and systems so that the overall impact on safety, security, and emergency preparedness of the plant can be evaluated.
- **Physical and Operational Security**
Including in-depth knowledge of the plant's physical and operational security program.
- **Additional Considerations**
In addition to the above requirements, specialized in-depth cybersecurity skills are required to perform the electronic validation testing and optional scanning activities. The plant may not have on-site personnel trained and experienced in this arena. If this expertise is not available onsite, corporate-level cybersecurity personnel, an independent cybersecurity organization, or other sources of the validation expertise may be considered.

insidertreatmitigation.org

Slide 5

Instructor Notes:

Cyber security is a component of a broader nuclear security program.



Risk Management Exercise

Slide 6:

Instructor Notes:

Scenario setup – Each small group is to act as if they collectively are the head of cyber security and make decisions as if they were in that role.

Tabletop: [IDENTIFY] Managing Risks Asset & Vulnerability Management	Overview of Exercise	
	<ul style="list-style-type: none">• A nuclear power plant has recently named you as head of cybersecurity• You will be responsible for making strategic cybersecurity decisions for this power plant• A series of scenarios will be reviewed.	
		insidertthreatmitigation.org

Slide 7:

Instructor Notes:

Identify – You cannot identify issues if you don't know what systems you have. The first step is to create an inventory of all our assets. They you will assess those systems for their primary goal to establish protection strategies. Assets/systems are then prioritized and mitigations applied in a graded approach.

Asset Management Asset & Vulnerability Management	Overview of Exercise	
	<p>Inventory With an inventory, IT/OT systems are identified and described in their interaction, for which appropriate protective measures must be defined in a security concept.</p> <p>Assessment When assessing the inventoried IT/OT systems, the need for protection is determined from an IT security perspective. The protection goals of IT security (C, I, A) must be defined.</p> <p>Prioritization Prioritisation involves determining and prioritising the necessary protection measures based on the defined protection needs.</p> <p>Mitigation The defined protective measures shall be concretely planned and implemented. The effectiveness of the measures shall be reviewed at regular intervals.</p>	
		insidertthreatmitigation.org

Risk Management Exercise



Slide 8:

Instructor Notes:

Establish the culture of the plant which is focused on barely meeting licensing requirements to maximize profits. Corner cutting that saves money without violating the ability to operate is generally ignored.

Scenario Setup
Asset & Vulnerability Management

Overview of
Exercise



Initial Situation:

- Lack of responsibilities in the area of IT security
- Lack of basic information (inventory of IT systems, lack of protection needs assessment, lack of risk management, etc.).

Objectives:

- Assigning roles that are necessary for mastering the scenarios, this shows that in an emergency not only one person decides, but the decisions must always be made in consideration of the current situation.
- Protection needs assessment (CIA) of the existing IT assets
- Targeted trading based on the scenarios

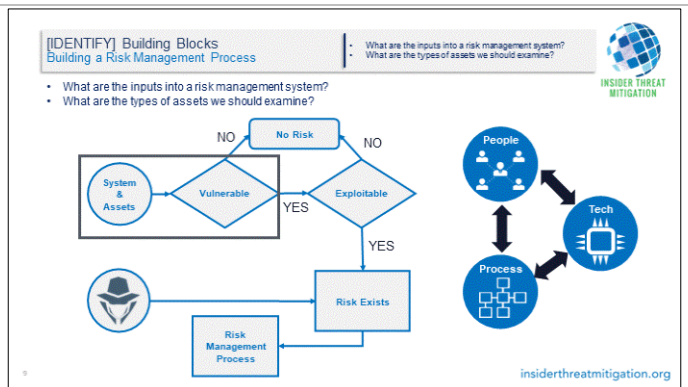
insidertthreatmitigation.org

Slide 9:

Instructor Notes:

Key Objective:

1. In this exercise we are going to look at a facility who has decided to start building a cybersecurity program.
2. This first step is building a Cybersecurity Assessment team. You guys are in charge.
3. In this exercise, we are going to look at identifying the critical digital assets at the facility.
4. The goal of this exercise is understanding why identifying and prioritizing assets is so crucial and important.



Risk Management Exercise

Slide 10:

Instructor Notes:

Share the following story with the class:


1. Your boss has asked you to establish a cybersecurity program.
2. You won't have an unlimited budget. As a result, we need to understand our risks so we can prioritize our actions.

Scenario: Decisions
June 17, 2018

- What are the core functions of a risk management program?
- Who should be involved in developing the program?

The plant director has issued an order for you to establish a cyber **risk management** program at Seaside.

1. What are the data needs to establish a risk management program?
2. What type of personnel is needed to accomplish this task?
3. To expedite the process, is hiring outside contractors appropriate?
4. What systems at the plant should your staff prioritize to complete the quickest?
5. How will you ensure the data is accurate?
6. What type of data about the assets should be accumulated?



"While cybersecurity is important, you must operate within a budget. As such, I need you to evaluate the cyber risks, prioritize, and make decisions that are fiscally responsible."

- Marill Vaxon

insidethreatmitigation.org

Instructions for class.

1. Review the questions.
2. Ask the students to answer the 6 questions through **Mentimeter**.

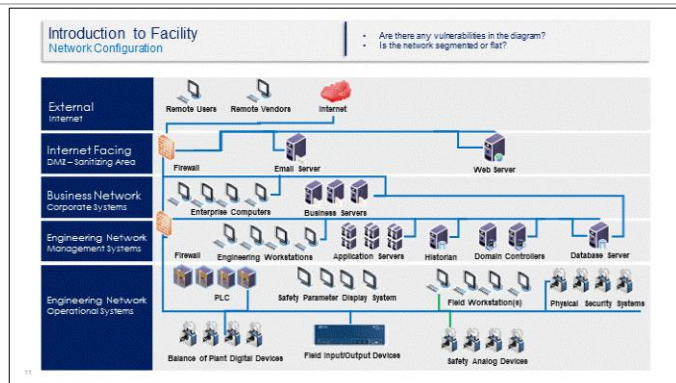
Please note: If trainees are not able to access **Mentimeter**, then administer the questions through a discussion. Start by dividing the trainees into groups. Ask trainees to discuss the questions within their group. Ask for a representative from each group to share their answers to the questions with the larger group when the larger group reconvenes.

3. One thing to highlight on the people, process, and tech front = Outside contractors are frequently hired to help an organization meet objectives that are limited duration but require significant labor.

Slide 11:

Instructor Notes:

1. Review the network diagram with the students.
 - A digital inventory was taken 3 years ago. Any configuration changes that have been made are not physically noted in the documentation
 - The key thing to bring up is that there are basically 2 networks at the facility: business and engineering.
 - There is a demilitarized zone (DMZ) between the outside and the business network.
 - There is a firewall separating the business network and the engineering network.
 - There are no engineering systems allowed to have direct access to the internet.
2. Be sure to state that the safety systems are analog.
3. Tried to set this up like a bus network, however it was challenging in PowerPoint.

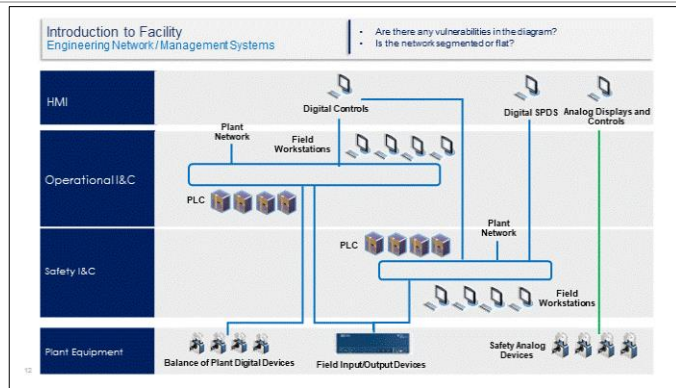


Risk Management Exercise

Slide 12:

Instructor Notes:

- Review the network diagram with the students.
 - A digital inventory was taken 3 years ago. Any configuration changes that have been made are not physically noted in the documentation
 - The key thing to bring up is that there are basically 2 networks at the facility: business and engineering.
 - There is a demilitarized zone (DMZ) between the outside and the business network.
 - There is a firewall separating the business network and the engineering network.
 - There are no engineering systems allowed to have direct access to the internet.
- Be sure to state that the safety systems are analog.
- Tried to set this up like a bus network, however it was challenging in PowerPoint.



Slide 13:

Instructor Notes:

Have the students prioritize which systems are the most crucial or have the most consequence if they failed and have them explain why.

What's the CIA value?

This is set up as a *Mentimeter* activity. Have participants do the activity through Menitmeter.

Prioritization is Key
August 1, 2018

• Be sure to reference the presentation materials
• What are the core systems of a nuclear power plant?

INSIDER THREAT MITIGATION

Categorize each of the 10 systems into either High, Medium or Low Priority.

- Access Control System for the Vital Area at the nuclear facility.
- Reactor Protection System
- Accounts Payable Enterprise System
- Turbine Operator Station
- Historian on the enterprise network
- Engineering / Database Developer Server
- Safety Systems
- Redundant Historians on Engineering Network
- Video Management System of limited area
- Radio Communications for Guard Force

Then, assign a CIA security goal to the items categorized as High or Medium Priority.

NAME: Tom Bombadil
ORGANIZATION: Sesside NUCLEAR POWER PLANT
RESPONSIBILITIES: CYBER SECURITY & INCIDENT RESPONSE
SPECIALTY: NETWORK ARCHITECTURE

Your deputy has requested assistance in prioritizing systems. You both decide to prioritize the systems based on the consequences if the system fails.

You are allowed:

- 2 - High Priority Systems
- 5 - Medium Priority Systems
- 3 - Low Priority Systems

insidethreatmitigation.org

Please note: If trainees are not able to access *Mentimeter*, then administer the questions through a discussion. Start by dividing the trainees into groups. Ask trainees to discuss the questions within their group. Ask for a representative from each group to share their answers to the questions with the larger group when the larger group reconvenes.

Risk Management Exercise

Slide 14:

Instructor Notes:

Walk them through the scenario.

- 09:00 – Tech support is reporting that they have received a ton of calls for a Saturday saying that the network or individual computers are operating really slowly. Next several hours – call frequency of problems increases with all reporting the same issue.
- 1330 – The new server that was being updated failed and crashed. None of the accounts payable division can reach their data on the server.

We don't know enough to make the call whether the plant is safe or not. We need more data.

Scenario Update #4: Accounts Payable is Down
January 26, 2019 [SATURDAY] @ 1715

- Are we safe?
- What information do we need? Is this a cyber incident?



Time Stamp on Events

Time	Description
0900	Several users working over the weekend have called technical support stating that the network is slow.
1330	The Accounts Payable servers that were being upgraded are "timing out" due to little to no bandwidth to complete normal tasks.



"Cyber Security is also about ensuring operational reliability! Get our Accounts Payable servers back into operation ASAP. These servers are bringing in the money and thus there are bringing on your income!"

- Mardil Voron

insidertreatmitigation.org

Slide 15:

Instructor Notes:


Have the students prioritize which systems are the most crucial or have the most consequence if they failed and have them explain why.

What's the CIA value?

Write this out on a whiteboard if possible.

Scenario Update #2: An Urgent Matter
December 14, 2018

- What is a worm?
- What systems are affected?
- What are should your first steps be in response?



What does SAPPHERE do?

- Once the server is infected, it endeavors to spread quickly by sending a similar payload to arbitrary IP addresses on the host network.
- This brings on a denial-of-service condition on its targets.

Mitigations Options

- Long-Term
 - Microsoft has created patch that can be installed
- Short-Term
 - Block SAPPHERE signature at the firewall.
 - Since the worm does not taint any files, an infected machine can be cleaned by just rebooting the machine to a previous configuration.
 - However, it can get re-contaminated if connected with another infected system.


WARNING!!! WARNING

MALWARE NAME: SAPPHERE

MALWARE TYPE: WORM

IMPACT: DENIAL OF SERVICE

SYSTEMS VULNERABLE: ALL WINDOWS SQL SERVERS



Sapphire Computer Worm – AKA "Sapphire" – exploits vulnerabilities in Microsoft SQL Servers.

It has little impact of home or desktop PCs.

It does not infect Linux, Mac, or Unix

insidertreatmitigation.org

Risk Management Exercise

Slide 16:

Instructor Notes:


It is fine if students want to come up with a 4th option.

The main thing is we need them to understand that any decision to do anything has pros and cons and impacts staff/personnel on the cyber team.

This is set up as a *Mentimeter* activity. Have participants do the activity through Mentimeter.

Options Analysis
December 14, 2018

With limited resources, how will you prioritize your action?
Which option is the best decision for Seaside?



Prioritizing Actions

Option 1	Option 2	Option 3	Option 4
<p>[ACTION] – Pull all cyber personnel off current duties and begin testing and deployment of Microsoft Patch</p> <p>[PRO] Quickest option to securing against SAPPHIRE</p> <p>[CON] Delay of inventory</p>	<p>[ACTION] – Block SAPPHIRE at the firewall between external and corporate network</p> <p>[PRO] Quickest way to prevent SAPPHIRE from getting into Seaside. Cyber staff continues inventory</p> <p>[CON] All systems still vulnerable to SAPPHIRE</p>	<p>[ACTION] – Hybrid of options 1 and 2. Requires identifying prioritized systems</p> <p>[PRO] Begins immediate defense against SAPPHIRE and continues inventory process.</p> <p>[CON] Some delay in inventory</p>	<p>[ACTION] – Participant Defined</p> <p>[PRO] – Participant Defined</p> <p>[CON] – Participant Defined</p>

insidertreatmitigation.org

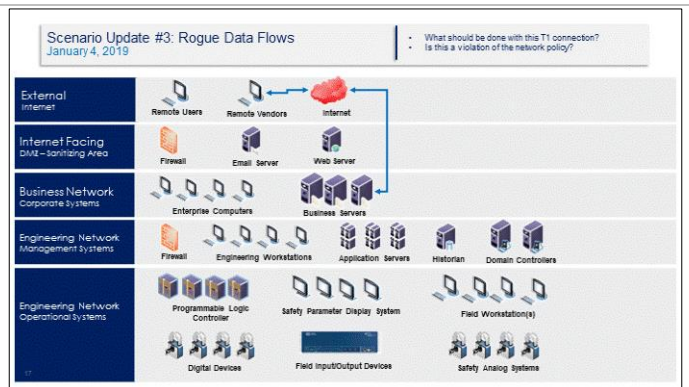
Please note: If trainees are not able to access *Mentimeter*, then administer the questions through a discussion. Start by dividing the trainees into groups. Ask trainees to discuss the questions within their group. Ask for a representative from each group to share their answers to the questions with the larger group when the larger group reconvenes.

Slide 17:

Instructor Notes:

Based on whatever option they chose, tell participants that the team is implementing their orders.

Meanwhile, Initial inventory analysis has identified a rogue T1 connection bridging a vendor working remotely to the business network. The purpose of the connection is to enable the vendor to work remotely on the corporate systems for a vital upgrade for the accounts payable division. The business entities at the plant state that this connection is important to their mission.



- What should be done about this rogue connection? Formalize it and establish it as an authorized conduit or kill it?
- What are the risks?

Risk Management Exercise

Slide 18:

Instructor Notes:


It is fine if students want to come up with a 4th option.

The main thing is we need them to understand that any decision to do anything has pros and cons and impacts staff/personnel on the cyber team.

This is set up as a *Mentimeter* activity. Have participants do the activity through Menimeter.

Options Analysis
January 4, 2019

- Is there a legitimate business need for the connection?
- Which option is the best decision for Seaside?



Prioritizing Actions

Option 1

[ACTION] – Redirect vendor's connection back through firewall

[PRO] Restores policy compliance

[CON] Negative impact to accounts payable and will delay new system implementation by months

Option 2

[ACTION] – Permit the connection during upgrades.

[PRO] Does not impact business operations

[CON] Bypass of firewall continues.

Option 3

[ACTION] – Permit the connection during upgrades but work with vendor to establish cyber rules

[PRO] No impact to business operations

[CON] Small delay in inventory activities

Option 4

[ACTION] – Participant Defined

[PRO] – Participant Defined

[CON] – Participant Defined

insidertreatmitigation.org

Please note: If trainees are not able to access *Mentimeter*, then administer the questions through a discussion. Start by dividing the trainees into groups. Ask trainees to discuss the questions within their group. Ask for a representative from each group to share their answers to the questions with the larger group when the larger group reconvenes.

Slide 19:

Instructor Notes:

Walk participants through the scenario.

- 1500 – Issues are now spreading from the business network to the engineering network.
- 1600 – Control Room operators see their numbers coming in slow.
- 1650 – Safety Parameter Display System (SPDS) Crashes.
- 1713 – Plant Process Computer (PPC) crashes.

We don't know enough to make the call whether the plant is safe or not. We need more data.

Scenario Update #4: SPDS is Down
January 26, 2019 [SATURDAY] @ 1715

- Are we safe?
- What information do we need? Is this a cyber incident?



Time Stamps on Events

Time	Description
1500	Users on the engineering network report their workstations are taking a long time to pull up data.
1600	Control Room Operators notice sluggish data from various systems.
1650	The Safety Parameter Display System (SPDS) – the plant's digital HMI for safety – has crashed.
1713	The Plant Process Computer (PPC) crashed.



"What is happening?!? I thought cybersecurity programs were supposed to protect us from this stuff. Is this a cyber event or a maintenance issue? Bottom line, I need to know, is the plant safe? You have 10 minutes to tell me."

– Mardil Voron

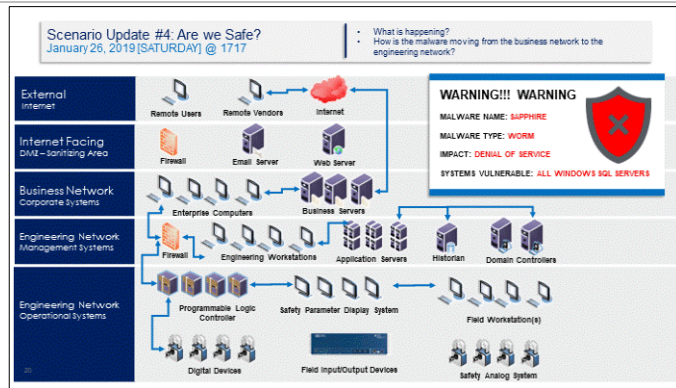
insidertreatmitigation.org

Risk Management Exercise

Slide 20:

Instructor Notes:

If the students chose option 1 to disconnect the T1, tell them that you gave the order, but no one implemented your order [true to life]. Also, the malware spread because the Firewall in the Corporate demilitarized zone (DMZ) had a ruleset for SAPPHIRE. We didn't set that same rule for the firewall between corporate and business because it wasn't connected to the internet. No one thought it would happen.



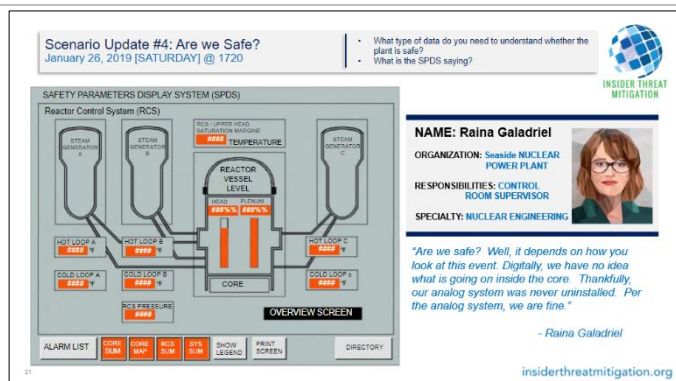
Is the plant safe? The answer should be: we as cyber individuals don't know enough to make that call. Further, it probably isn't our call. Who should we speak to get more data?

Slide 21:

Instructor Notes:

Participants are asked the following 4 questions in the upcoming slides through **Mentimeter**:

- What type of data is communicated by the SPDS?
- Is this important information?
- Is this a critical system?
- What is its CIA Triad value?



Everything is timing on data entry. As a result, we are only getting ### in place of requisite data. Per Raina, the analog system is still up.

Which system numbers do you think are trustworthy?

Please note: If trainees are not able to access **Mentimeter**, then administer the questions through a discussion. Start by dividing the trainees into groups. Ask trainees to discuss the questions within their group. Ask for a representative from each group to share their answers to the questions with the larger group when the larger group reconvenes.

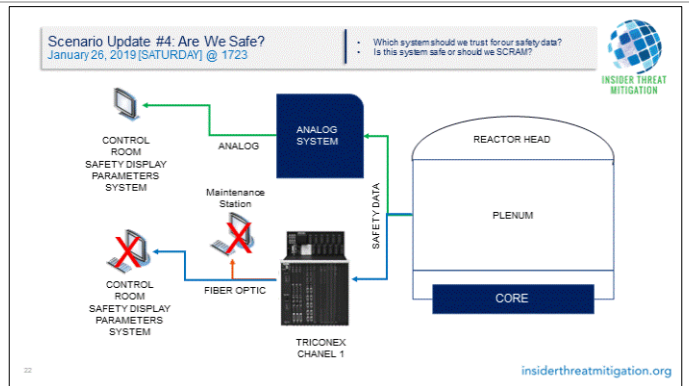
Risk Management Exercise

Slide 22:

Instructor Notes:

The old analog system shows all is functioning normally.

The digital system is not returning any information.



Slide 23:

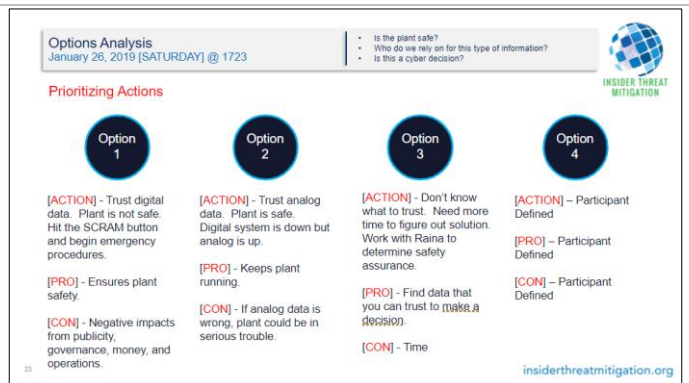
Instructor Notes:

It is fine if students want to come up with a 4th option.

The main thing is we need them to understand this wouldn't really be the cyber team's call. But here is a cyber issue that is causing safety to be questioned.

This is set up as a *Mentimeter* activity. Have participants do the activity through Menitmeter.

Please note: If trainees are not able to access *Mentimeter*, then administer the questions through a discussion. Start by dividing the trainees into groups. Ask trainees to discuss the questions within their group. Ask for a representative from each group to share their answers to the questions with the larger group when the larger group reconvenes.

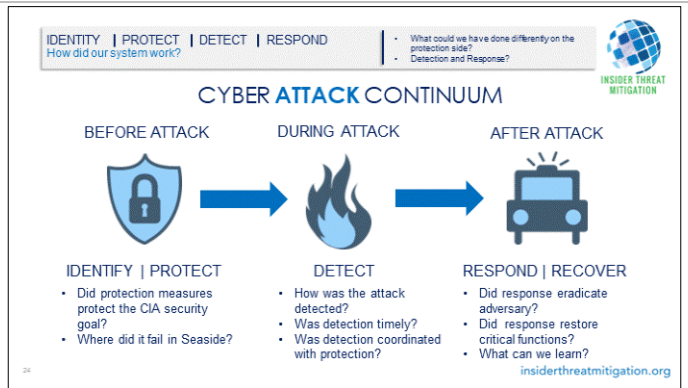


Risk Management Exercise

Slide 24:

Instructor Notes:

What happened between 09:00 a.m. and 4:00 p.m. The issue is that the slow network which was an Indicator of Compromise (IOC) for SAPPHIRE sat with computer support thinking it was a network issue. What can we do on the detection side to speed up analysis between 09:00 a.m. and 4:00 p.m.?



Slide 25:

Instructor Notes:

INSIDER CATEGORIES

<https://vimeo.com/639223567>

Password: pT!u~9V

Seaside Nuclear Power Plant (Davis-Besse Incident): Starts at 10:17



Risk Management Exercise

Slide 26:

Instructor Notes:

There are two options to run this exercise.

1. Small group discussion and/or
2. Mentimeter (or equivalent)

Instructions for class:


Have students review the questions through **Mentimeter**. Please note: If trainees are not able to


access **Mentimeter**, then administer the questions through small group discussion. Start by dividing the trainees into groups. Ask participants to discuss the questions within their group. Ask for a representative from each group to share their answers to the questions with the larger group when the larger group reconvenes.

Lessons Learned
June 17, 2018

1. What is the insider impact?
2. What is impacted?
 - a) Business Continuity (Organization survivability)
 - b) Worldwide Implication
 - c) Safety
3. How could these incidents have been prevented?
 - a) Organizational measures
 - b) Technical measures
4. What was missing in the organization?
 - a) Lack of policy
 - b) Lack of awareness
 - c) Lack of technical measures
5. Timeline Discussion:
 - a) Examples (NotPetya, Fukushima, etc.)

- What are the core functions of a risk management program?
- Who should be involved in developing the program?





"While cybersecurity is important, you must operate within a budget. As such, I need you to evaluate the cyber risks, prioritize, and make decisions that are fiscally responsible."
-Mardil Voron

insidertreatmitigation.org

Slide 27:

Instructor Notes:

Walk them through the real deal.

Walk them through slammer scenario similar to Davis Besse except for Seaside.


<! - - Source Data - ->

The breach did not pose a safety hazard. The troubled plant had been offline since February 2002, when workers discovered a 6-by-5-inch hole in the plant's reactor head. Moreover, the monitoring system, called a Safety Parameter Display System, had a redundant analog backup that was unaffected by the worm. But at least one expert says the case illustrates a growing cybersecurity problem in the nuclear power industry, where interconnection between plant and corporate networks is becoming more common and is permitted by federal safety regulations.

The Davis-Besse plant is operated by FirstEnergy Corp., the Ohio utility company that's become the focus of an investigation into the northeastern U.S. blackout last week.

The incident at the plant is described in an April e-mail to the Nuclear Regulatory Commission (NRC) from FirstEnergy, and in a similarly-worded March safety advisory distributed privately


Davis Besse & Slammer
January 25, 2003 [SATURDAY]




You note in your cover letter that the Davis-Besse plant was "in a safely defueled condition" at the time of infection. This is not reassuring.

- What would be the safety consequences of Slammer had the plant been fueled an operational?
- What impact would the infection have had on the ability to respond to any problems?
- How will you ensure that the plants enforce orders as directed?

- What really happened?
- What can we learn from this attack in a real-world environment?





insidertreatmitigation.org

Risk Management Exercise

throughout the industry over the "Nuclear Network," an information-sharing program run by the Institute of Nuclear Power Operations. The March advisory was issued to "alert the industry to consequences of Internet Worms and Viruses on Plant Computer Systems," according to the text.

The reports paint a sobering picture of cybersecurity at FirstEnergy.

The Slammer worm entered the Davis-Besse plant through a circuitous route. It began by penetrating the unsecured network of an unnamed Davis-Besse contractor, then squirmed through a T1 line bridging that network and Davis-Besse's corporate network. The T1 line, investigators later found, was one of multiple ingresses into Davis-Besse's business network that completely bypassed the plant's firewall, which was programmed to block the port Slammer used to spread.

"This is in essence a backdoor from the Internet to the Corporate internal network that was not monitored by Corporate personnel," reads the April NRC filing by FirstEnergy's Dale Wuokko. "[S]ome people in Corporate's Network Services department were aware of this T1 connection and some were not."

Users noticed slow performance on Davis-Besse's business network at 9:00 a.m., Saturday, January 25th, at the same time Slammer began hitting networks around the world. From the business network, the worm spread to the plant network, where it found purchase in at least one unpatched Windows server. According to the reports, plant computer engineers hadn't installed the patch for the MS-SQL vulnerability that Slammer exploited. In fact, they didn't know there was a patch, which Microsoft released six months before Slammer struck.

Operators Burdened

By 4:00 p.m., power plant workers noticed a slowdown on the plant network. At 4:50 p.m., the congestion created by the worm's scanning crashed the plant's computerized display panel, called the Safety Parameter Display System.

An SPDS monitors the most crucial safety indicators at a plant, like coolant systems, core temperature sensors, and external radiation sensors. Many of those continue to require careful monitoring even while a plant is offline, says one expert. An SPDS outage lasting eight hours or more requires that the NRC be notified.

At 5:13 p.m., another, less critical, monitoring system called the "Plant Process Computer" crashed. Both systems had redundant analog backups that were unaffected by the worm, but, "The unavailability of the SPDS and the PPC was burdensome on the operators," notes the March advisory.

It took four hours and fifty minutes to restore the SPDS, six hours and nine minutes to get the PPC working again.

FirstEnergy declined to elaborate on the incident. The company has become the focus of an investigation into last week's northeastern U.S. blackout. Though the full cause of the blackout has yet to be determined, investigators have reportedly found that it began when an Ohio high-voltage transmission line "tripped" after sagging into a tree. An alarm system that was part of FirstEnergy's Energy Management System failed to warn operators at the company's control center that the line had failed.

Asked if last week's "Blaster" worm might have had a hand in the alarm system failure, just as Slammer disabled the Davis-Besse safety display panel, FirstEnergy spokesman Todd Schneider said, "We're investigating everything right now."

"I have not heard of anything like that," added Schneider. "The alarm system was the only system that was not functioning."

SCADA Issues

The Davis-Besse incident was not Slammer's only point of impact on the electric industry. According to a document released by the North American Electric Reliability Council in June, Slammer downed one utility's critical SCADA network after moving from a corporate network, through a remote computer to a VPN connection to the control center LAN.

A SCADA (Supervisory Control and Data Acquisition) system consists of central host that monitors and controls smaller Remote Terminal Units (RTUs) sprinkled throughout a plant, or in the field at key points in an electrical distribution network. The RTUs, in turn, directly monitor and control various pieces of equipment.

In a second case reported in the same document, a power company's SCADA traffic was blocked because it relied on bandwidth leased from a telecommunications company that fell prey to the worm.

Reports on the effect of last week's Blaster worm on the electric grid, if any, have yet to emerge.

The Slammer attacks came after years of warnings about the vulnerability of power plants and electric distribution systems to cyber attack. A 1997 report by the Clinton White House's National Security Telecommunications Advisory Committee, which conducted a six-month investigation of power grid cybersecurity, described a national system controlled by Byzantine networks riddled with basic security holes, including widespread use of unsecured SCADA systems, and ample connections between control centers and utility company business networks.

"[T]he distinct trend within the industry is to link the systems to access control center data necessary for business purposes," reads the report. "One utility interviewed considered the

business value of access to the data within the control center worth the risk of open connections between the control center and the corporate network."

Future Safety Concerns

An energy sector cybersecurity expert who's reviewed nuclear plant networks, speaking on condition of anonymity, said the trend of linking operations networks with corporate LANs continues unabated within the nuclear energy industry, because of the economic benefits of giving engineers easy access to plant data. An increase in plant efficiency of a couple percentage points "can translate to millions upon millions of dollars per year," says the expert.

He says Slammer's effect on Davis-Besse highlights the dangers of such interconnectivity.

Currently, U.S. nuclear plants generally have digital systems monitoring critical plant operations, but not controlling them, said the expert. But if an intruder could tamper with monitoring systems like Davis-Besse's SPDS, which operators are accustomed to trusting, that could increase the risk of an accident.

Moreover, the industry is moving in the direction of installing digital controls that would allow for remote operation of plant functions, perhaps within a few years, if the NRC approves it. "This is absolutely unacceptable without drastic changes to plant computer networks," says the expert. "If a non-intelligent worm can get in, imagine what an intruder can do."

Jim Davis, director of operations at the Nuclear Energy Institute, an industry association, says those concerns are overblown. "If you break all the connections and allow no data to pass from anywhere to anywhere, you've got great security -- but why'd you put the digital systems in the first place?," says Davis.

Davis says the industry learned from the Davis-Besse incident, but that the breach didn't prove that connections between plant and corporate networks can't be implemented securely. "You can put a well-protected read-only capability on a data stream that provides you reasonable assurance that nobody can come back down that line to the control system," says Davis.

Last year the NEI formed a task force to develop updated cybersecurity management guidelines for the industry. The results -- which will be secret -- are expected within a few months. As part of a research effort earlier this year, the NEI's task force worked with the NRC and a contractor to review cybersecurity at four nuclear power plants. The details of the review are classified as "Safeguards" material, but Davis says the investigation found no serious problems. "There are no issues that generate a public health and safety concern," says Davis.

Risk Management Exercise

"Sometime people get very anxious about digital systems and what you could or couldn't do with digital systems, but in lots of cases you've got switches and valves and little override buttons on this thing and that thing that could cause a component to shut down as quickly as any digital system," Davis says.

Despite the Slammer breach, FirstEnergy was apparently not in violation of NRC's limited, and aging, cybersecurity regulations. For its part, the commission wouldn't comment on the incident. The NRC has faced fierce criticism for not acting sooner to curb far more serious physical safety problems at the plant.

Slide 28:

Instructor Notes:

This slide is optional. Use it if you want to have a discussion on nuclear security culture and how culture can impact all aspects of security. If not hide or delete the slide.

1. Review the bullets below with the students to give them a history of the facility.
2. Ask the questions in the top right section to have the students make an evaluation of the facilities' culture for compliance.
 - Seaside Industrial Solutions is a multi-national radiological / nuclear provider. Their revenue streams range from energy production to building radiological equipment for industrial purposes.
 - Earlier this year at one of their nuclear power plants, a cavity was discovered in the reactor pressure vessel head adjacent to a control rod drive mechanism (CRDM) nozzle penetration
 - Corrosion caused by boric acid leakage from the CRDM nozzle cracks

The slide content is as follows:

- Introduction to Facility**
Seaside Industrial Solutions
- Seaside Power Plant 1**
Pressurized Water Reactor
- History of Safety Issues**
Boric Acid Leakage / Reactor Vessel Degradation

Questions in the top right:

- Does culture at a facility impact security?
- What does this plant's culture tell you?

Logos: INSIDER THREAT MITIGATION and insidertreatmitigation.org

Risk Management Exercise

- Cavity extended through the base metal of the vessel head to the 3/8" stainless steel cladding on the inside of the head.
- Stainless steel cladding was not designed to maintain reactor coolant pressure boundary.
- During an inspection by the competent authority, Seaside leadership was scolded for not taking a proactive approach to this problem.
- Despite the reprimand, the competent authority agreed that performance indicators at the plant were "green" meaning the corrosion did not impact safety or the operability of the plant.
- However, it is felt by personnel throughout the plant that making suggestions to leadership that increase cost are discouraged.
- There is a culture of complacency and lack configuration control.

Slide 29:

Instructor Notes:

Have a round table discussion with participants. Ask participants to share their feedback on the following questions:

- What suggestions do you have for improving any specific lesson?
- Was anything missing from the lesson content that would have improved the learning experience?
- What parts of the training benefited you the most, and why?

