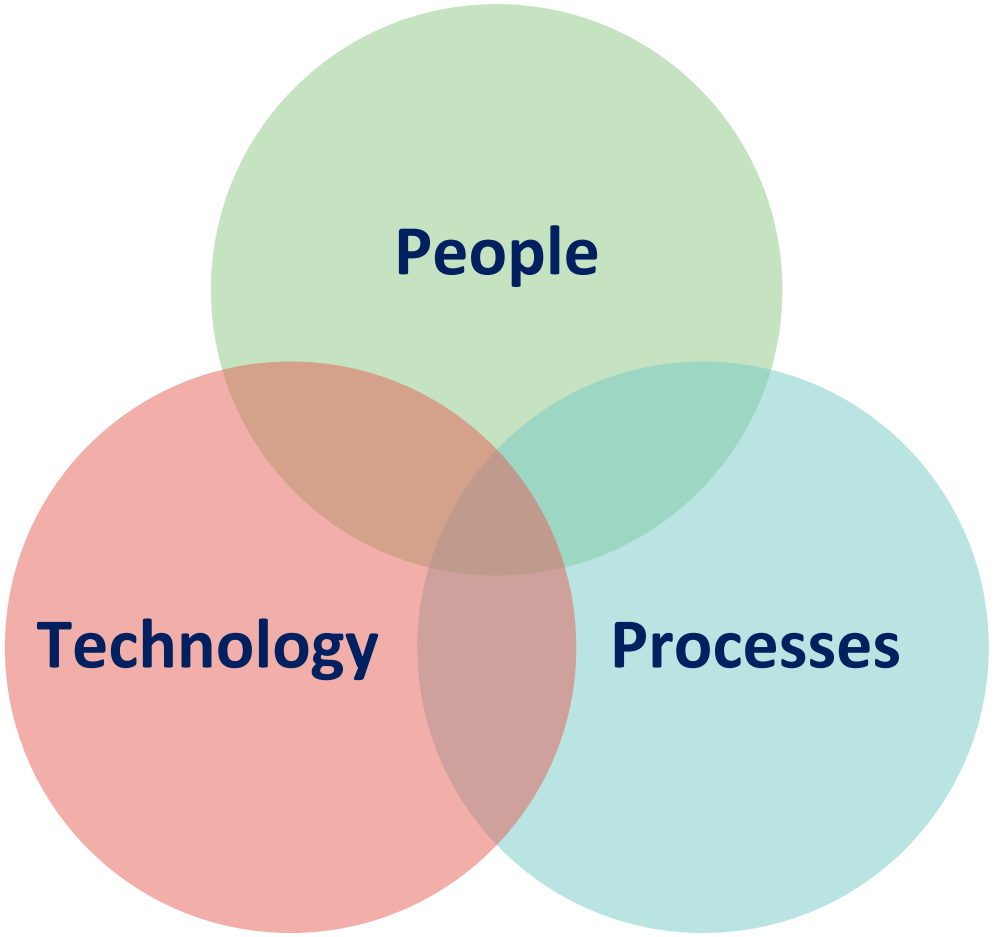
OAECIT

Incident Response Tabletop Exercise

Jacek Szamrej

SEDC

SEDC's Cyber Resilience Initiative (CRI)



Agenda

- **Module 1 - Implementing Incident Management Plan**
- **Module 2 - Tabletop exercise (TTX)**
- **Module 3 - Exercises review, closing discussion**

Module 1
Implementing Incident Management Plan

- Resources for preparing plan
- Types of Information Security Incidents
- Incident response methodology (NIST)
- Incident response phases
- Incident response preparation

Resources for Implementing Incident Management Plan

- Computer Security Incident Handling Guide
  NIST 800-61 Revision 2

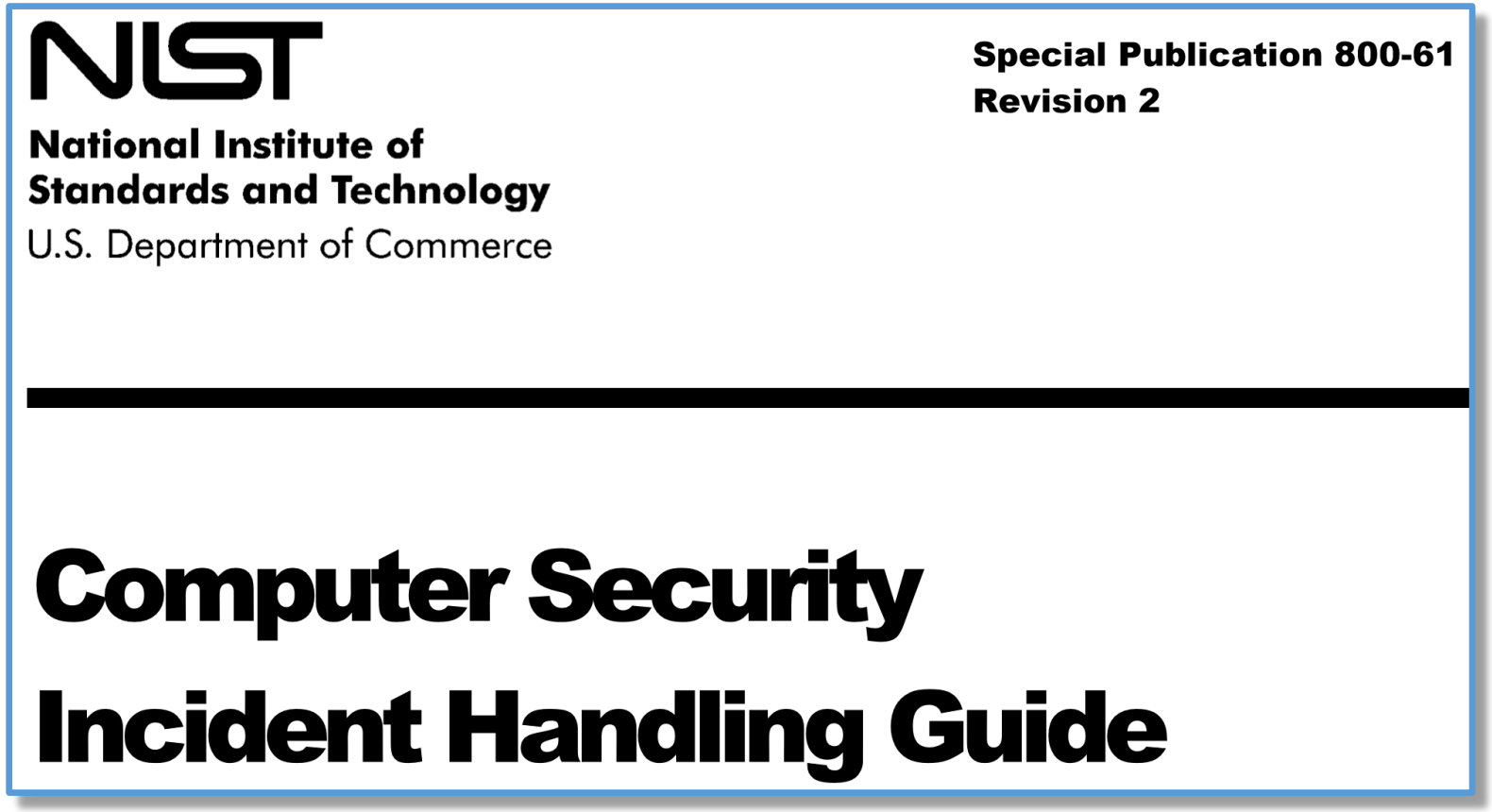
- Information Security Program Library (ISPL SEDC)
  https://www.sedata.com/ispl-v1-1-package/

- NRECA – RC3 Tabletop Exercise (TTX) Toolkit

- APPA - Cyber Incident Playbook
  https://www.publicpower.org/resource/public-power-cyber-incident-response-playbook

Incident Response Methodology

The most popular methodology:



Types of Information Security Incidents

Information Security Incident - a wide variety of events which may impact confidentiality, integrity or availability of information stored by the utility

Examples of information security incidents include:

- Malware or virus detection on workstation or server
- Unauthorized access to computers or facilities by current or former employee
- Data breach and stealing confidential information (i.e., personally identifiable information, credit card information)

Incident Response Phases

I. Preparation

- Adopt policy, procedure and plan
- Define incident response team
- Prepare communication lists and tool

II. Detection and analysis

- Analyze reported suspicious activities
- Determine impact categories

III. Containment, eradication and recovery

- Isolate impacted systems
- Removing elements of the threat from the systems
- Return all systems to original functionality

IV. Post-incident activities

- Perform a detailed investigation of the incident, to devise approaches for prevention of similar incidents in the future

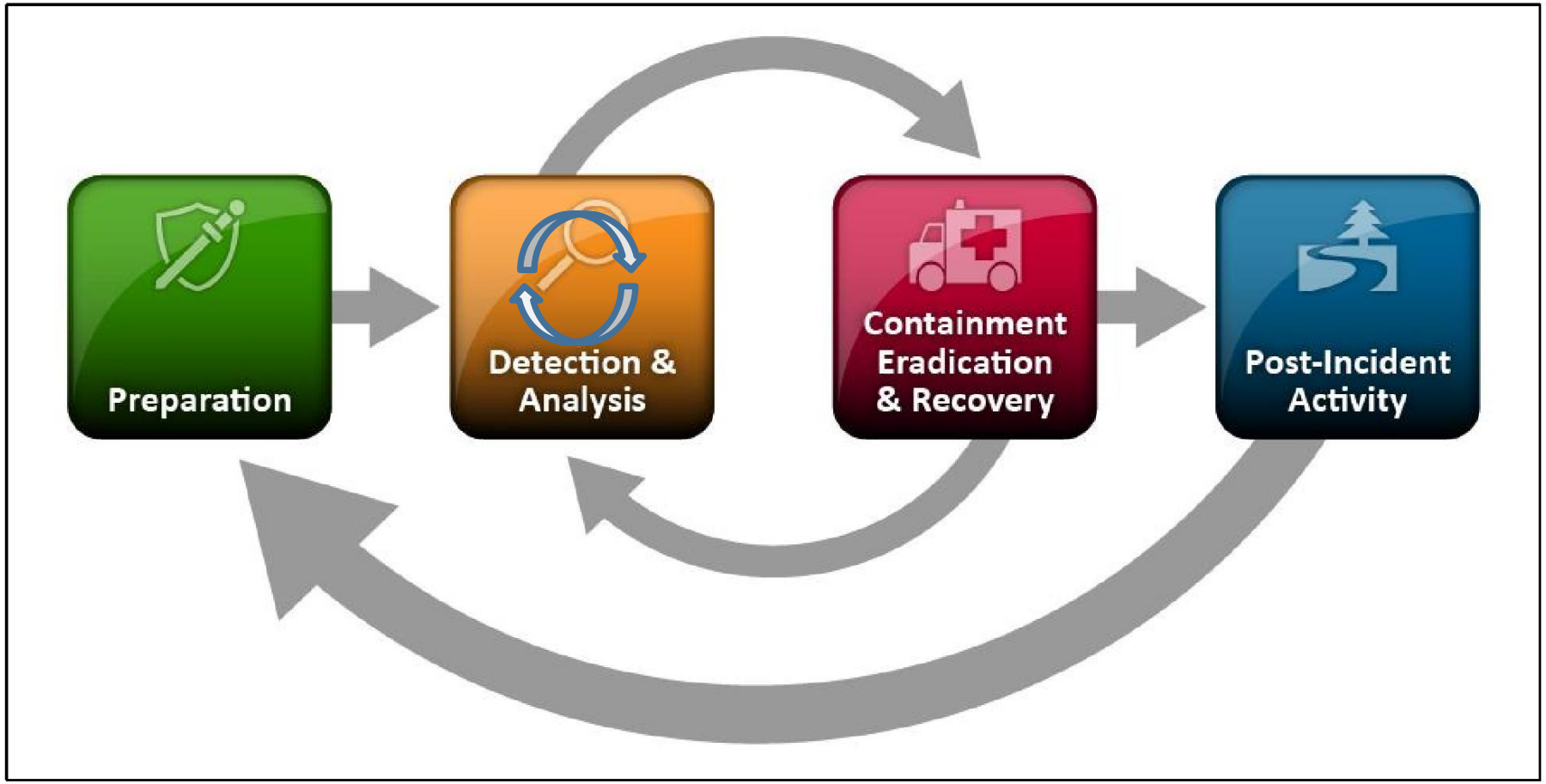


Figure 3-1. Incident Response Life Cycle

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Phase 1: Incident Response Preparation

- Implement policy, plan, procedure guidelines
- Prepare tools
- Conduct Tabletop Exercise (TTX) on annual basis
  - Adjust processes and documentation
  - Maintain and update incident response tools

Processes: ISPL

SEDC's Information Security Program Library is a best practices collection of Cybersecurity Policies, Procedures, & Guidelines

- ***ISPL v1.0*** introduced at UC2016
- ***ISPL v1.1*** distributed publicly Feb. 2017
- ***ISPL v2.0*** available now on The Bridge

ISPL – Incident Response

- Documents examples:
  - Information Security Incident Policy
    - Incident Response Plan
    - Incident Response Form
    - Incident Response Contact List

Information Security Response Plan - Contact List Example

Internal Contact List

Incident Response Function	Primary/Backup	Name	Position	Availability	Phone (desk)	Phone (mobile)	Pager	Phone
IT Incident Handler	Primary	James Brown	IT Manager	24/7	111-111-1111			
IT Incident Handler	Backup	John Smith	IT Admint	24/7	222-222-2222			
Legal Support	Primary							

External Contact List

Type	Institution/Company	Name	Availability	Phone	Email	Other Contact
Law enforcement	Local police station		24/7			
Law enforcement	FBI		24/7			
Internet Provider	SkyLaser		24/7			
Hardware vendor	Dell					
Software vendor	SEDC					
Incident response consultant	SecurityFirst Inc.	James Smith	Business hours			
Insurance company	Federated					
Public Utility Comissioner	Public Utility Comissioner	Randy Smith				

ncident Detection & Analysis

	Description
lent #	
loyee Reporting	
lent Category	• CAT 1 – Unauthorized Access, Compromised machine, Compromised Asset, Data Theft, Espionage etc. • CAT 2 – Denial of Service (DoS/DDoS) • CAT 3 – Malware or Malicious Code • CAT 4 – Reconnaissance or Scans or Probes etc. • CAT 5 – Policy Violations or Improper Usage • CAT 6 – Others or Uncategorized
ct Level	• IL 1 – Low - single computer or system is affected by can be quickly isolated • IL 2 – Medium - several systems are affected, possible impact on operations and possible PII date theft • IL 3 – High - degradation of systems supporting operations, evidence of PII data theft.
cted Systems	
h systems are affected)	
lent Attributes	
(how systems were affected)	
Incident Actors	
(whose actions affected system)	

Incident Handling Checklist

Action	Completed
Detection and Analysis	
Determine whether an incident has occurred	
Analyze the precursors and indicators	
Look for correlating information	
Perform research (e.g., search engines, knowledge base)	
As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery	
Acquire, preserve, secure, and document evidence	
Contain the incident	
Eradicate the incident	
Identify and mitigate all vulnerabilities that were exploited	
Remove malware, inappropriate materials, and other components	
If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
Recover from the incident	
Return affected systems to an operationally ready state	
Confirm that the affected systems are functioning normally	
If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity	
Create a follow-up report	
Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Source: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

IR Plan Implementation Steps

1. Adopt Incident Management Policy
2. Adopt Incident Response Plan
   A. Establish Response Team and define roles
   B. Define communication guidelines
      - Internal and external contact list (call tree)
      - External communication requirements
   C. Define detection capabilities (in-house or contractor)
   D. Define analysis capabilities (in-house or contractor)
   E. Define tools for incident response (disk images, etc.)
3. Conduct tabletop exercise

IR: Team and Roles

Example:

Role	Description	Primary Person	Backup Person
Incident Manager	Analyze event information and estimate incident impact. Coordinate Team effort in all phases of response.	IT Manager	IT Administrator
Incident Response Team Member	Reports to Incident Manager	IT Administrator, GIS Technician,	IT Administrator, GIS Technician, E&O technician
CEO	Provide management support		
Legal Counsel	Provide legal support		
External Communication	Communicate with BOD, regulators, media	Public Relations or Marketing	
Logistics	Provide logistic support for longer incidents	Clerical or administrative employees	

IR: Documenting All Activities

- ISPL includes templates:
  - Incident Management Policy
  - Incident Response Plan
  - Incident Response Form
    - Incident Handling Checklist
- Following the processes, collecting data and documenting
  - Create standardized reports rather than random formats

Information Security Incident Response Form

11 Incident Detection & Analysis

Item	Description
Incident #	
Date	
Incident Indicators (employee report, SIEM, IDS or others)	
Determine whether an incident has occurred	
Affected Systems (which systems are affected)	
Attack Vectors (how systems were affected)	(External/Removable Media, Attrition, Web, Email, Impersonation, Improper Usage, Equipment Loss or Others)
Incident Actors (whose actions affected system)	
Functional Impact (how significant is the system impact)	(None, Low, Medium, High)
Information Impact	(None, Privacy Breach, Proprietary Breach, Integrity Loss)
Recoverability Effort	(Regular, Supplemented, Extended, Not Recoverable)
Internal Notification (list internal notifications that	

Phase 2: Incident Detection

Two categories of signs of incidents: precursors and indicators

- **Precursor -** an incident that may occur in the future, **Indication of Attack (IOA)**
  - Email from hacktivist group saying that they are preparing attack
  - Information about new malware which use vulnerability also presented in our system
  - Indication from system log about logging attempts from foreign IP address
- **Indicator -** an incident may have occurred or may be occurring now**, Indication of Compromise (IOC)**
  - Alert from antivirus software
  - Alert from IDS system showing Command and Control (CC) communication

Incident Detection - Example

SEDC MSS has detected suspicious network activity:

- **Workstation ENG2015A made several DNS requests:**
  - **pzvtyiahfyayvew.net**
  - **ichnzsgfoaxnjo.net**
  - **ordixfydmfppfvqj.net**
  - **sqvobgvnklavmucqe.net**
  - **ncsiifdfdvgsk.net**
- **MSS IDS interpreted this as a possible TROJAN Zeus GameOver DGA communication**

- **What we do next?**

Incident Detection - Example

Information Security Incident Response Form

1 Incident Detection & Analysis

Item	Description
Incident # **57**	
Date **04/15/2017**	
Incident Indicators (employee report, SIEM, IDS or others)	**SEDC MSS – Trojan Zeus GameOver – DNS request**
Determine whether an incident has occurred	
Affected Systems (which systems are affected)\	
Attack Vectors (how systems were affected)	(External/Removable Media, Attrition, Web, Email, Impersonation, Improper Usage, Equipment Loss or Others)
Incident Actors	

Incident Analysis

- Possible to have some (or many) false positive indicators, which should be also documented
- Even with correct indicators, may not be security issue (i.e., disk failed on the server)
- May require event correlation between many sources
- Really need SIEM or other tools for correlating between information collected from different cybersecurity products

Incident Analysis - Example

- **Let’s check computer ENG2015A**
- **We use Malwarebytes and we found it!!!**

Incident Analysis - Example

Information Security Incident Response Form

1 Incident Detection & Analysis

Item	Description
Incident # **57**	
Date **04/15/2017**	
Incident Indicators (employee report, SIEM, IDS or others)	**SEDC MSS – Trojan Zeus GameOver – DNS request**
Determine whether an incident has occurred	**Yes**
Affected Systems (which systems are affected)	**ENG2015A**
Attack Vectors (how systems were affected)	(External/Removable Media, Attrition, Web, Email, Impersonation, Improper Usage, Equipment Loss or Others)
Incident Actors	

IR: Functional Impact Categories

Category	Definition	Examples
None	No effect to the organization's ability to provide all services to all users	• Single computer affected by virus
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency	• Two workstations affected by ransomware • Several laptops were affected by virus
Medium	Organization has lost the ability to provide a critical service to a subset of system users	• GIS server affected by exploit, maps not updated • AVL affected by DDoS, vehicle locations not updated
High	Organization is no longer able to provide some critical services to any users	• OMS and AMI affected by APT • Firewall firmware was changed affecting communication with the Internet

IR: Information Impact Categories

Category	Definition	Examples
None	No information was exfiltrated, changed, deleted, or otherwise compromised	• Single computer affected by virus
Privacy Breach	Sensitive personally identifiable information (PII) of Members or employees was accessed or exfiltrated	• Employees (PII) data was extracted and found on dark web
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated	• Diagrams of fiber communication and substations was accessed from IP address in Iran
Integrity Loss	Sensitive or proprietary information was changed or deleted	• Documentation with distribution lines protection settings were changed

IR: Recoverability Effort Categories

Category	Definition	Examples
Regular	Time to recovery is predictable with existing resources, and will meet RTO	• Affected workstations will be restored in 4 hours
Supplemented	Time to recovery is predictable with additional resources and, will exceed RTO	• Restoring systems affected by ransomware require systems and application images
Extended	Time to recovery is unpredictable; additional resources and outside help are needed	• Repeated DDoS require ISP support and changing DNS pointers • Software vendor assistance is required in restoring OMS
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation	• Member's PII information published by hackers

Incident Analysis - Example

Item	Description
Incident # 57	
Date 04/15/2017	
Incident Indicators (employee report, SIEM, IDS or others)	**SEDC MSS – Trojan Zeus GameOver – DNS request**
Determine whether an incident has occurred	**Yes**
Affected Systems (which systems are affected)	**ENG2015A**
Attack Vectors (how systems were affected)	(External/Removable Media, Attrition, Web, Email, Impersonation, Improper Usage, Equipment Loss or Others)
Incident Actors (whose actions affected system)	
Functional Impact (how significant is the system impact)	(**None**, Low, Medium, High)
Information Impact	(**None**, Privacy Breach, Proprietary Breach, Integrity Loss)
Recoverability Effort	(**Regular**, Supplemented, Extended, Not Recoverable)
Internal Notification	**No**
External Notification	**No**
Other information	**MD5 and Trojan Zeus GameOver description was reviewed**

Phase 3: Incident Containment, Eradication & Recovery

Factors to consider for containment actions:

- Potential damage to and theft of resources
- Need for evidence preservation
- Requirements for service availability
- Time and resources needed for containment
- Effectiveness (e.g., partial containment, full containment)
- Duration of the solution (e.g., emergency solution in four hours, temporary workaround to be removed in two weeks, permanent solution)

Incident Containment, Eradication & Recovery - Example

- ENG2015A was disconnected from network
- Trojan was removed
- Other computers checked, ENG2015A was the only affected computer
- Reviewed file system to determine when system was compromised
- User reported that he received an email and clicked on the link
- Re-imaged ENG2015A
- Installed applications on ENG2015A, verified suspicious email was delete/purged

Incident Containment, Eradication & Recovery - Example

2 Containment, Eradication and Recovery

2.1 Containment

Item	Description
Incident Status	Containment completed
Integrity Assessment	
Containment Measures	Scanned other computers with Malwarebytes

2.2 Eradication

Item	Description
Incident Status	Eradication completed
Vulnerability Assessment	Conducted additional scans on other workstations
Eradication Measures	Computer ENG2015A re-imaged

2.3 Recovery

Item	Description
Incident Status	Recovery completed
Recovery Plan	ENG2015A re-imaged and applications re-installed
Recovery Process Documentation	Assets inventory updated
Validation	MSS is not reporting any new indications

Phase 4: Post-incident Activities

Follow-up is important after each incident:

- Exactly what happened, what was the timetable?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed earlier?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently next time?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?

Post-incident Activities - Example

3 Post Incident Analysis & Forensic

Item	Description
Collected Forensic Data	MD5 hash, description provided by Malwarebytes Information provided by SEDC MSS
Evaluation Process	Analyzed infection process thru email
Lessons Learned	ENG2015A was infected by malware downloaded when user clicked on link delivered by phishing email
Action Items	- Another phishing simulation campaign is needed to increase users awareness - Check if other AV programs could stop this infection - Check that IDS was working correctly

Incident Handling Checklist

Action		Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the Incident Manager believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Reference: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Module 2
Tabletop Exercise (TTX)

Tabletop Exercise (TTX)

Goals:

- Prepare participants to conduct TTX in their environment
- Simulate steps for each incident response phase
- Learn from your peers to take back to your utility

TTX Structure

- **Introduction to Bison Valley Electric Cooperative**
  - Distribution electric utility with 55,000 members
  - Has an AMI system
- **Injects and Responses**
  - A Facilitator for every 2 tables, 2 Technical experts roaming (raise flag)
  - One Scribe and one Speaker selected (volunteered) per table
  - Several injects (describing incident events), introduced one at a time
  - Table discussions on what actions should be taken in response to inject
  - Short description of responses will be written on flipchart
  - After discussing each inject, 2 tables will present their responses
- **Hot Wash**
  - At the end, we will debrief following Hot Wash format

TTX Guidelines and Ground Rules

- Everyone speaks
- Respect the speaker
- Titles left outside the door
- No idea is dumb
- Avoid “Bar Discussions”
- Start on Time / End on Time

Bison Valley Electric Coop

TTX : Inject 1

6/3/2019 2PM

- BVEC IT noticed huge amount of events/alarms on BVEC firewall.
  Source addresses were showing many different countries including US.

- Several members notified BVEC that www.bvec.net website is not available.

- Internet Service Provider notified BVEC about Distributed Denial of Service attack targeting BVEC servers.
  Attack last for 2.5 hours with 45Gbps at the peak.

- BVEC IT found that 7 external mailboxes (OWA) were locked due to unsuccessful login attempts.

TTX : Inject 2

6/4/2019 10PM

- Several BVEC employees received email from organization or person called ShadowHamsters.

- They are requesting to pay 200 Bitcoins in 48 hours, otherwise BVEC system will be shut down, but they are not describing any details.

TTX : Inject 3

6/5/2019 7AM

- BVEC IT Department received several calls from other BVEC employees who are not able to login into BVEC network. IT Department quickly found that BVEC Active Directory system has been compromised and even system administrators are not able to login into workstations, servers, domain controllers.

6/5/2019 9AM

- FedEx courier delivered envelope with ransom request from ShadowHamsters and details on how to pay ransom.

TTX : Inject 4

6/5/2019 11AM

- BVEC IT Department restored Active Directory from backup and everything return to normal. After about one hour employees were not able to login into BVEC network again.

Incident Handling Checklist

Action		Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the Incident Manager believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Reference: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Module 3

HOT WASH

1. Top 3 Takeaways
2. Top 3 Next Steps
3. Feedback

Thanks!

jaceks@sedata.com