Poll Question 1

Does your organization have an incident response plan?

Poll Question 2

Has your organization had a cybersecurity incident within the past year?
Scenario 1

User notices strange behavior on AIS 

System is infected with a virus. User doesn't know signs / symptoms 

Significant network outage while cleaned 

Virus is able to spread to other systems 

Scenario 2

User notices strange behavior on AIS 

User has been trained on the incident response plan 

Minimal business impact 

CSIRT is activated and follows process 

Purpose of Incident Response

✓ Protects networks and assets 

✓ Reduces downtime and recovery time 

✓ Prevents future incidents
**Events**

Event: Any observable occurrence in a system or network that may affect performance

- System reboots
- Crashes
- Network slowdown
- Certain types of input

An event may be an indication that an incident is occurring!
Incidents

Incident: An occurrence that threatens or negatively impacts the confidentiality, integrity or availability of a system.

- Unauthorized access
- Denial of service
- Malware infection
- Data spillage

Incident Categories

CAT 1: Unauthorized Access
CAT 2: Denial of Service
CAT 3: Malicious Code
CAT 4: Improper Usage
CAT 5: Scans / Probes / Attempted Access
CAT 6: Unconfirmed or Uncategorized

https://www.us-cert.gov/government-users/reporting-requirements#tax

Incident Notification

Containment difficulty
1. Develop a plan
2. Make sure employees are aware of their responsibilities
3. Test it regularly (at least annually)
4. goto 1

An Incident Response Plan:

- Provides a road map for incident response
- Describes the structure / organization of the incident response capability
- Provides a high-level approach
- Is tailored to the organization
- Defines reportable incidents

Incident Response Plan (cont)

- Provides metrics for measuring the capability within the organization
- Defines the resources and management roles
- Reviewed and approved by leadership
- Is integrated across sections/divisions/elements
Incident Response Process

1. Report
2. Contain
3. Preserve evidence
4. Recover

- Assess
- Determine severity
- Notify external agencies
- Assess damage / cost

Document steps and findings

Review and update training / policies

Data Breaches

- Get leadership support
- Develop specific guides for likely scenarios
- Define process for major decisions
- Provide to all users as appropriate

- Identify Single Points of Failure
- Train and exercise
- Review and update

Lessons Learned

- Get leadership support
- Develop specific guides for likely scenarios
- Define process for major decisions
- Provide to all users as appropriate

- Identify Single Points of Failure
- Train and exercise
- Review and update
Summary

- Defining events and incidents
- Incident response process and plans
- When and why to develop an incident response capability
- Lessons learned
- Toolkit