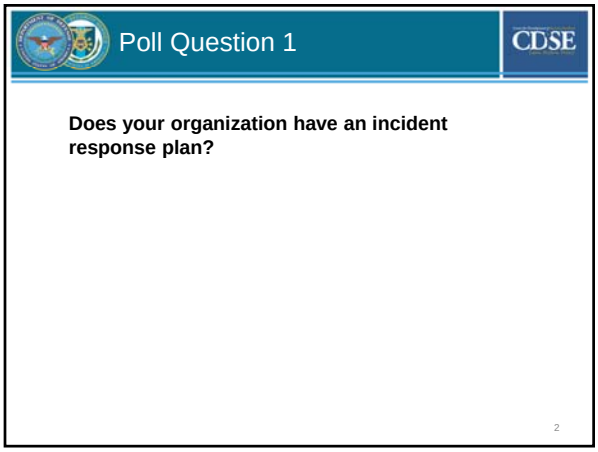
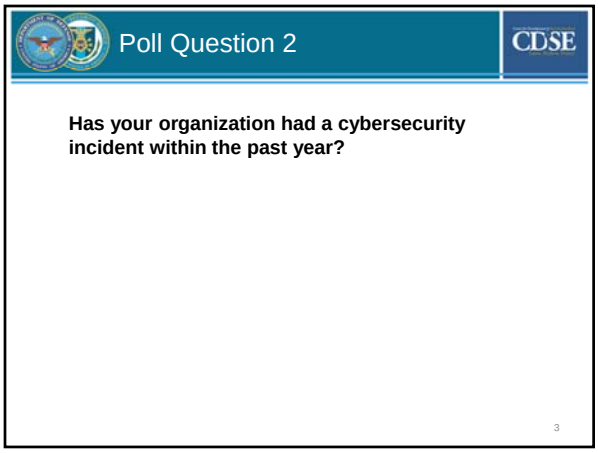

Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
SECURITY SERVICE
Incident Response

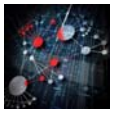

Poll Question 1
CDSE
Does your organization have an incident response plan?
2


Poll Question 2
CDSE
Has your organization had a cybersecurity incident within the past year?
3

Scenario 1

User notices strange behavior on AIS

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



Virus is able to spread to other systems

Significant network outage while cleaned

4

Scenario 2

User notices strange behavior on AIS

User has been trained on the incident response plan

CSIRT is activated and follows process

Minimal business impact

5

Purpose of Incident Response

- ✓ Protects networks and assets
- ✓ Reduces downtime and recovery time
- ✓ Prevents future incidents

6

Parallel to Physical Security

Events, Alerts, and Incidents

Event: a change to the normal behavior or environment. Updates and installations are events.

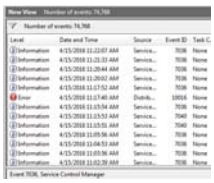
Alert: a notification to responsible parties that an event has occurred.

Incident: a malicious event that can lead to business disruption. For example, a breach or hack.

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!

9

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

10

Incident Categories

CAT 1: Unauthorized Access

CAT 2: Denial of Service

CAT 3: Malicious Code

CAT 4: Improper Usage

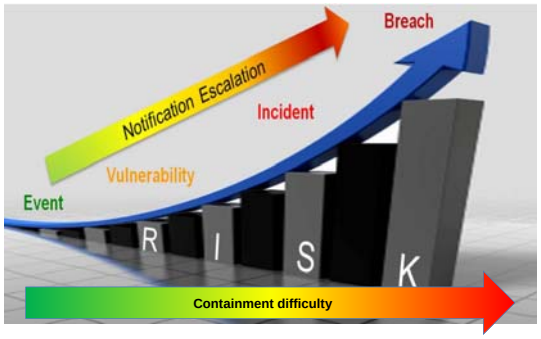
CAT 5: Scans / Probes / Attempted Access

CAT 6: Unconfirmed or Uncategorized

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

11

Incident Notification



Incident Response

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

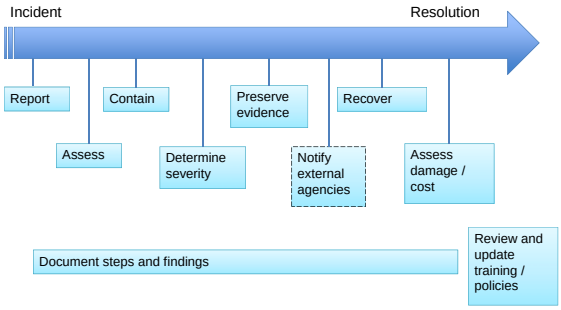
An Incident Response Plan:

- 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)

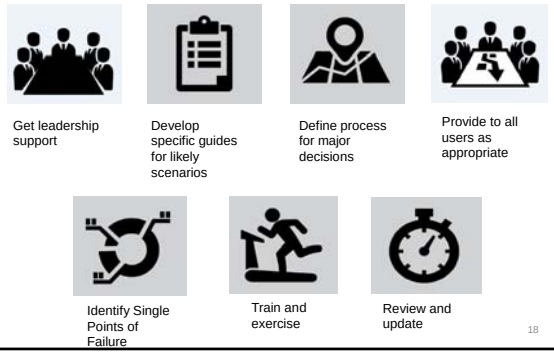
- Provides metrics for measuring the capability within the organization
- Defines the resources and management roles
- Reviewed and approved by leadership
- Is integrated across sections/divisions/elements

Incident Response Process



Data Breaches

Lessons Learned



Summary

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

19

20