



**Incident Response**

---

---

---

---

---

---

---

---

 Poll Question 1 

**Does your organization have an incident response plan?**

2

---

---

---

---

---

---

---

---

 Poll Question 2 

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

3

---

---

---

---

---

---

---

---

**Scenario 1** CDSE

User notices strange behavior on AIS

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

VIRUS DETECTED

Virus is able to spread to other systems

Significant network outage while cleaned

Sorry WE'RE CLOSED

4

---

---

---

---

---

---

---

---

**Scenario 2** CDSE

User notices strange behavior on AIS

User has been trained on the incident response plan

Emergency!!!

CSIRT is activated and follows process

Minimal business impact

Open for Business

5

---

---

---

---

---

---

---

---

**Purpose of Incident Response** CDSE

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

6

---

---

---

---

---

---

---

---

**Parallel to Physical Security** CDSE

---

---

---

---

---

---

---

---

---

---

**Events, Alerts, and Incidents** CDSE

**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** CDSE

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

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

Level	Date and Time	Source	Event ID	Task C.
Information	4/25/2016 11:28:07 AM	Service...	7038	Name
Information	4/25/2016 11:28:10 AM	Service...	7038	Name
Information	4/25/2016 11:28:14 AM	Service...	7038	Name
Information	4/25/2016 11:28:17 AM	Service...	7038	Name
Error	4/25/2016 11:57:40 AM	Event...	10018	Name
Information	4/25/2016 11:57:50 AM	Service...	7038	Name
Information	4/25/2016 11:57:51 AM	Service...	7040	Name
Information	4/25/2016 11:57:51 AM	Service...	7040	Name
Information	4/25/2016 11:57:56 AM	Service...	7038	Name
Information	4/25/2016 11:58:03 AM	Service...	7038	Name
Information	4/25/2016 11:58:06 AM	Service...	7038	Name
Information	4/25/2016 11:58:20 AM	Service...	7038	Name

Event Viewer, Service Control Manager

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

---

---

---

---

---

---

---

---

---

---

 **Incidents** CDSE

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** CDSE

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

---

---

---

---

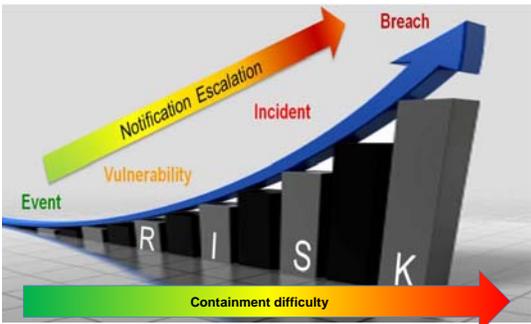
---

---

---

---

 **Incident Notification** CDSE



---

---

---

---

---

---

---

---

 Incident Response CDSE

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: CDSE

- 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) CDSE

- 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

---

---

---

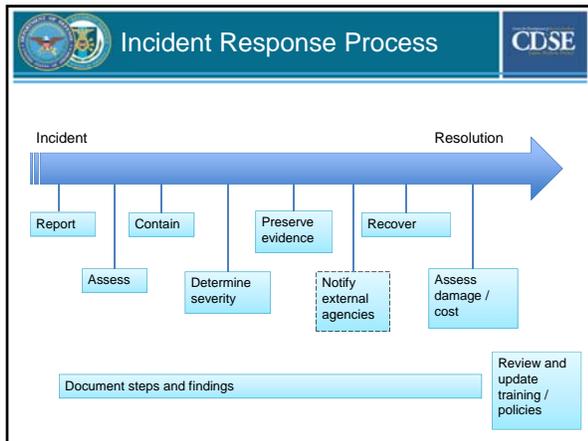
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

---

---

**Data Breaches** (CDSE)

**TJX Data Breach Exposed 94M Credit Cards**  
By Dan 2017-11-09 02:27  
 Still no word on whether the \$2.5 billion in stolen credit cards is being returned to the retailer, TJX Cos., to recover their losses. But those losses keep growing. [More »](#)

**CareFirst BlueCross BlueShield**  
 1.1 million records compromised

**DATA BREACH INVESTIGATION**  
 "Protecting our customer information is something we take extremely seriously, and we're glad to see our partner working to protect their data."

Logos for **Target** and **CareFirst BlueCross BlueShield** are also visible.

---

---

---

---

---

---

---

---

---

---

---

---

**Lessons Learned** (CDSE)

- Get leadership support** (Icon: Group of people)
- Develop specific guides for likely scenarios** (Icon: Clipboard)
- Define process for major decisions** (Icon: Location pin)
- Provide to all users as appropriate** (Icon: People with arrows)
- Identify Single Points of Failure** (Icon: Gear with red X)
- Train and exercise** (Icon: Person running)
- Review and update** (Icon: Stopwatch)

18

---

---

---

---

---

---

---

---

---

---

---

---

 **Summary** CDSE

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



The screenshot shows a webpage titled "Cybersecurity Toolkit" with a navigation menu and a grid of icons. A blue arrow points to the "Incident Response" icon, which features a yellow warning triangle with an exclamation mark.

19

---

---

---

---

---

---

---

---

 **CDSE**



A close-up photograph of several computer keyboard keys. The central focus is a white key with a blue question mark. Other keys with letters 'P', 'F', and 'D' are visible around it.

20

---

---

---

---

---

---

---

---