JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Security Incidents

CYBER INCIDENT RESPONSE

Cyber Incidents Will Happen

- No matter what your organization does to prevent a cyber incident…
  eventually one will happen to you

- How will you respond?

- How will you react?

- How will you recover?

You Must Plan Your Response

- Plan in advance your response
- Allows you to have a coordinated and methodical response
- Prior planning minimizes the damage and decreases your response time

Security Events and Incidents

- Event
  - Any observable occurrence in a system or network
- Adverse Event
  - Any event that has negative consequences
- Incidents
  - An imminent threat of violation, or a violation itself, of a security policy, acceptable use policy, or standard security practice

Security Events and Incidents

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Not every event is an incident,

but every incident contains

at least one event

Computer Security Incident Response Team (CSIRT)

Team of professionals responsible for handling a security incident within an organization by using a standardized procedures

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE