JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Incident Classification

CYBER INCIDENT RESPONSE

Incident Classification

- All incidents should be classified by their threat and severity
- Allows comparison of current incident with past and future ones
- Aids in personnel's understanding of the incident being worked on

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Classifying Threats

- External or Removable Media
  - Attack executed by removable media or peripheral
- Attrition
  - Attack employing brute-force to compromise, deny, or degrade services, systems, or networks
- Web
  - Attack executed from web-based application or site
- Email
  - Attack executed from email or attachment

Classifying Threats

- Impersonation
  - Attack that replaces something benign with something malicious (spoofing, SQL inject, etc)
- Improper Usage
  - Violation of organization’s AUP (P2P program)
- Loss or Theft of Equipment
  - Computing device or media is lost or stolen
- Unknown
  - Attack that comes from an unknown origin

Classifying Threats

- Other
  - Attack that comes from a known origin, but doesn't fit into the other categories
- Advanced Persistent Threat (APT)
  - Not a category under NIST, but prevalent today
  - Often funded by nation stations, organized crime, or other sources
  - Highly skilled and sophisticated attackers
  - Often takes advantage of zero-day vulnerabilities

Classifying Severity: Scope of Impact

- Degree of impairment that an incident causes an organization and the effort to recover from the incident
- Functional impact
    - Degree of impairment to an organization
- Economic impact
    - Amount of financial loss to an organization
- Recoverability impact
    - Amount of time lost by an organization

Classifying Severity: Scope of Impact

- Functional impact
  - Degree of impairment to an organization

Category	Definition
None	None; No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

NIST 800-61(Table 3-2)

Classifying Severity: Scope of Impact

- Economic impact
  - Amount of financial loss to an organization

Category	Definition
None	None; No financial loss experienced by the organization
Low	Minimal effect; the organization expects to experience a loss of $25,000 or less
Medium	Organization expects to experience a loss of $25,000 to $999,999
High	Organization expects to experience a loss of $1,000,000 or more

Not covered by NIST 800-61

Classifying Severity: Scope of Impact

- Recoverability impact
  - Amount of time lost by an organization

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (such as sensitive data exfiltrated and posted publically); launch investigation

NIST 800-61 (Table 3-4)

Classifying Severity: Types of Data

- The type of data involved in the incident also affects the classification of severity

- Information impact
  - Degree of information compromise during incident

Classifying Severity: Types of Data

- Information impact (Government)
  - Degree of information compromise during incident

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive PII of taxpayers, employees, beneficiaries, etc was access or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

NIST 800-61 (Table 3-3)

Classifying Severity: Types of Data

- Information impact (Private Company)
  - Degree of information compromise during incident

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Regulated Information Breach	Information regulated by an external compliance obligation was accessed or exfiltrated (GLBA, SOX, HIPAA, etc)
Intellectual Proprietary Breach	Sensitive proprietary information was accessed or exfiltrated
Confidential Proprietary Breach	Corporate confidential information was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Not covered by NIST 800-61