SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #19

Incident Response and Management

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # # 19

Protect the organization’s information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker’s presence, and restoring the integrity of the network and systems.

CIS Top 20 Critical Security Controls

In short, a well-crafted IR plan will help your organization perform at its best by preparing for the worst.

CIS Top 20 Critical Security Controls

Why Is This Control Critical?

CIS Controls™

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

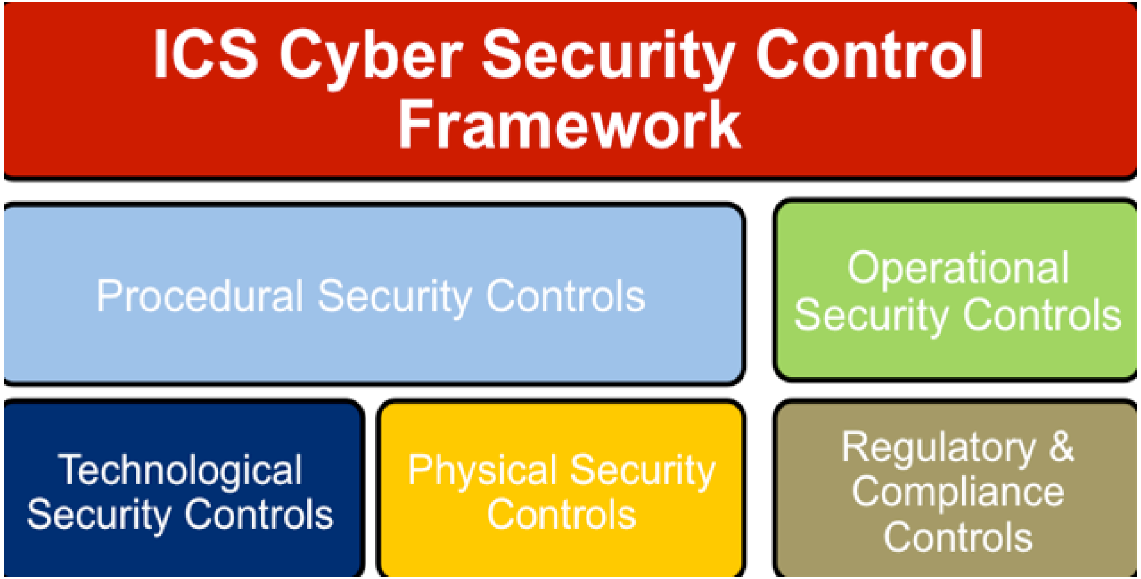
17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Understanding the Control types



ICS Cyber Security Control Framework

Procedural Security Controls

Operational Security Controls

Technological Security Controls

Physical Security Controls

Regulatory & Compliance Controls

CIS Top 20 Critical Security Controls

If your company suffers a data breach or a phishing, ransomware, or DDoS attack, are you prepared to respond?

CIS Top 20 Critical Security Controls

An incident response plan can speed forensic analysis, minimizing the duration of a security incident and shortening recovery time

CIS Top 20 Critical Security Controls

Key sections to include in an incident response plan

- Policy, definition and scope.
- A diagrammatic representation of the process
- Incident reporting
- First responders: contact details, roles and responsibilities
- Incident assessment
- Incident countermeasures
- Identifying corrective actions
- Monitoring corrective

CIS Top 20 Critical Security Controls

- Different types of security attacks merit different response strategies. It is important that your incident response plan details separate procedures (runbooks) for various type of incidents, such as:
  - Malware/ransomware outbreaks
  - Phishing attacks
  - Data loss/theft
  - DDoS
  - Unauthorized access
  - Privilege escalation
  - Improper use

CIS Top 20 Critical Security Controls

Key considerations for incident response planning

- Senior management support is essential
- Keep the plan simple.
- Communicate regularly on the incident status
- Review and test
- Be flexible

CIS Top 20 Critical Security Controls

Components of an incident response plan

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons learned

CIS Top 20 Critical Security Controls

BUILD YOUR IR TEAM

CIS Top 20 Critical Security Controls

TEST YOUR PLAN

CIS Top 20 Critical Security Controls

INCIDENT RESPONSE AWARENESS

CIS Top 20 Critical Security Controls

ADDITIONAL CONSIDERATIONS:

JOIN COMMUNITIES

MANAGED DETECTION & RESPONSE

INCIDENT RETAINER

CYBER-INSURANCE

CIS Top 20 Critical Security Controls

How to Get Started

Step 1. Gap Assessment.

2. Implementation Roadmap
3. Implement the First Phase of Controls
4. Integrate Controls into Operations
5. Report and Manage Progress

CIS Top 20 Critical Security Controls CSC # 18

- Sample Gap questions

1. Does the organization have a detailed, documented incident response plan in place?
2. Has the organization's incident response plan been approved and endorsed by senior management?
3. Are the roles of all classes of organizational staff defined in the incident response plan?
4. Have contact plans been established for engaging law enforcement during an incident?
5. Have incident handlers and staff been properly trained in technical capabilities for handling incidents?

CIS Top 20 Critical Security Controls

19.1	Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.
19.2	Assign job titles and duties for handling computer and network incidents to specific individuals.
19.3	Define management personnel who will support the incident handling process by acting in key decision-making roles.
19.4	Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.
19.5	Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an e-mail address of security@organization.com or have a web page http://organization.com/security).
19.6	Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.
19.7	Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.

CIS Top 20 Critical Security Controls

- *19-1* - Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.

CIS Top 20 Critical Security Controls

- *19-2* - Assign job titles and duties for handling computer and network incidents to specific individuals.

CIS Top 20 Critical Security Controls

- *19-3* - Define management personnel who will support the incident handling process by acting in key decision-making roles.

CIS Top 20 Critical Security Controls

- *19-4* - Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.

CIS Top 20 Critical Security Controls

- *19-5* - Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an e-mail address of security@organization.com or have a web page http://organization.com/security).

CIS Top 20 Critical Security Controls

- *19-6* - Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.

CIS Top 20 Critical Security Controls

- *19-7* - Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team

CIS Top 20 Critical Security Controls

- You are invited!!
  - SynerComm IT Summit
  - October 22-23rd
  - Milwaukee @ Potawatomi
  - Enabling Secure Digital Transformation
  - Registration

CIS Top 20 Critical Security Controls

Thank you for Attending.

Hope you can join us for the Complete CIS Top 20 CSC

Tuesday October 16th

CIC CSC # 20

Pentest and Red team Exercises