SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #13

Data Protection

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # 13 - *The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information*

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

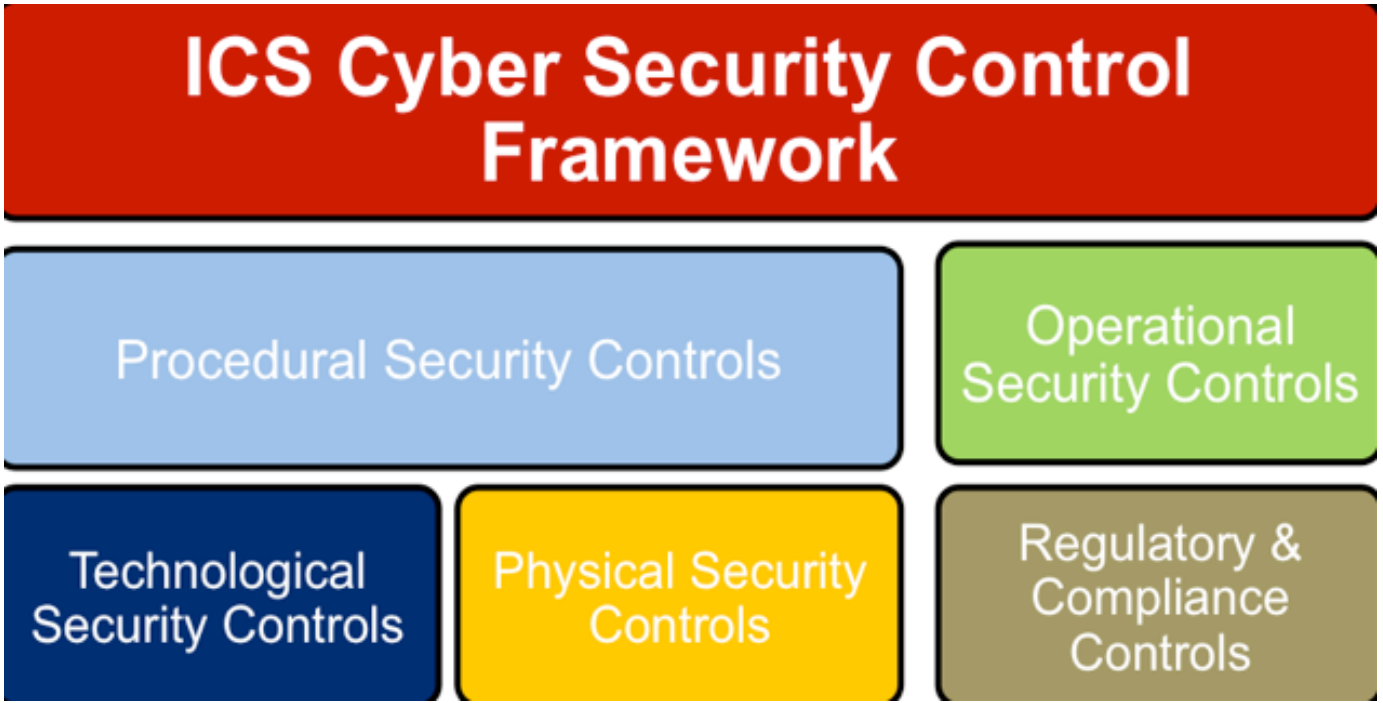
Foundational

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

CIS Top 20 Critical Security Controls



CIS Top 20 Critical Security Controls

- The Good news
- The Bad news
- The bottom line

CIS Top 20 Critical Security Controls

- Cloud Data Protection….

CIS Top 20 Critical Security Controls

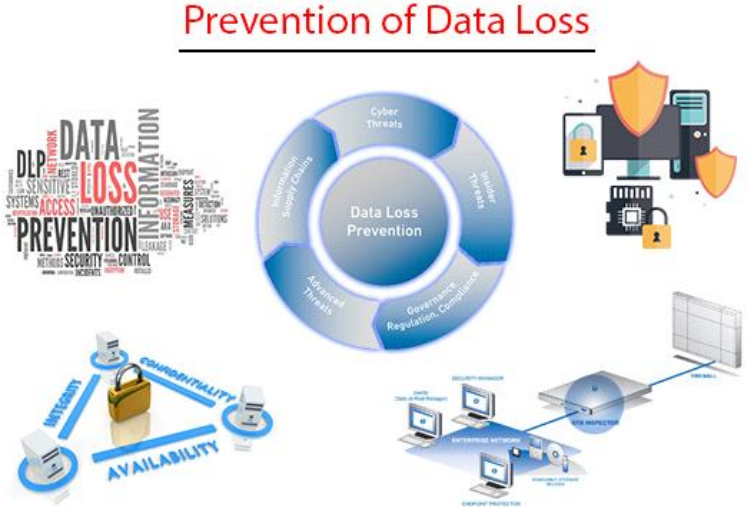
- The adoption of data encryption, both in transit and at rest, provides mitigation against data compromise.

CIS Top 20 Critical Security Controls

- The loss of control over protected or sensitive data by organizations is a serious threat to business operations and a potential threat to national security

CIS Top 20 Critical Security Controls

- How can this control be implemented, automated, and its effectiveness measured?



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

- Sample Gap questions

1. Has the organization defined data classification levels for the organization?
2. Are guidelines provided to data owners for how to classify resources and examples of datasets at each level?
3. Are the organization's security controls based on the classification level of the information system?
4. Are older, less secure encryption algorithms such as the Data Encryption Standard (DES) or MD5 in use in the organization?
5. Are symmetric encryption algorithms with keys less than 112 bit in use in the organization?
6. Is all highly sensitive data stored by the organization properly encrypted?
7. Is all highly sensitive data transmitted by the organization properly encrypted?

CIS Top 20 Critical Security Controls

13.1	Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls
13.2	Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.
13.3	Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.
13.4	Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.
13.5	If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.
13.6	Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.
13.7	Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.
13.8	Block access to known file transfer and e-mail exfiltration websites.
13.9	Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want.

CIS Top 20 Critical Security Controls

13-1 - Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls

- Free Tools
  - Windows Security & Compliance server - Data Classification Infrastructure (DCI) allows you to classify data if it contains content you specify as a certain classification (SSN = high), then applies rules to certain levels of classification (do not copy/print, encrypt, etc..).
- Commercial Tools
  - Varonis - Shows where in file systems sensitive data resides, who has access to it, who should and shouldn't have access to it, who uses it, who owns it, and where is it over exposed.
  - Netwrix Auditor - Change auditing and reporting for IT systems.
  - Digital Guardian - Classify files as they are created and create rules on what to do with certain classifications.

CIS Top 20 Critical Security Controls

- *13-2 Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.*
- Free Tools
  - BitLocker - Offered on Windows 7 Enterprise, and Windows 8, 8.1, 10 Professional Can be controlled through GPO.
  - FileVault - for Mac OSX
  - Linux - Most modern OS deployment wizards will ask if you wish to encrypt certain areas or the full disk.
- Commercial Tools
  - Voltage, Symantec, McAfee, Digital Guardian

CIS Top 20 Critical Security Controls

- *13-3 - Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.*

- Free Tools
  - opendlp - open source Data Loss Prevention suite of software
  - MyDLP Community Edition - Comodo DLP solution
- Commercial Tools
  - Netskope, Symantec, ForcePoint, Digital Guardian

CIS Top 20 Critical Security Controls

- *13-4 - Conduct periodic scans of server machines using automated tools to determine whether sensitive data (i.e., personally identifiable information, health, credit card, and classified information) is present on the system in clear text.*

- Free Tools
  - Do not recommend as data discovery is critical and without control of opensource not sure what is getting logged or transferred.
- Commercial Tools
  - McAfee, Symantec, Sophos, Forcepoint

CIS Top 20 Critical Security Controls

- *13-5 If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.*
- Free Tools
  - opendlp - open source Data Loss Prevention suite of software
  - MyDLP Community Edition - Comodo DLP solution
- Commercial Tools
  - Forcepoint, Symantec, McAfee

CIS Top 20 Critical Security Controls

- *13-6 - Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.*
- Free Tools
- Commercial Tools
  - Varonis - Shows where in file systems sensitive data resides, who has access to it, who should and shouldn't have access to it, who uses it, who owns it, and where is it over exposed.
  - Netwrix Auditor - Change auditing and reporting for IT systems.
  - Digital Guardian - Classify files as they are created and create rules on what to do with certain classifications.
  - ForcePoint

CIS Top 20 Critical Security Controls

- *13-7 - Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.*
- Free Tools
- Commercial Tools
  - Many modern Firewalls (Open Source included) offer deep packet inspection, whereby you proxy all outbound HTTPS traffic through your device, which will decrypt the traffic, scan for data loss prevention (DLP) and re-encrypt before leaving the network. This requires that you import and trust the network device's Certificate on all client machines.

CIS Top 20 Critical Security Controls

- 13-8 Block access to known file transfer and e-mail exfiltration websites.

- **Free Tools**
  - Black list subscriptions. (SANS storm center)
- **Commercial Tools**
  - URL filtering categorizations
  - NGFW can granularly allow access put prevent file transfer
  - Proofpoint, Fireeye

CIS Top 20 Critical Security Controls

- 13-9 Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want.
- Free Tools
  - Again, not something I would skimp on.
- Commercial Tools
  - Symantec, Digital Guardian, Forcepoint, Sophos, TrendMicro

CIS Top 20 Critical Security Controls

CIS Top 20 Critical Security Controls

Thank you for Attending.

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

Tuesday July 24th

CIC CSC # 14

Controlled Access on Need to Know