SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #10

Data Recovery Capability

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # 10 – Data Recovery Capability

Center for Internet Security (CIS) states the following is the key principle of this control:

"The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it."

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

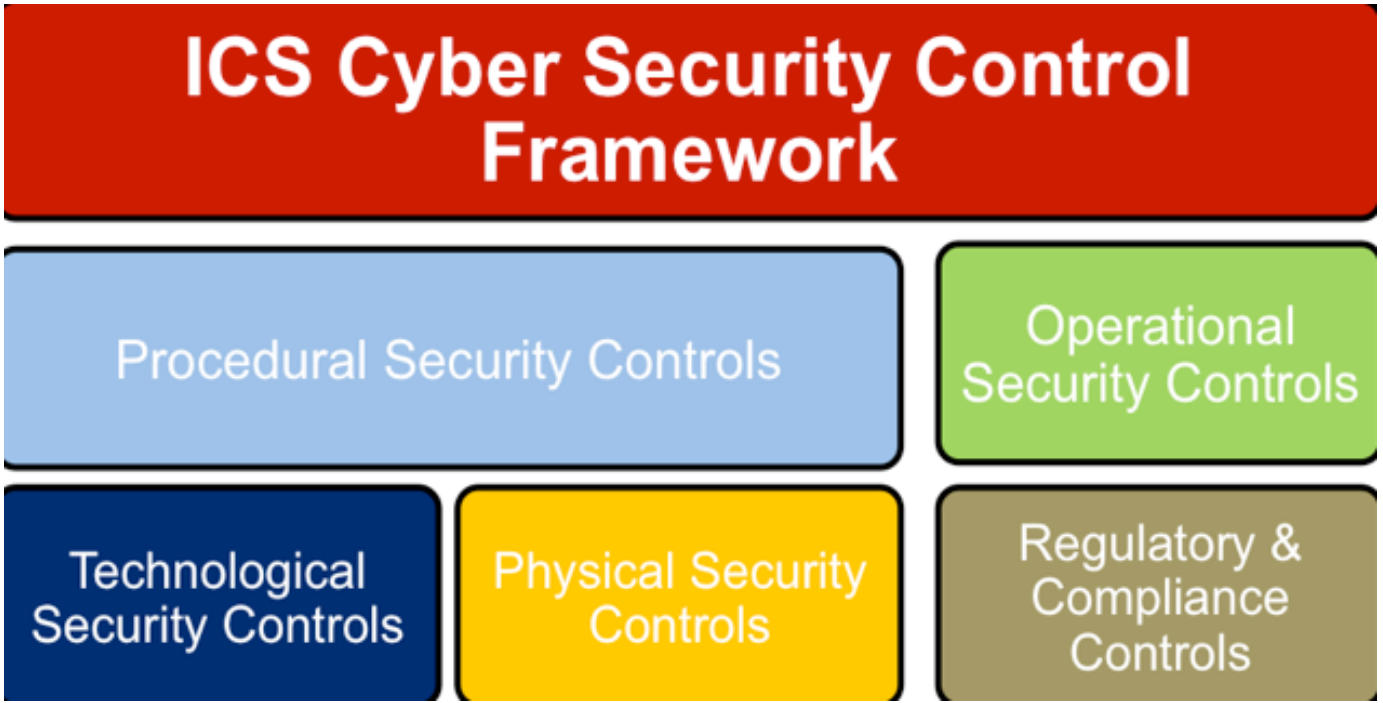
Foundational

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

- Who Cares About CIS Critical Control 10?
- As I have in the past, you may be wondering why this matters. So what? Who cares? What's the big deal here?

CIS Top 20 Critical Security Controls

- How to Implement This Security Control

CIS Top 20 Critical Security Controls

- As part of common procedures and practice, an organization should conduct backup tests quarterly.

CIS Top 20 Critical Security Controls

- Like many things in life, practice makes perfect…

CIS Top 20 Critical Security Controls

- **Key Takeaways for Control 10**
  - Backups can save your company.
  - Don’t forget to test.
  - How often is a regular basis?

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

System	10.1	Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.
System	10.2	Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
System	10.3	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
System	10.4	Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations.

CIS Top 20 Critical Security Controls

- 8-1 - *Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.*

- Free Tools
  - Cobian Backup - A long time player in the data backup arena, Cobian has all the settings you could ever want...except full OS backup. It backs up data, and very well.
  - Paragon Backup Free - A free full OS, disk, and data backup utility.
- Commercial Tools
  - There are many, and it's a hot topic. So, I will point you to the 2015 Gartner Magic Quadrant for Backup / Recovery Software

CIS Top 20 Critical Security Controls

- 8-2 - *Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.*
  - This is more of a procedure than a tool.

CIS Top 20 Critical Security Controls

- 8-3 - *Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.*
  - This is more of a procedure than tool. Though, do consider if your storage where backups are stored does not offer disk encryption, many backup software vendors offer strong encryption at the cost of slower backups and higher CPU usage.

CIS Top 20 Critical Security Controls

- 8-4 - *Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls.*
  - *This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations.*
- Again, more of a process than tool.

CIS Top 20 Critical Security Controls

Things to consider when implementing or evaluating your data recovery solution.

1. Implement a file system that supports snapshots.
2. Encrypt your data at rest as well as in transit.
3. Implement a one-way backup solution. Devices should be able to create new backups, not change or delete old ones.
4. Test your backup solution. Testing your backups should be part of your process, not part of your panic.
5. Replicate your backups. Having a backup in one place is great. Having it in two places is better.
6. Create a backup policy. Plan your backup policy to follow any regulatory or official requirements and include current diagrams of your backup process.
7. Create offsite or offline backups.
8. Implement a reporting system. You should know when backups have failed or backup configurations has been changed.
9. By implementing data recovery, you stand the best chance to protect your data from attackers via ransomware or other data attacks.

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 June 12th

CIC CSC # 11

Secure Configuration of Network Devices