

The webcast will start at 1:00 p.m. Eastern

- Visit capincrouse.com/security-controls-1 to access these resources from today's webcast:
 - Handout
 - Recording
- To receive CPE credit, you must respond to the polling questions, which are not available on mobile devices. To receive CPE credit, you must log in on a computer.
- CPE certificates will be emailed to you within the next few weeks.

18 Critical Security Controls – Part 1

Allison Ward, Partner
Katie Kane, Senior Manager
05.24.2023



The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, tax, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.

3

Polling Question 1

Do you want CPE credit?

4



Utilizing a Control Framework

 CAPINTECH

Why use a framework?

- PCI DSS
- NIST CSF
- CIS Top 18
- ISO 27001
- COBIT
- HIPAA
- FFIEC



6

What is the Center for Internet Security (CIS)?

“Making the Connected World a Safer Place”

Source: [cisecurity.org](https://www.cisecurity.org)

7

Why use **this** framework?

- Essential cyber hygiene
- Buildable and adaptable
- Identify, protect, detect, respond, and recover
- Prioritize implementation
 - Risk profile
 - Available resources

8

Summary of Controls and Safeguards

CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards 161 2/5 162 4/5 163 5/5	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards 161 3/7 162 6/7 163 7/7	CONTROL 03 Data Protection 14 Safeguards 161 6/14 162 12/14 163 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards 161 7/12 162 11/12 163 12/12	CONTROL 05 Account Management 6 Safeguards 161 4/6 162 6/6 163 6/6	CONTROL 06 Access Control Management 8 Safeguards 161 5/8 162 7/8 163 8/8
CONTROL 07 Continuous Vulnerability Management 7 Safeguards 161 4/7 162 7/7 163 7/7	CONTROL 08 Audit Log Management 12 Safeguards 161 3/12 162 11/12 163 12/12	CONTROL 09 Email and Web Browser Protections 7 Safeguards 161 2/7 162 6/7 163 7/7

Source: cisecurity.org/controls/implementation-groups

9

Summary of Controls and Safeguards

CONTROL 10 Malware Defenses 7 Safeguards 161 3/7 162 7/7 163 7/7	CONTROL 11 Data Recovery 5 Safeguards 161 4/5 162 5/5 163 5/5	CONTROL 12 Network Infrastructure Management 8 Safeguards 161 1/8 162 7/8 163 8/8
CONTROL 13 Network Monitoring and Defense 11 Safeguards 161 0/11 162 6/11 163 11/11	CONTROL 14 Security Awareness and Skills Training 9 Safeguards 161 8/9 162 9/9 163 9/9	CONTROL 15 Service Provider Management 7 Safeguards 161 1/7 162 4/7 163 7/7
CONTROL 16 Applications Software Security 14 Safeguards 161 0/14 162 11/14 163 14/14	CONTROL 17 Incident Response Management 9 Safeguards 161 3/9 162 8/9 163 9/9	CONTROL 18 Penetration Testing 5 Safeguards 161 0/5 162 3/5 163 5/5

Source: cisecurity.org/controls/implementation-groups

10

Navigator Tool

<input type="checkbox"/>	Sub	Title	Asset Type	Implementation Group:	IG1	IG2	IG3	HIPAA	NISTCSF
CIS Control 1 - Inventory and Control of Enterprise Assets Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.									
<input type="checkbox"/>	1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Devices		●	●	●	●	●
<input type="checkbox"/>	1.2	Address Unauthorized Assets	Devices		●	●	●		
<input type="checkbox"/>	1.3	Utilize an Active Discovery Tool	Devices			●	●		●
<input type="checkbox"/>	1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Devices			●	●		●
<input type="checkbox"/>	1.5	Use a Passive Asset Discovery Tool	Devices				●		●

Source: cisecurity.org/controls/cis-controls-navigator/

11

Polling Question 2

Are you currently using a framework to design your controls?

12

What is included in Implementation Group (IG) 1?

- Minimum standards for all enterprises
- Foundational set of 56 safeguards
- Necessary to defend against common attacks



Which organizations will benefit from IG1?

- Limited IT and security expertise
- Limited tolerance for downtime
- Sensitivity of data being protected is low
- Thwarting general, non-targeted attacks
- Using commercial, off-the-shelf hardware and software
- Organizations working toward IG2/IG3



Controls We Will Skip Today



None of these controls are in IG1.

Source: cisecurity.org/controls/implementation-groups

15



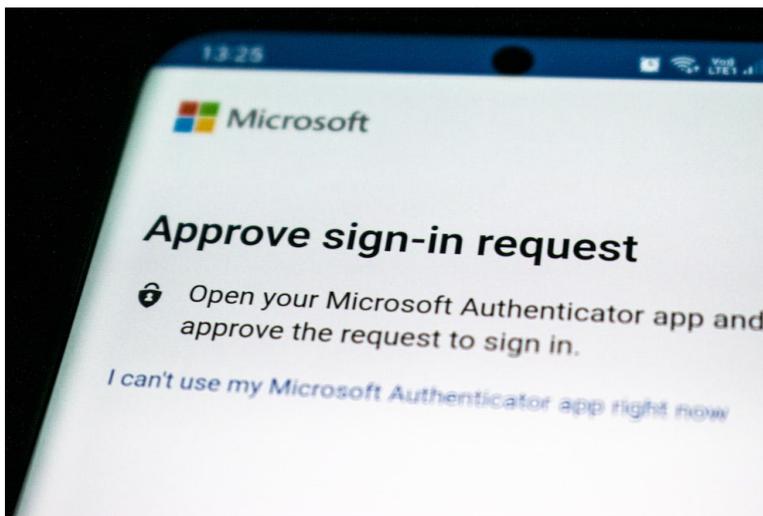
Cisco: A Breach to Learn From

Step 1: Stolen Credentials



17

Step 2: Gaining MFA Approval to VPN



18

Step 3: Persistence and Movement



19



Review of Controls

1. Inventory and Control of Enterprise Assets

- Establish and maintain detailed enterprise asset inventory
- Address unauthorized assets

21

2. Inventory and Control of Software Assets

- Establish and maintain a software inventory
- Ensure authorized software is currently supported
- Address unauthorized software



22

3. Data Protection

- Establish and maintain a data management process
- Establish and maintain a data inventory
- Configure data access control lists
- Enforce data retention
- Securely dispose of data
- Encrypt data on end-user devices

23

4. Secure Configuration of Enterprise Assets and Software

- Establish and maintain a secure configuration process
- Establish and maintain a secure configuration process for network infrastructure
- Configure automatic session locking on enterprise assets
- Implement and manage a firewall on servers

24

4. Secure Configuration of Enterprise Assets and Software

- Implement and manage a firewall on end-user devices
- Securely manage enterprise assets and software
- Manage default accounts on enterprise assets and software

25

5. Account Management

- Establish and maintain an inventory of accounts
- Use unique passwords
- Disable dormant accounts
- Restrict administrator privileges to dedicated administrator accounts

26

6. Access Control Management

- Establish an access granting process
- Establish an access revoking process
- Require MFA for externally exposed applications
- Require MFA for remote network access
- Require MFA for administrative access



27

Polling Question 3

What kind of multi-factor authentication (MFA) are you using on your systems?

28

7. Continuous Vulnerability Management

- Establish and maintain a vulnerability management process
- Establish and maintain a remediation process
- Perform automated operating system patch management
- Perform automated application patch management

29

8. Audit Log Management

- Establish and maintain an audit log management process
- Collect audit logs
- Ensure adequate audit log storage

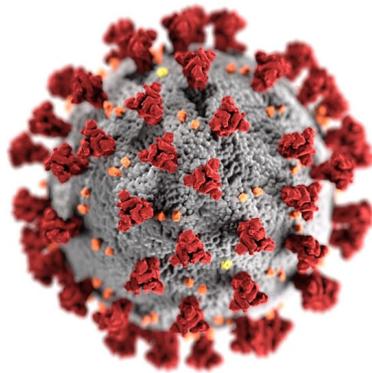
30

9. Email and Web Browser Protections

- Ensure use of only fully supported browsers and email clients
- Use DNS filtering services



10. Malware Defenses



- Deploy and maintain anti-malware software
- Configure automatic anti-malware signature updates
- Disable autorun and autoplay for removable media

11. Data Recovery

- Establish and maintain a data recovery process
- Perform automated backups
- Protect recovery data
- Establish and maintain an isolated instance of recovery data

33

12. Network Infrastructure Management

- Ensure network infrastructure is up to date



34

Polling Question 4

Based on what you've heard so far, are you interested in using the CIS Top 18 control framework?

35

14. Security Awareness and Skills Training

- Establish and maintain a security awareness program
- Train workforce members on:
 - Recognizing social engineering attacks
 - Authentication best practices
 - Data handling best practices

36

14. Security Awareness and Skills Training

- Train workforce members on:
 - Causes of unintentional data exposure
 - Recognizing and reporting security incidents
 - How to identify and report if their enterprise assets are missing security updates
 - The dangers of connecting to and transmitting enterprise data over insecure networks

37

15. Service Provider Management

- Establish and maintain an inventory of service providers



17. Incident Response Management

- Designate personnel to manage incident handling
- Establish and maintain contact information for reporting security incidents
- Establish and maintain an enterprise process for reporting incidents



Join Us for Part 2 on August 30

Free Cyber Series Webcast

18 Critical Security Controls – Part 2

Wednesday, August 30
1:00 – 2:00 p.m. EDT

Scan the QR code or visit
capincrouse.com/events to register!



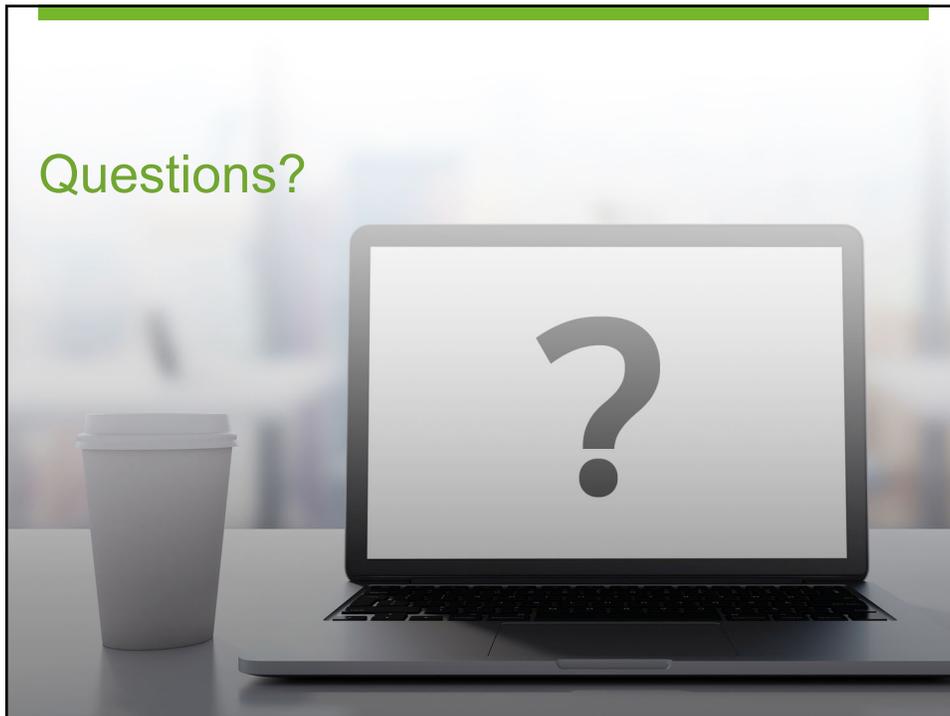
You Could Win a Free CapinTech Cyber Checkup or Phishing Test!

- Receive one entry for each 2023 CapinTech Cyber Series webcast you:
 - Attend live, or
 - Watch the recording of within one week of the webcast date
- Winner selected after the final webcast of the 2023 series



41

Questions?





Thanks!

Allison Ward
Partner, CapinTech

✉ award@capincrouse.com
📱 505.50.CAPIN ext. 2008

Katie Kane
Senior Manager, CapinTech

✉ kkane@capincrouse.com
📱 505.50.CAPIN ext. 2007

