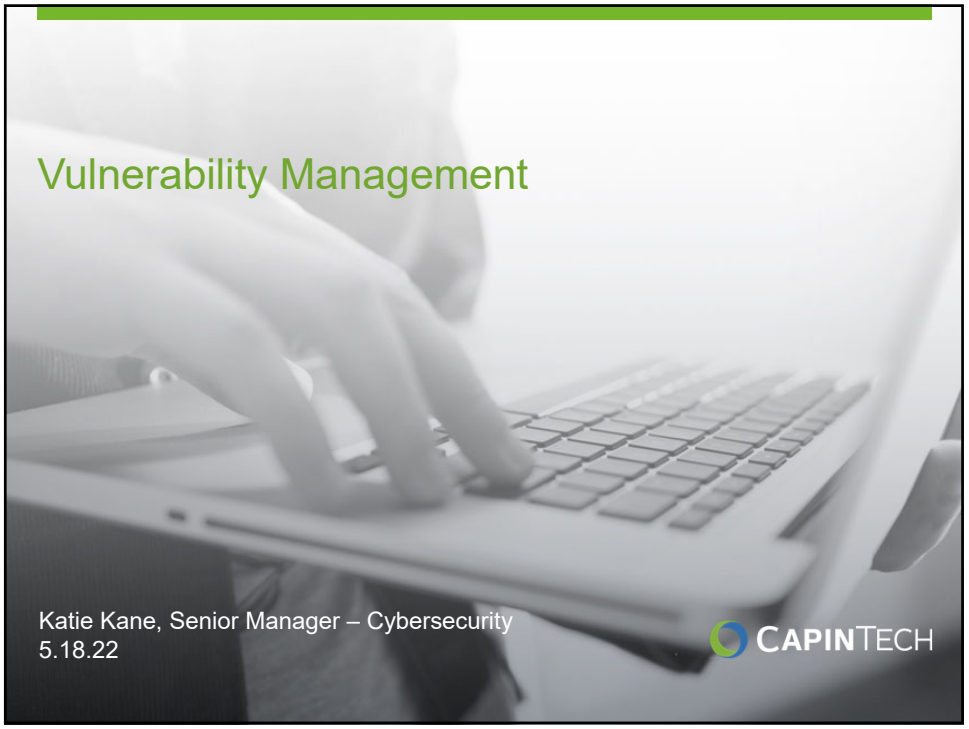
The webcast will start at 1:00 p.m. Eastern

- Visit capincrouse.com/vulnerability-management 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.



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, 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.

Polling Question 1

Do you want CPE credit?

Objectives

- What is a vulnerability
- Recent vulnerabilities, including zero-day vulnerabilities
- Controls and processes to aid in detection
- Baseline controls for ongoing mitigation

What is a vulnerability?

- Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source
- Hole in code
- Allows cyber criminals to compromise systems
- Discovered daily

Examples of Vulnerabilities

- Software/operating system
- Firewall/network configuration
- Zero-day
- Authentication

Polling Question 2

How prepared do you feel your organization is?

Colonial Pipeline Company — May 2021

- Result of a vulnerability that led to a single compromised VPN password that granted access on April 29, 2021
  - Account was enabled but not active
- Password since discovered inside a batch of leaked passwords on the dark web
  - Colonial employee may have used the same password on another account that was previously hacked

Microsoft Power Apps — August 2021

- Result of a vulnerability in the design of the application
- Approximately 38 million records across 47+ organizations
- Various types of records exposed
  - Employee records; COVID-19 testing, tracing, and vaccinations; names, dates of birth, Social Security numbers, addresses, and demographic details
- Misconfiguration was by third party, not Microsoft directly

Apache Log4j December 2021

- What is Log4j?
- Many don't know how they were affected
- Extensive efforts to pinpoint vulnerable devices
- Thousands of attempts to exploit the vulnerability

Apache Log4j December 2021

- Organizations have a duty to take reasonable steps to mitigate known software vulnerabilities
- FTC threatening action against those failing to mitigate
- Incident response component
- You patched and resolved the issue.
  - But were you already affected?

Bernalillo County — January 2022

- Result of a vulnerability that led to a ransomware attack, resulting in a data breach
- Ramifications
  - Closing government buildings
  - Blocking of jail camera feeds and entrapment of inmates due to failure of automatic door mechanisms
  - Some public services unavailable
- Fire and rescue operations continued due to backup contingencies

Puma — January 2022

- Sports manufacturer notified of data breach following a ransomware attack against a third party (Kronos) in December 2021
- Personal information of over 6,632 employees, including Social Security numbers, compromised
- No customer data was affected
- Did not regain access to data until end of January

Bridgestone — February 2022

- Ransomware attack that led to the disconnection of manufacturing from the network (production halted for a week)
- Announced in March that they would leak the stolen data if ransom not paid
- Able to do a comprehensive security check and reconnect network

GiveSendGo — February 2022

- Result of a vulnerability that led to a compromise of donor data
- Data included names, donation amounts, and limited credit card information of over 92,000 donors
- Website redirected to a rogue domain that offered a downloadable file
- Just three days after, the company was alerted to serious security issues


SECURITY
GAP


Reputation
Risk

Establish Baseline Controls

- Monitor different sites that give vulnerability information
- Monitor vendor alerts
- Establish an inventory of hardware and software so you know what could be vulnerable
- Perform vulnerability scanning
  - Penetration testing

Security Concerns

- Third-party vendors
  - New relationships
  - Existing vendors
- Organization responsibilities
- End-user assistance

New Third-Party Vendor Relationships

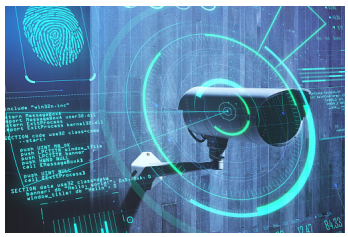
- General inquiry
- Workforce
- Information security
  - Cloud storage
- Policy documentation

Existing Vendor Relationships

- Periodic oversight procedures
  - Review of audit reports
  - Backup or disaster recovery testing
  - Financial condition
  - Existing contracts
  - Vendor oversight

Organizational Responsibilities

- Ongoing monitoring of critical infrastructure and vendor services
  - Patch management reporting
  - Malware management reporting
  - Backup process
  - Vulnerability scanning
  - Network penetration testing



Inventory

- Hardware inventory
  - Servers, workstations, laptops
  - Mobile devices
  - Networking equipment
- Software
  - Installed applications
  - Web applications

Vulnerability Testing

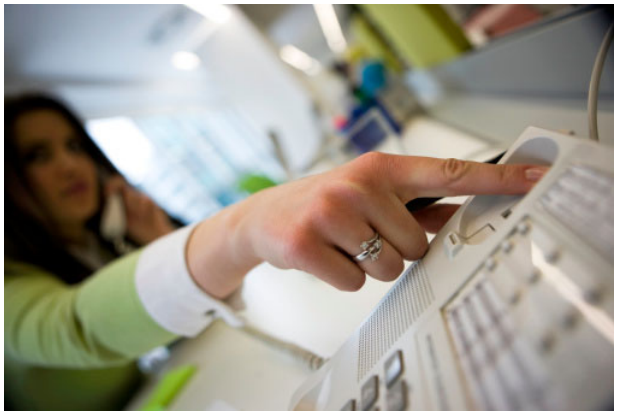
- Identification of potential vulnerabilities that may be exploited
- Assurance of system state (updates and upgrades implemented)
- Identification of security control weaknesses along with related risk ratings according to industry classification

Network Penetration Testing

- Vulnerability verification to prove existence of vulnerabilities
- Benefits
  - Reveals vulnerabilities that can be exploited successfully
  - Reveals ways hackers could actually gain access to your resources
  - Tests ability to respond to a real threat

End-User Assistance

If you see something, say something!

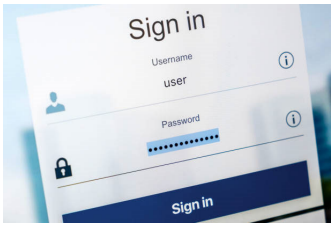


Polling Question 3

Has your organization experienced any major vulnerabilities within your environment?

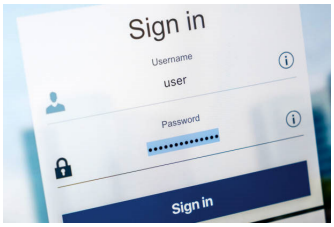
System Provisioning

- Establish system-hardening process
  - Remove unnecessary applications
  - Disable built-in administrator account
  - Install anti-malware solution
  - Apply system restrictions (USB access, local administrative rights, etc.)
- Implement review procedures (never set and forget)



User Provisioning and Access

- Minimum rights for users
- Review regularly
  - Job transfers
  - No longer needed



Password Security

- Numbers, characters, symbols
- Avoid common words
- Change often and when compromised
- Length – 8…12…??

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

› Learn about our methodology at hivesystems.io/password

Password Security

- Unique and private passwords
  - Password manager?
- Business ≠ personal
- Account lockout and inactivity threshold
- Biometrics
- Layered security

Multi-Factor Authentication

- Critical for all cloud applications
  - Remote access, email, AWS/Azure
- Mobile devices, email message, tokens
- Consider IP address, time, and day restrictions

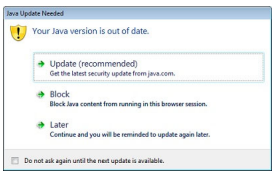
Email

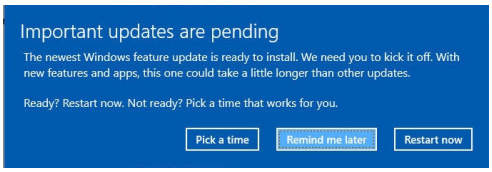
- Easily spoofed or hacked
- Not all services are encrypted
- Confidential email MUST be secured
  - Sending and receiving
- If not needed, limit or restrict web mail

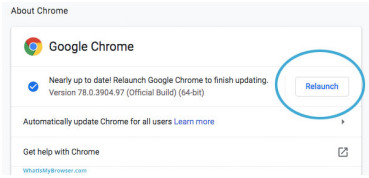
Wi-Fi Networks

- Ensure properly secured Wi-Fi, including those at home offices (WPA2 encryption or better)
  - Avoid use of public Wi-Fi; if necessary, use a VPN!
- Secure password for access
- Guest network for non-business systems (segregate)
- Keep personal and business devices up to date
- Consider the use of mobile hotspots

Malware and Patch Management







Device Management

- Centralized system
  - All devices present
  - Receive latest updates or definition files
  - Remediate issues
- Limited user rights
  - Downloaded apps from Internet
  - Browser add-ons

Web Surfing

- Avoid questionable websites
- Be cautious when downloading
- Use updated browsers
- Inspect URLs
- Be wary of malvertising

Social Networking

- Impersonation
  - Phishing and vishing
- Identity theft
- Pretexting
- Security questions and answers
- Data not always private

Data Storage

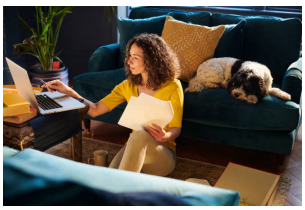
- Cloud applications typically can be accessed from any location on any device
- Risk of applications being accessible on unauthorized devices, resulting in data management concerns

Internet of Things (IoT) Devices

- Inventory devices in use
- Layered security controls
  - Strong passwords
  - Evaluate data and analytics sharing
  - Patching procedures
  - Disable features
  - Segmented network
- Consider listening capability

Remote Access Tools

- VPNs, LogMeIn, GoToMyPC, Remote Desktop Protocol (RDP)
- Increase in end users
- Require proper security measures
  - Quick fixes vs. long-term solution
- Does this affect strategic planning?



Shadow IT

- Apps or devices that are utilized without IT knowledge
  - Personal or mobile devices
- Rogue cloud services
  - Personal email, document scanning, cloud storage
- Appropriate authorization procedures

Incident Response

- Determine cause of the incident
- Determine the impact and how to resolve
- Notify appropriate parties
- Contact vendors, if applicable

Polling Question 4

Do you feel that this presentation was helpful?

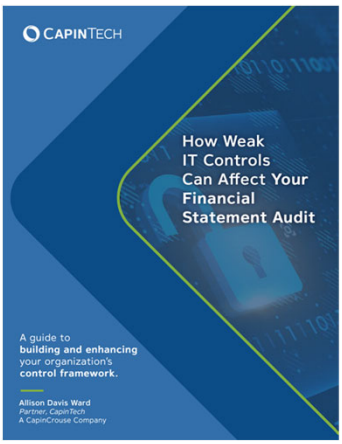
Key Takeaways

- New threats happening every day — no one is immune!
- Loss of reputation can be significant
- Manage vendor relationships appropriately
- Establish ways to identify vulnerabilities within your own environment

Key Takeaways

- Maintain adequate security controls
  - Provide necessary tools for users
  - Doesn’t have to be expensive!
  - Train to build culture of awareness

New E-book Now Available!



Download your free copy!
Scan this QR code or visit
capincrouse.com/it-controls

You Could Win a Free CapinTech Cyber Checkup!

- Receive one entry for each 2022 CapinTech Cyber Series webcast you:
  - Attend live, or
  - Watch the recording of within one week of the webcast date
- Winner announced December 16

Questions?

Thanks!

Katie Kane, Senior Manager

kkane@capincrouse.com

505.50.CAPIN ext. 2007

CAPINTECH