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

- Visit capincrouse.com/it-controls-webcast 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.

How Weak IT Controls Could Affect Your Financial Statement Audit

Allison Davis Ward, Partner
3.2.22

CAPINTECH

3

Polling Question 1

Do you want CPE credit?

4

Technology Touches Everything

5

Overview for Today

- Perimeter security

- Vulnerability management

- Backup management and disaster recovery planning

- Application controls

- What next?

6

What Is the Impact?

- Wreak havoc

- Disrupt operations

- Steal sensitive data

- Prevent you from generating complete and accurate financial data

7

Weak Controls ≠ Material Misstatement

- Multiple ways to mitigate risks

- Compensating factors may aid in recreation or recapturing of impacted data
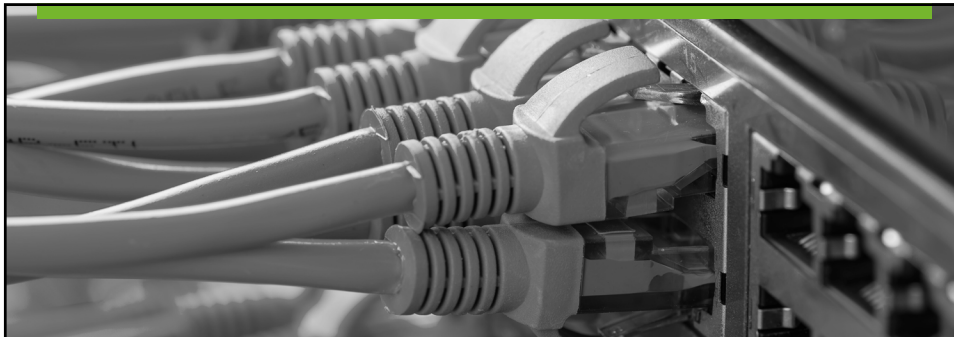
- Aim for layered controls

8

Roadblocks to Implementing Controls

- Time constraints
- Budgetary constraints
- Understaffing

- Lack of expertise
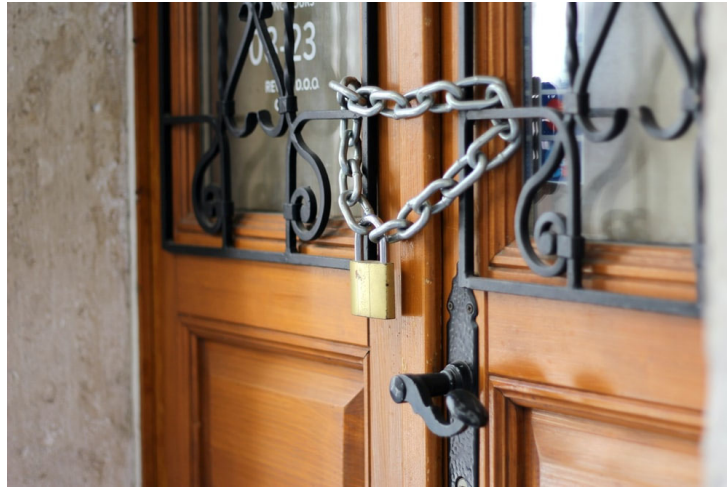- Balancing security with efficiency/operations

9

Perimeter Security
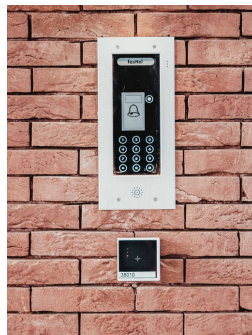
CAPINTECH

The Need for Perimeter Security

11

Firewalls and Intrusion Detection/Prevention

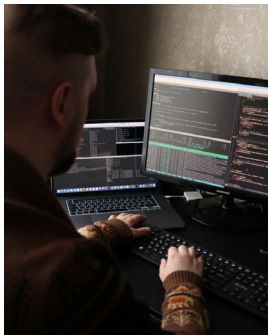| Firewall = door	Intrusion detection system = alarm	Intrusion prevention system = patrol

12

Impact of Weak Perimeter Security

13

Impact of Weak Perimeter Security

14

Impact of Weak Perimeter Security

15

How to Strengthen Controls

- Establish a robust firewall

- Implement intrusion detection capabilities

- Configure alerts and monitor

  - 24x7 visibility

  - Internally vs. third party

16

How to Strengthen Controls Under Constraints

- Implement conservative configurations

- Update your device regularly

- Enhance intrusion prevention

- Monitor proactively as feasible

  - Evaluate alerting capabilities

  - Involve more staff

17

Polling Question 2

What area of perimeter security do you think could be enhanced at your nonprofit?

18

Vulnerability Management

CAPINTECH

The Need for Vulnerability Management

20

Patch and Anti-Malware Management

- Vulnerabilities arise from outdated or obsolete items

- Malware often allows exploitation of the vulnerabilities

- If it connects to the Internet, patch it!

  - Update firmware, operating systems, and applications

  - Decommission end-of-life devices

- Utilize anti-malware protection on relevant endpoints

  - Signature based vs. behavioral based

21

Vulnerability Scanning

- Vulnerability scanning

  - Passive test

  - External vs. internal

  - Perform frequently

  - Remedy results quickly

- Penetration testing

  - Active test

22

Impact of Weak Vulnerability Management

23

Impact of Weak Vulnerability Management

24

Impact of Weak Vulnerability Management

25

How to Strengthen Controls

- Identify your assets

- Identify vulnerabilities

  - External vulnerability scanning

  - Internal vulnerability scanning

  - Monitoring various resources

  - Monitoring vendor alerts

26

How to Strengthen Controls

- Develop patching processes

- Install anti-malware protection

- Utilize centralized monitoring tools

- Limit user access rights

27

Polling Question 3

Which of the following areas do you feel could have the biggest impact on your financial statements?

28

Backup and Disaster Recovery
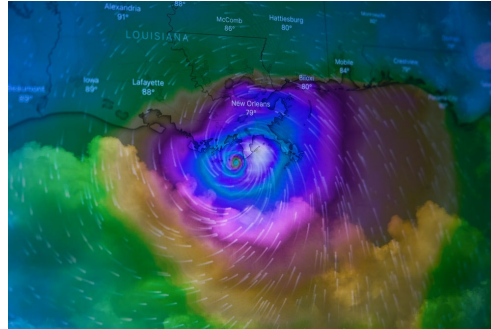
CAPINTECH

The Need for Backups and Disaster Planning

30

Facets of the Backup Process

- Frequency and retention schedules

- Location of backups in relation to source data

  - What disasters are you prone to?

- Encryption

- Impact of ransomware

31

Disaster Recovery Planning

- Identify critical assets, people, processes, vendors, and hosting locations

  - Define recovery processes

  - Develop manual operating procedures to support continuance of key operations

- Consider vendor dependencies

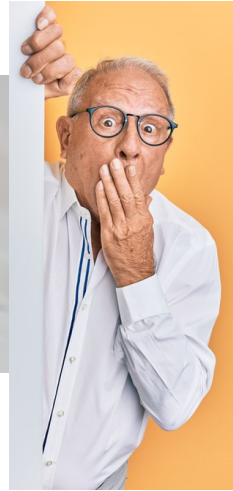- Document, test, and train

32

Impact of Poor Backup Processes

33

Impact of Poor Backup Processes

34

Impact of Poor Backup Processes

35

Impact of Poor Backup Processes

36

How to Strengthen Controls

- Establish a robust backup process

  - Monitor backups for success

  - Test the ability to restore from backups

- Perform a business impact analysis

- Reduce risks to a level within your risk appetite

  - One size does NOT fit all

37

How to Strengthen Controls

- Store data off-site

  - Sufficient distance away

  - Sent off-site at appropriate frequency

- Enable encryption as feasible

- Mitigate risk and impact of ransomware

38

19

How to Strengthen Controls

- Develop business continuity/disaster recovery plans

  - Include key personnel

  - Document and train staff

- Test plans

  - Live vs. scheduled

  - Tabletop discussions

39

Application Controls

CAPINTECH

The Need for Application Security

- Brute force attacks are rampant

- We continually use bad password practices

- Database breaches can have an impact on us

41

Settings to Consider

- Password length, complexity, and expiration

- Intruder lockout settings

- Multi-factor authentication (MFA)

  - Something you know (e.g., password)
    + something you have (e.g., text code)
    + and/or something you are (fingerprint)

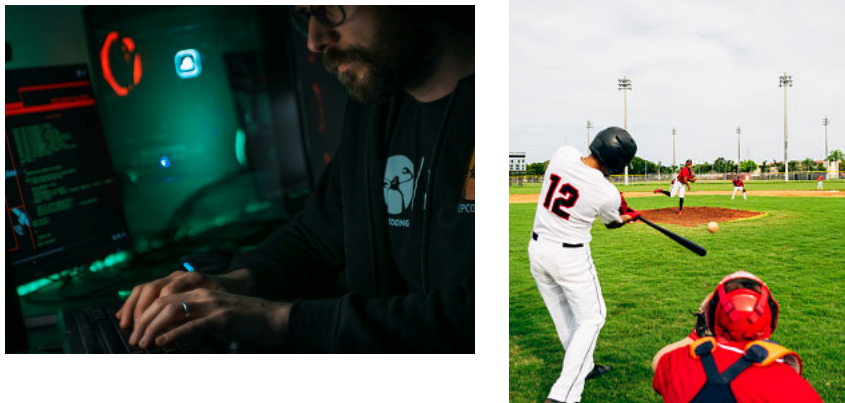- Other (e.g., inactivity timeouts, IP/country restrictions, time and day restrictions)

42

Impact of Weak Application Controls

43

Examples of Underdeveloped Controls

44

Examples of Underdeveloped Controls

45

Polling Question 4

Which application setting could be enhanced to further protect your systems?

46

How to Strengthen Controls

- Learn your current settings

- Review industry best practices

  - Traditional settings

  - Evolving recommendations (e.g., NIST, Microsoft)

- Visit capincrouse.com/password-management for a handout and recording of the Password Management and Authentication Security webinar

47

How to Strengthen Controls

- Evaluate available enhancements

- Determine how they would impact your users

- Consider compensating factors and layered controls

- Increase focus on lockout settings and MFA

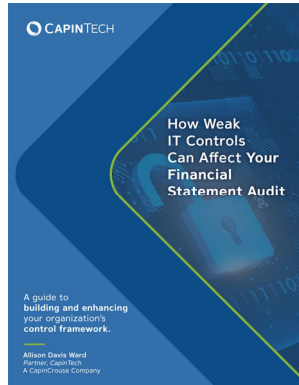- Train your user base

48

What's Next?

CAPINTECH

What's Next?

- Don't be discouraged

- Conduct a risk assessment

  - Identify your top risks

  - Determine where additional controls are warranted

- Plan for enhancements

- Remember the goal is **layers of control**

50

New E-book Available Soon!

Sign up to receive your free copy at
capincrouse.com/it-controls

51

Additional Resources

- Website: capintech.com

- Email: cybersecurity@capincrouse.com

- Articles and blog posts:
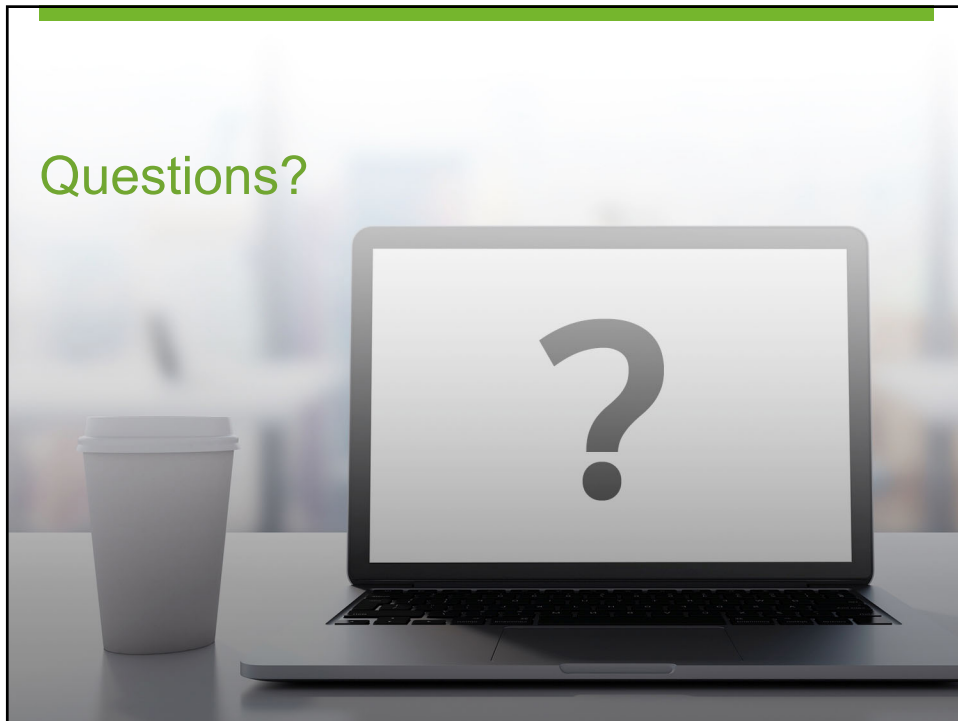 capincrouse.com/category/cybersecurity

52

3/2/2022

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

53

Questions?

27
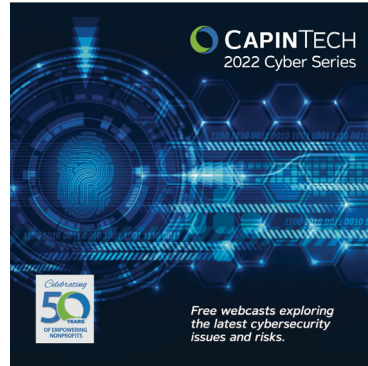
Thanks!

Allison Ward, CISSP, CISA, CISM
Partner, CapinTech

✉ award@capincrouse.com

📱 505.50.CAPIN ext. 2008

CAPINTECH