We’ll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

10 Cybersecurity Questions for Health Care Organizations

September 17, 2025

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Session CPE Requirements

- You need to attend 50 minutes to receive the full 1 CPE credit.
- There will be 4 polling questions throughout the presentation. You must respond to a minimum of 3 to receive the full 1 CPE credit.

Both requirements must be met to receive CPE credit

Presenting Today

Javier Young, CISSP, Principal

Javier is a principal within the Cybersecurity department in CLA's National Digital group and has been in the cybersecurity field for more than 15 years. Prior to joining CLA, Javier spent ten years supporting the Department of Defense as well as a financial services company in the fields of insider threat, incident response, fraud, waste and abuse, analytics, and systems engineering. Since Javier has been with CLA, he has spent the majority of his time providing IT security, risk, and consulting services to clients in healthcare, higher education, and financial related institutions.

Serving *You*

CLA creates opportunities for businesses, individuals, and communities through our wealth advisory, outsourcing, digital, audit, tax and consulting services. With nearly 9,000 people, more than 130 U.S. locations, and a global vision, we promise to know you and help you.

Learning Objectives

1

Recognize the top questions a health care organization should be able to answer with respect to cybersecurity

2

Identify the current state of cybersecurity maturity at an organization

3

Recall the importance of proactive cybersecurity endeavors

Polling Question

How optimistic are you on the current economic conditions and the impact to your organization?

- 5 = Very confident
- 4 = Confident
- 3 = Neutral
- 2 = Somewhat confident
- 1 = Not at all confident

One: Do We Have a Formal Information Security Program in Place?

The Information Security Program Should Establish

The importance of information

The need to protect information

Roles and responsibilities

Enforcement of policies

Policies, Standards, and Procedures

Network and system policies

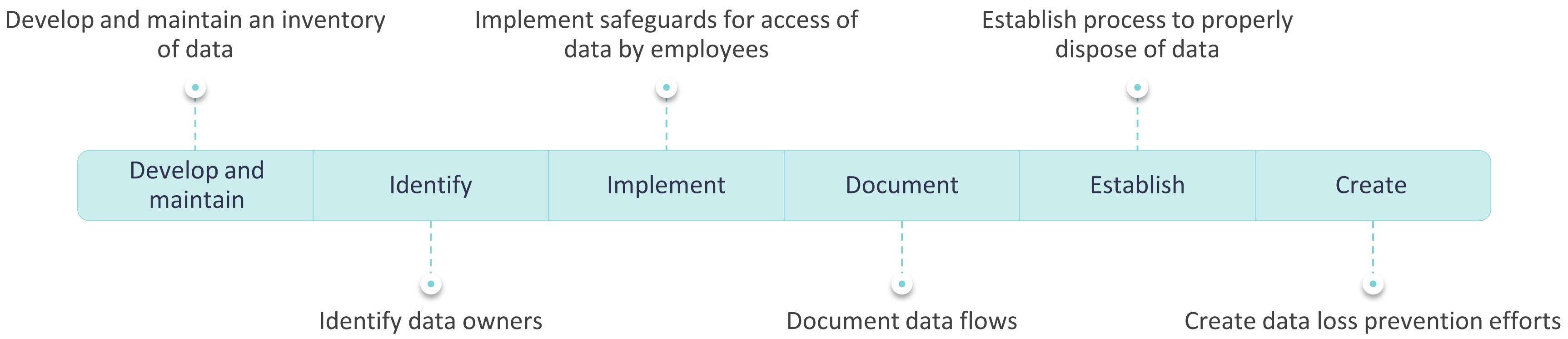
- Logging and monitoring of security events
- Remote access
- Wireless networking
- Patch management
- Firewall management
- Antivirus management
- Intrusion detection/prevention

The Board should review (annually)

- Information security program and status
- IT and information security policies
- Security breaches or attempted breaches
- IT strategic plan
- Information security risk assessment
- Business continuity plan and testing results
- Incident response plan
- Results from vendor management reviews
- Insurance coverage for cybersecurity

Two: What Data is Important to Our Organization?

Data Protection



Develop and maintain an inventory of data

Implement safeguards for access of data by employees

Establish process to properly dispose of data

Develop and maintain

Identify

Implement

Document

Establish

Create

Identify data owners

Document data flows

Create data loss prevention efforts

https://www.cisecurity.org/controls/

Organizations should strive to have at least three levels of data classifications.

- Public
- Internal use
- Confidential

Data Classification

Controls should be implemented for each level of classification regarding data handling.

Data Backups

Attackers are getting smarter and deleting or encrypting online backups; so, organizations should enhance that they have off-line copies of backup and restore files available

Backup and restore files should be saved in well secured location

Perform an in-depth review of file permissions for network file shares

Test the restoration of your data

Three: When Was Our Last HIPAA Risk Assessment or Security Audit Performed?

HIPAA Risk Assessment

Identify potential risks and vulnerabilities to the confidentiality, integrity, and availability (C.I.A) of all e-PHI that the organization creates, receives, maintains, or transmits.

- System characterization
- Threat and vulnerability identification
- Assessment of current security measures
- Threat likelihood and impact analysis
- Risk determination
- Control recommendations
- Results documentation

The risk analysis should be reviewed or updated annually to assess changes to the security environment.

HIPAA Risk Assessment

The risk analysis should be reviewed or updated annually to assess changes to the security environment.

Audit tracking mechanism should be in place to regularly report on the status of outstanding audit and assessment findings.

Polling Question

When was your last HIPAA Risk Assessment performed?

- 2025
- 2024
- We have not had one in recent years
- We plan to perform one ASAP
- N/A - we do not transmit/process/store electronic Protected Health Information (ePHI)

Four: How Are Vulnerabilities Managed at the Organization?

Vulnerability Management

How are vulnerabilities defined and identified?

Threat intelligence?
Internal scanning?
Vendor collaboration?

Within how many days are critical and high vulnerabilities addressed for:

Operating systems?
Network devices?
Applications?

Are there any end-of-life systems in the environment?

What is the goal with these systems?

Are exceptions documented?

Is there an approval process?

How often do we scan our networks for vulnerabilities?

Scan profiles?

Five: Are Employees Receiving Security Awareness Training?

Consistent Security Awareness Training is Essential

1 HIPAA training based on current HIPAA regulations

2 Password strength and confidentiality

3 Document destruction

4 Locking and logging off computers

5 Social engineering and phishing

6 Data loss risks (removable media, email, third-party storage sites, social media posts)

7 Acceptable use

User Education and Phishing Awareness

- Malware typically needs a helper to do its job.
- Educate users on phishing scenarios and consider internal phishing “tests” to gauge employee readiness.
- Tests should familiarize employees with common phishing scenarios as well as teach employees how to identify masked links and spoofed sender addresses.

Six: Are We Ready For a Cyber Attack?

Are We Ready?

What are we doing to prevent cyber attacks?

What will we do if we are attacked?

Have we been attacked/compromised in recent history?

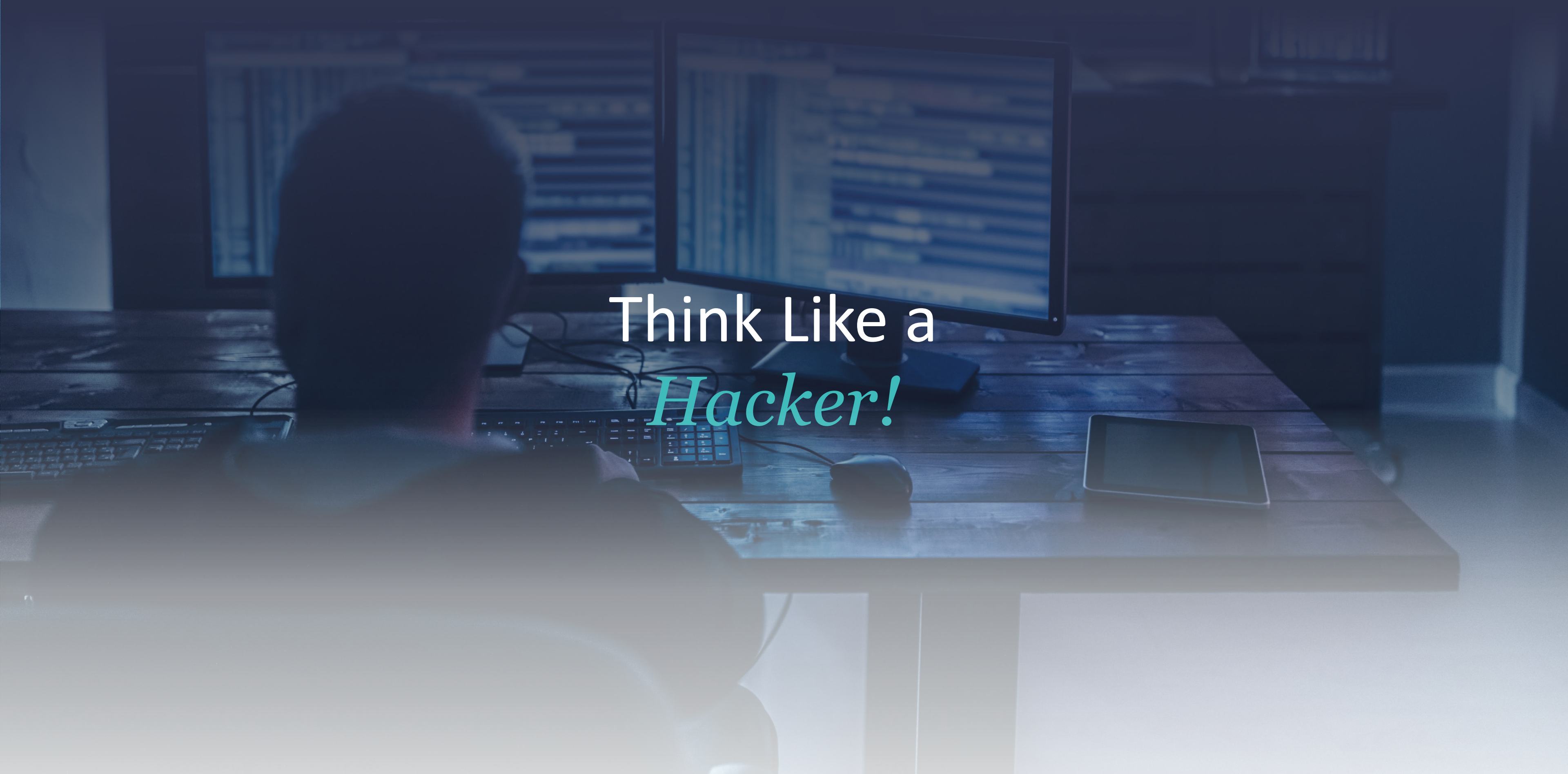
Did this result in data loss?

Polling Question

Do you believe your organization is prepared for a cyber-attack?

- Yes
- No
- Somewhat
- It is scary to think about if we are or aren't

Seven: What Could an Attacker Do in Our Environment?



Think Like a *Hacker!*

©2025 CliftonLarsonAllen LLP

Penetration Testing Uncovers Risks and…

Reveals system vulnerabilities and misconfigurations that are beyond the scope of a vulnerability scanner

Evaluates the effectiveness of security awareness training and employees' ability to detect and report social engineering attacks (email phishing, pretext phone calls)

Allows organizations to receive a “fresh look” at the network from an outside perspective that is free from internal bias

Evaluates the effectiveness of security event logging controls and mechanisms to detect/prevent suspicious activities

*Penetration testing of information systems should be performed at least annually or when major changes occur.

Eight: Do We Have an Incident Response Plan in Place?

The Incident Response Lifecycle

Preparation

Identification

Containment

Eradication

Recovery

Lessons learned

Preparation

Can we properly respond to comprehensive security incidents?

Create incident response policies

Develop roles and responsibilities

Establish communication procedures

Verify we have the correct people, process, and tools/technologies in place

Practice the Plan

- Like all emergency procedures, they need to be practiced
- Table-top exercises- simulations where participants walk through the incident and response procedures
- Two types of table-top exercises
  - Technical
  - Management
- Both types should be conducted annually

Prove the Plan

Many businesses end up over-notifying customers about data breaches, significantly increasing costs and risk of litigation

Low visibility into IT infrastructure means lack of forensic evidence to determine which system or data hackers accessed

Conduct trial forensic exercises to determine you have the proper data and visibility

Nine: How Do We Assess Third-Party Risks?

Vendor Due Diligence

How do we select and onboard vendors?

Is there an assessment of risk associated with the onboarding of vendors?

Do vendors adhere to our policies, standards, and procedures?

Do we review assessments/audits of our vendors?

Ten: Do We Have a Business Continuity and Disaster Recover Plan in Place?

Business Continuity Planning

Continuity event planning and preparedness – Business Impact Analysis (BIA) documentation

Responsibilities and communication plans

Alternate procedures for critical business processes while systems/applications and facilities are unavailable

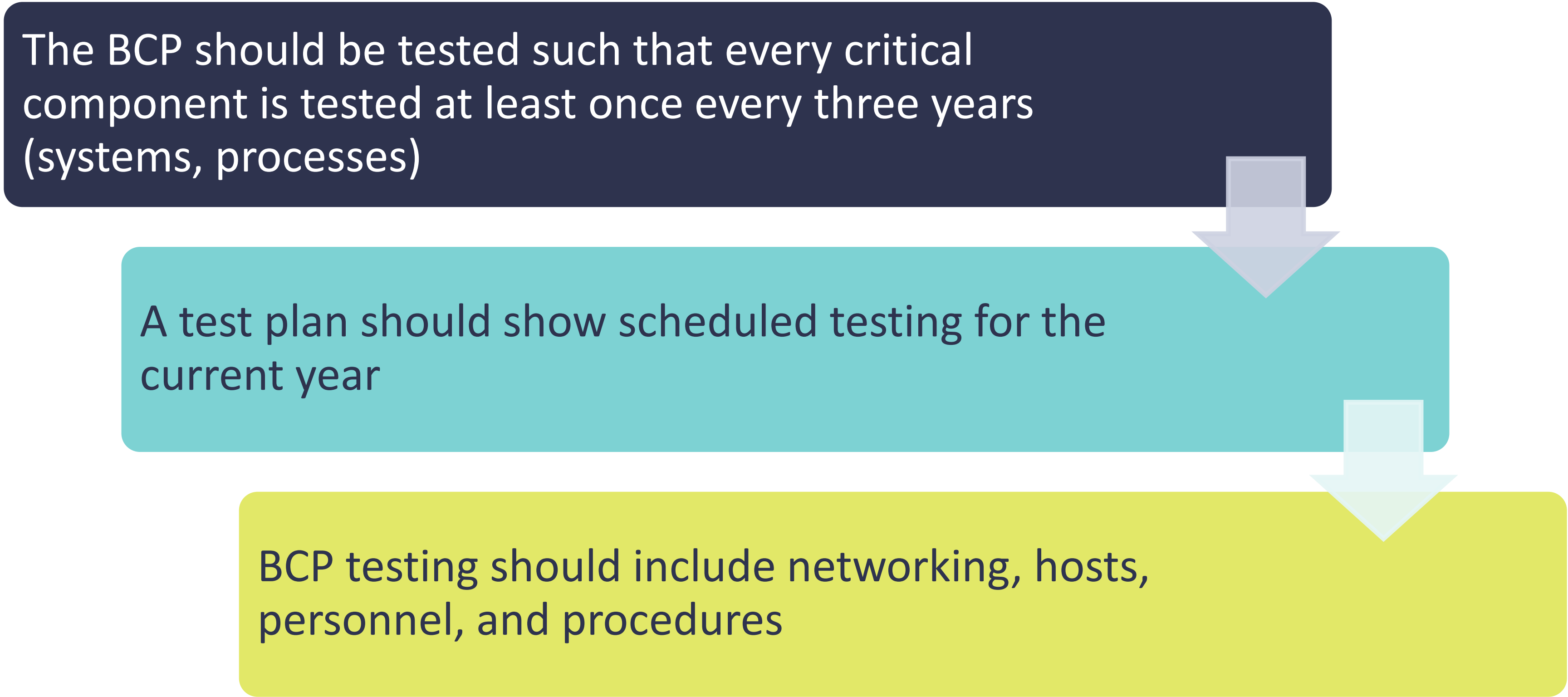
Alternate locations/facilities where work can commence during disaster situation

Recovery strategies and procedures for critical systems/applications

Continuity planning for key technology service providers and vendor-hosted systems/applications

Planning for a ______________ (pandemic)

Plan the Test and Test the Plan!



The BCP should be tested such that every critical component is tested at least once every three years (systems, processes)

A test plan should show scheduled testing for the current year

BCP testing should include networking, hosts, personnel, and procedures

Polling Question

I would like someone from CLA to contact me to discuss the following services:

- HIPAA Risk Assessment
- Penetration Testing
- Business Continuity and Disaster Recovery
- Social Engineering and Security Awareness Training
- Nothing at this time

Thank you!

Javier Young
Principal – Cybersecurity
704-816-8470
javier.young@CLAconnect.com

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS