



# 10 Cybersecurity Questions your Healthcare Organization Should be able to Answer!

Javier Young, CISSP, MBA  
Principal, Cybersecurity Services Group  
CLA (*CliftonLarsonAllen LLP*)

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

# Disclaimer

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.



# About CLA



CLA exists to create opportunities for our clients, our people, and our communities through industry-focused wealth advisory, digital, audit, tax, consulting, and outsourcing services.

With more than 8,500 people, 130 U.S. locations, and a global vision, we promise to know you and help you. For more information visit [CLAconnect.com](https://CLAconnect.com).

CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See [CLAglobal.com/disclaimer](https://CLAglobal.com/disclaimer). Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.



# Learning Objectives

## Recognize

- Recognize the top questions a healthcare organization should be able to answer with respect to cybersecurity

## Identify

- Identify the current state of cybersecurity maturity at an organization

## Understand

- Understand the importance of proactive cybersecurity endeavors.





# 1. Do we have a Formal Information Security Program in Place?

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

# 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





## 2. What Data is Important to our Organization?

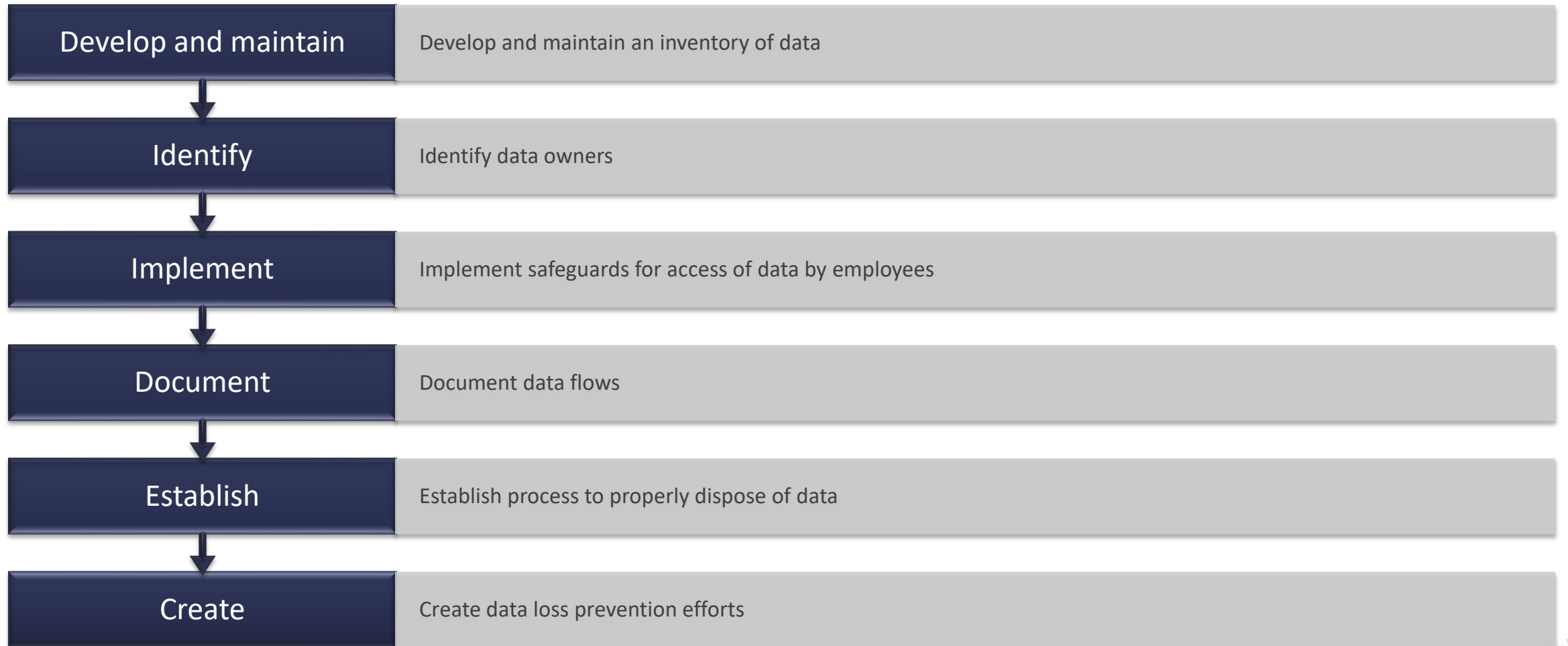
*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.



# Data Protection



# Data Classification



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

Public  
Internal Use  
Confidential



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 ensure that they have off-line copies of backup and restore files available



Backup and restore files should be saved in well secured location



Perform a thorough review of file permissions for network file shares



Test the restoration of your data





3. When was our last HIPAA  
Risk Assessment or Security  
Audit performed?

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

# 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 (cont.)



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.



## 4. How are Vulnerabilities Managed at the Organization?

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

# Vulnerability Management



How are vulnerabilities documented?



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?







## 5. Are Employees Receiving Security Awareness Training?

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

# Consistent Security Awareness Training is Essential

HIPAA training based on current HIPAA regulations

Password strength and confidentiality

Document destruction

Locking and Logging Off Computers

Social Engineering and Phishing

Data Loss Risks (Removable Media, Email, Third-Party Storage Sites, Social Media Posts)

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.





## 6. Are we Ready for a Cyber Attack?

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

# 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?





## 7. What Could an Attacker do in our Environment?

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

# Think like a Hacker!



# 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.







## 8. Do we have an Incident Response Plan in Place?

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

# 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

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

# Practice the Plan

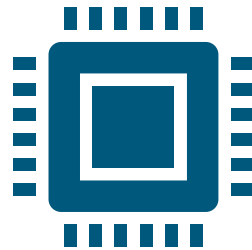
- Like all emergency procedures, they need to be practiced
- Table-top exercises- simulations where participants walk through the incident and response procedures
- Two types of table-top exercises
  - Technical
  - Management
- Both types should be conducted annually



# 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 ensure you have the proper data and visibility



## 9. How do we Assess Third-Party Risks?

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

# 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?



# 10. Do we have a Business Continuity and Disaster Recover Plan in Place?

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.



# Business Continuity Planning

---

Continuity event planning and preparedness

---

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)



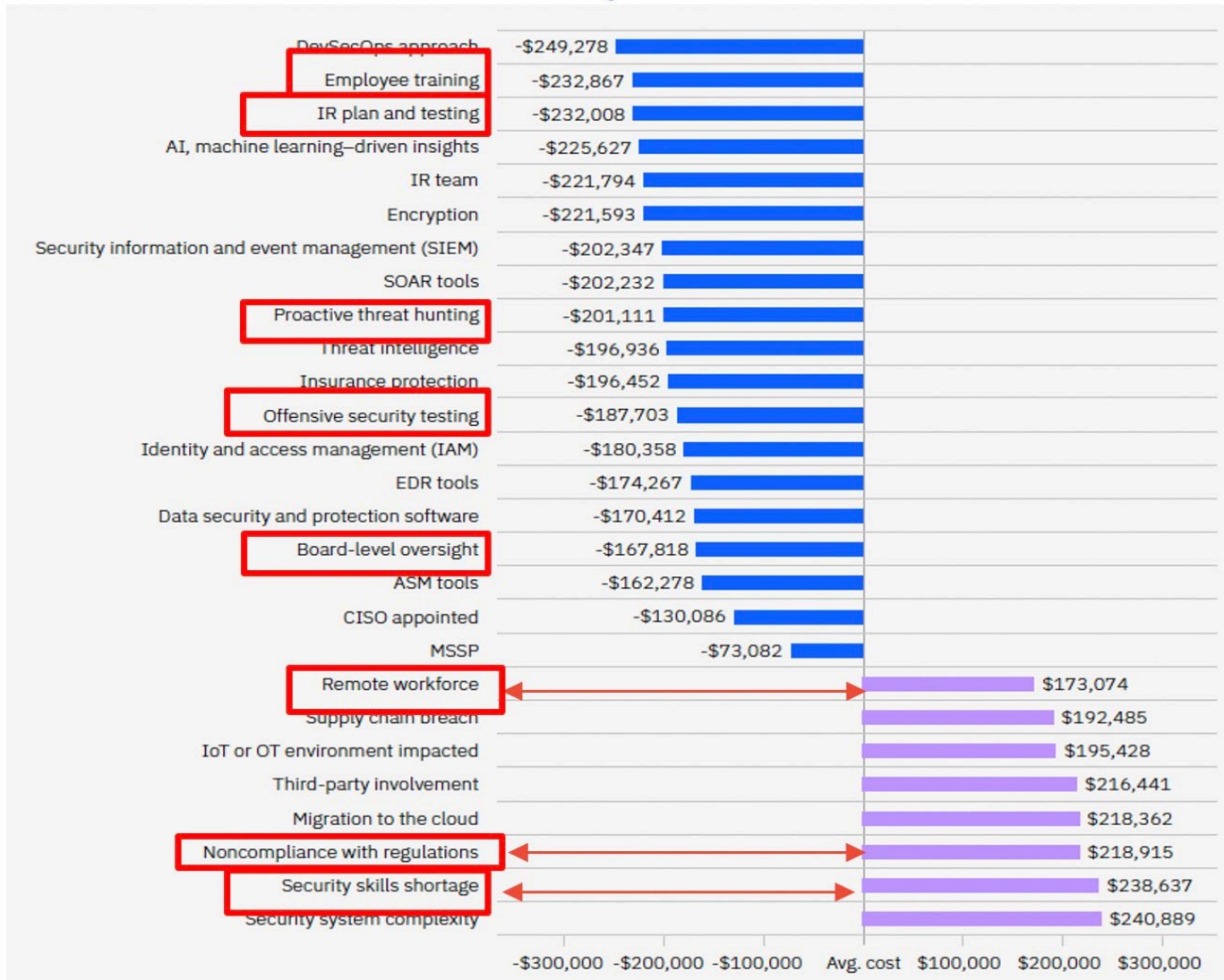
A test plan should show scheduled testing for the current year



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



# Incident Response Preparedness- Cost Savings



The impact of 27 factors on the average cost of a data breach

\$10.93 Million – The average cost of a data breach in the Healthcare industry in the US



Source: IBM Security Cost of a Data Breach Report 2023



Thank You!

Javier Young  
Principal – Cybersecurity  
704-816-8470  
Javier.Young@claconnect.com

*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

©2022 CliftonLarsonAllen LLP. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.