We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

10 Cybersecurity Questions Your Organization Should Be Able to Answer!

March 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.

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.

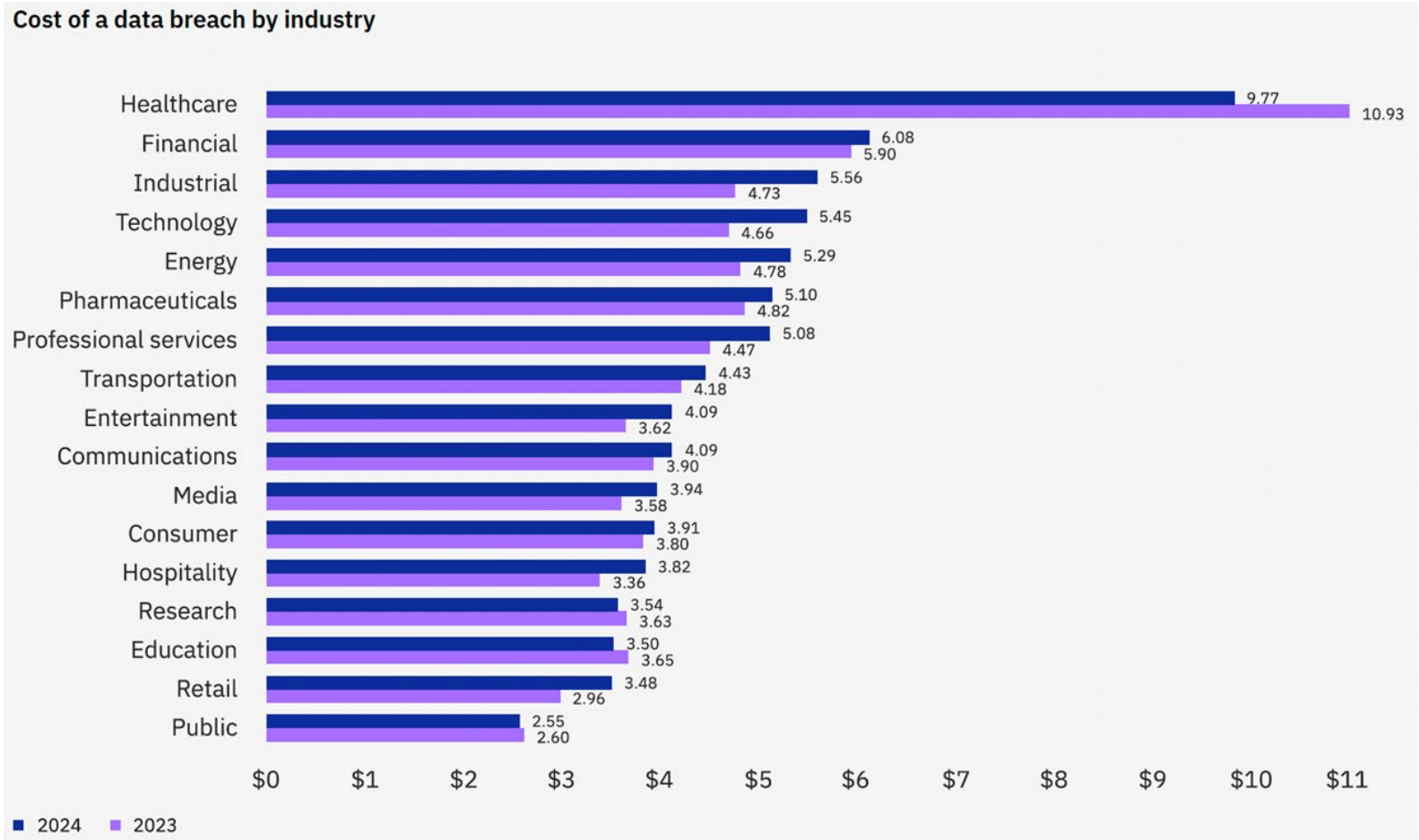
With nearly 9,000 people, 130 U.S. locations, and a global vision, we promise to know you and help you. For more information visit CLAconnect.com.

Learning Objectives

At the end of this session, you will be able to:

- Recognize common threats and social engineering techniques
- Identify online behaviors that can lead to increased exposure
- Recall where the organization can focus valuable risk mitigation resources
- Discuss how to develop and refine a framework of knowledge to plan future security efforts

The Why



Source: IBM Security Cost of a Data Breach Report 2024

1. Do We Have a Formal Information Security Program in Place?

The importance of information

The need to protect information

The Information Security Program Should Establish

Roles and responsibilities

Enforcement of policies

Policies, Standards, and Procedures

Network and system policies

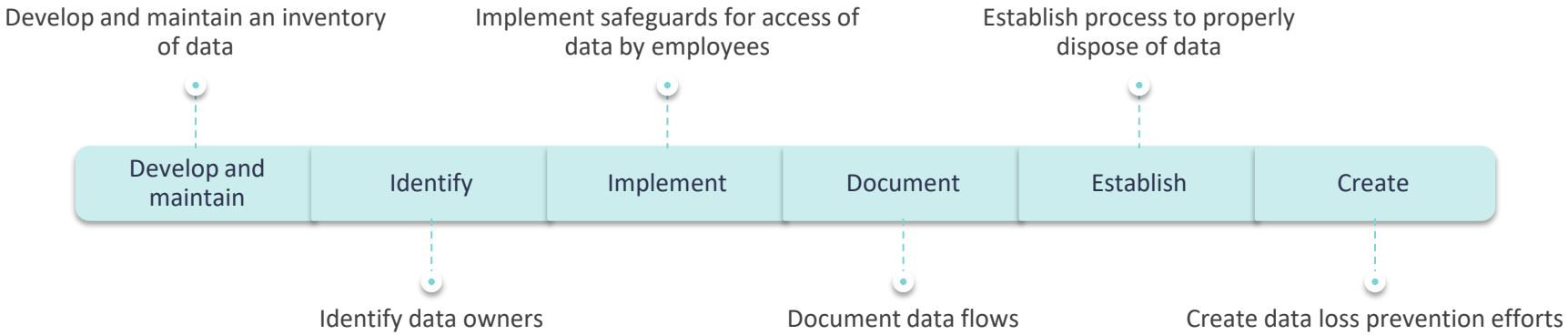
- Logging and monitoring of security events
- Remote access
- Wireless networking
- Patch management
- Firewall management
- Antivirus management
- Intrusion detection/prevention

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?

Data Protection



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 confirm 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

3. When Was Our Last Compliance or Security Audit Performed?

Compliance and Operational Frameworks

Regulatory, Contractual, and Operational frameworks require regular/periodic assessments

- GLBA, FERPA, HIPAA, NERC/CIP, State Laws --- Regulatory
- PCI – DSS, CMMC --- Contractual
- CIS Critical Controls, NIST Standards, HITRUST --- Operational standards

- These all have defined expectations for system settings, controls, operational procedures, and independent testing, assessment and reporting.

In nearly every case, these frameworks require independent testing at least annually.

IT Systems are changing under the covers all the time: security patches, features updates, user roles and permissions, etc…

Independent security assessments should validate adherence to standards and expectations and shine a light on risks related to exceptions.

Annual Security Assessments

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

4. 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?

5. Are Employees Receiving Security Awareness Training?

Consistent Security Awareness Training is Essential

1. _____ training based on current _____ requirements
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.

6. Are We Ready For a Cyber Attack?

Are We Ready?

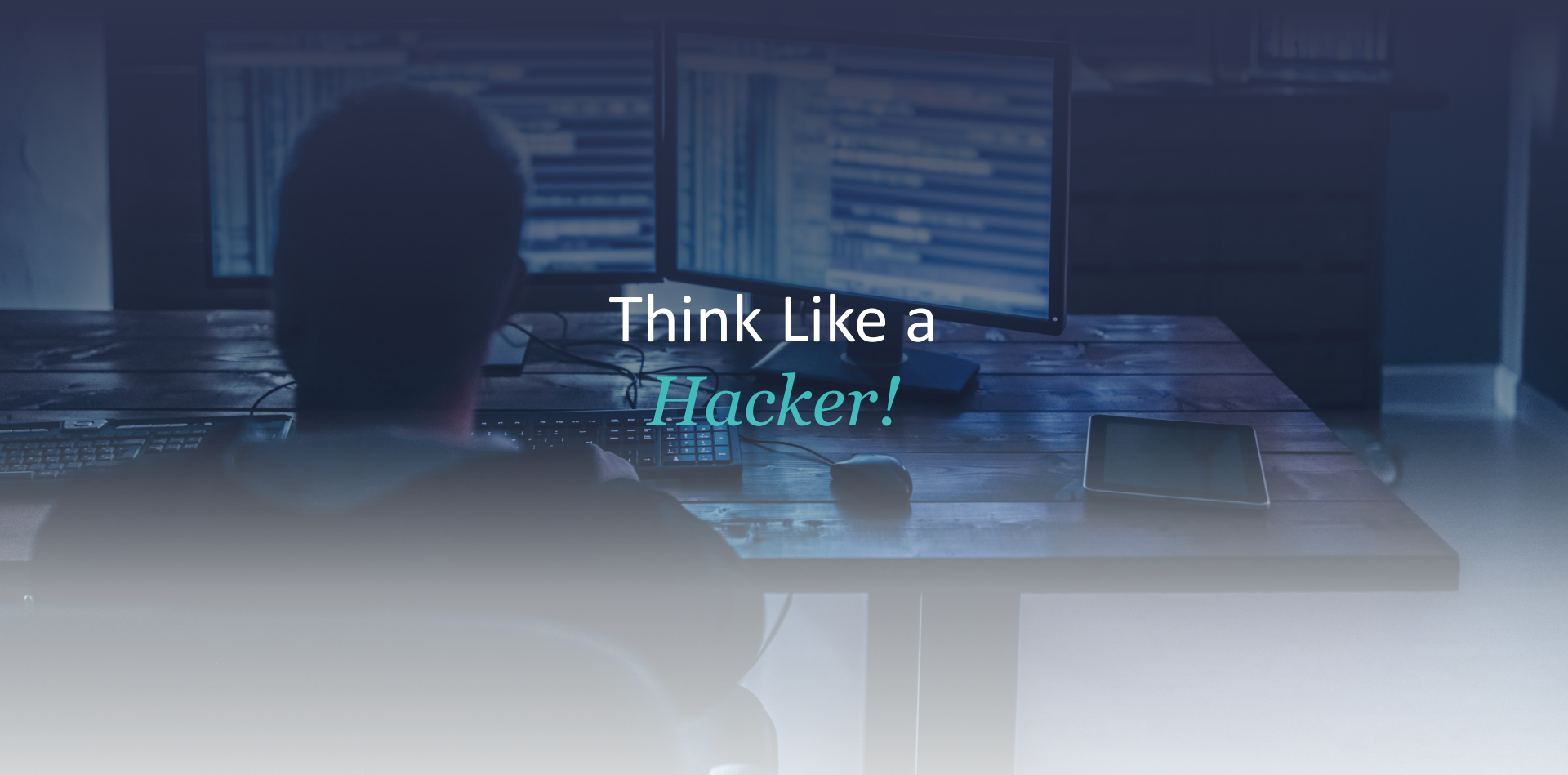
What are we doing to prevent cyber attacks?

What will we do if we are attacked?

Have we been attacked/compromised in recent history?

Did this result in data loss?

7. What Could an Attacker Do in Our Environment?



Think Like a *Hacker!*

Penetration Testing Uncovers Risks and…

Reveals system vulnerabilities and misconfigurations that are beyond the scope of a vulnerability scanner; validates effectiveness of monitoring, logging and alerting

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

Red Team/Black Box/Adversarial Simulations test the systems and the staffs “recognize, react, and respond capabilities”

*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?

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

9. 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?

10. 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

Incident Preparedness Cost Savings

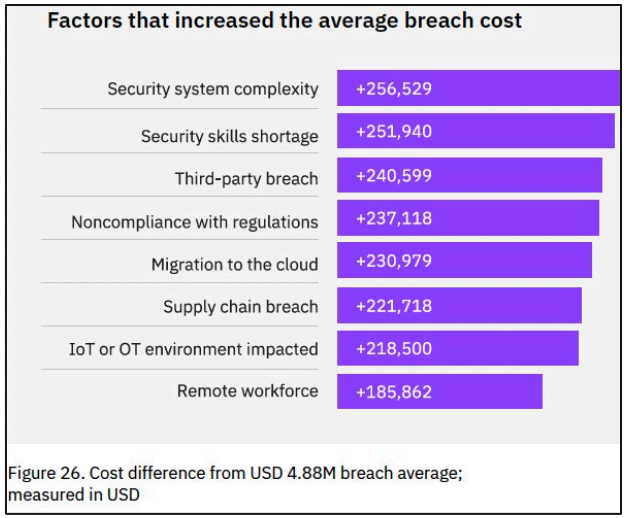


Figure 26. Cost difference from USD 4.88M breach average; measured in USD

Source: IBM Security Cost of a Data Breach Report 2024

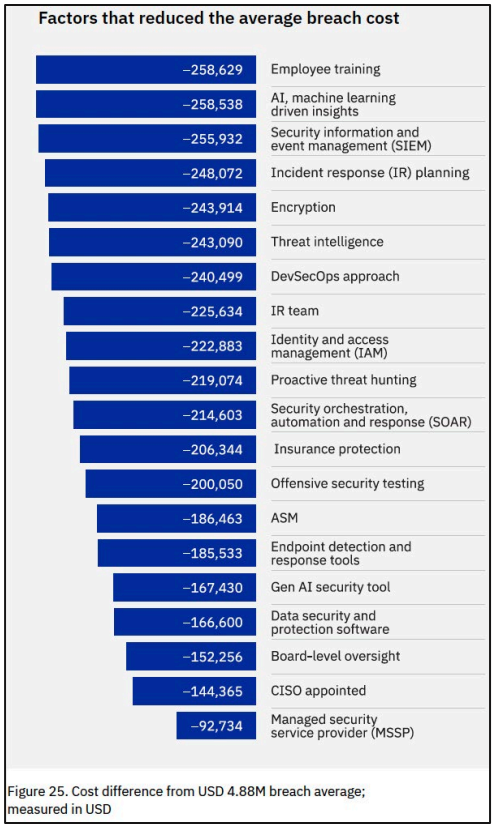


Figure 25. Cost difference from USD 4.88M breach average; measured in USD

- Global Average cost is $3.5M
- The impact of 28 factors on the average cost of a data breach

Thank you!

Randy Romes
CISSP, CRISC, CISA, MCP, PCI-QSA, MEd
Principal – Cybersecurity
612.397.3114
randy.romes@claconnect.com

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS

Resources

- CLA Cybersecurity Services:
  - https://www.claconnect.com/en/services/information-security
- CLA Digital Services:
  - https://godigital.claconnect.com/
- IBM Annual Data Breach Report
  - https://www.ibm.com/reports/data-breach
- Center for Internet Security – Critical Controls Resources
  - https://www.cisecurity.org/controls

CLA – A Professional Services Firm

A professional services firm with five distinct business lines

- Audit
- Tax
- Outsourcing
- Wealth Advisory
- Digital

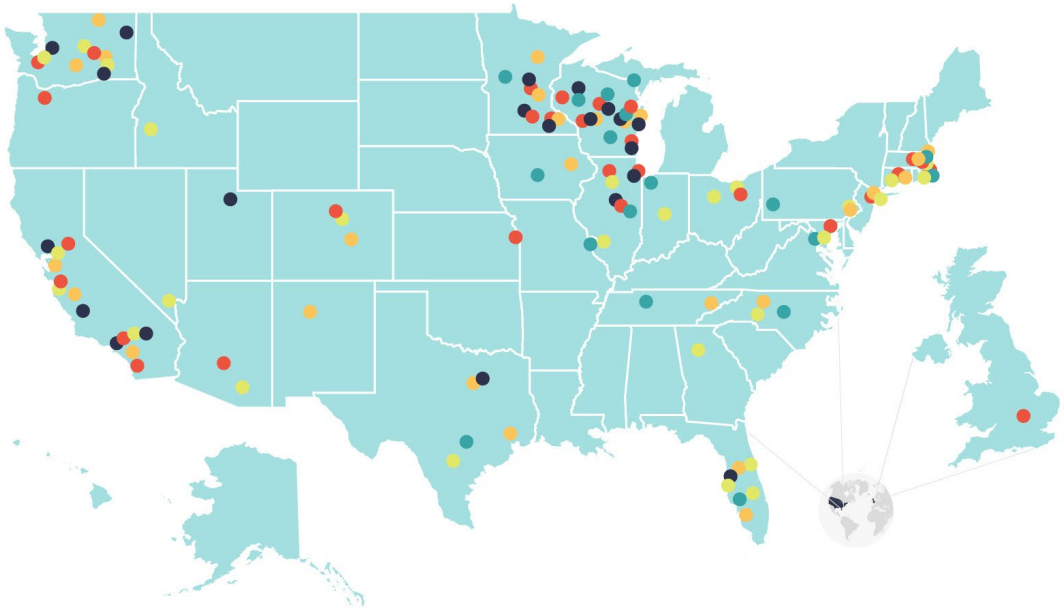
9,000
NEARLY 9,000 PEOPLE

130+
LOCATIONS

AN INDEPENDENT NETWORK MEMBER OF
CLA Global

CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.



Cyber Security Services At CLA

Information Security offered as specialized service offering for over 25 years

- Penetration Testing and Vulnerability Assessment
  - Black Box, Red Team, and Collaborative Assessments
- IT/Cyber security risk assessments
- IT audit and compliance (HIPAA, GLBA/FFIEC, NIST, CMMC, CIS, etc.)
- PCI-DSS Readiness and Compliance Assessments (PCI-DSS)
- Outsourced Information Security Advisory
- Incident response and forensics
- Independent security consulting
- Remediation assistance
- Internal audit support

CLA Cybersecurity Helps Clients

Governance, risk, and compliance

Risk assessments
IT controls assessments (NIST, CIS, etc.)
Policy development
Compliance assessments (PCI, GLBA, HIPAA, etc.)

Security testing

Penetration testing
Vulnerability assessments
Social engineering (phishing, phone calls)
Computer forensics

Scan here to learn more!