ACUA Webinar

10 Cybersecurity Questions Your Organization Should be Able to Answer

06/26/2025

Virtual Learning Committee

Director
Wendee Shinsato, CPA, CIA
Assistant Vice Chancellor
California State University

Volunteer
Christiana Oppong, CIA, CCSA
Senior Auditor
Princeton University

Volunteer
Brenda Auner, CIA, CFE
Senior Auditor
California State University

Volunteer
Virginia L. Kalil, CIA, CISA, CFE, CRISC
Chief Internal Auditor
University of South Florida

10 Cybersecurity Questions Your Organization Should Be Able to Answer

ACUA 2025

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

Recognize where the organization can focus valuable risk mitigation resources

Recall the ways to develop and refine a framework of knowledge to plan future security efforts

The Why

Cost of a data breach by industry

Industry	2024	2023
Healthcare	9.77	10.93
Financial	6.08	5.90
Industrial	5.56	4.73
Technology	5.45	4.66
Energy	5.29	4.78
Pharmaceuticals	5.10	4.82
Professional services	5.08	4.47
Transportation	4.43	4.18
Entertainment	4.09	3.62
Communications	4.09	3.90
Media	3.94	3.58
Consumer	3.91	3.80
Hospitality	3.82	3.36
Research	3.54	3.63
Education	3.50	3.65
Retail	3.48	2.96
Public	2.55	2.60

■ 2024 ■ 2023

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

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 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

Polling Question #1

Organizations should strive to have at least 3 levels of data classifications (Confidential, Internal, and Public)?

True	False

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?

Polling Question #2

Organizations should strive to remediate High Risk vulnerabilities within 7 days?

True

False

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?

Polling Question #3

Penetration test is a simulated cyberattack to identify and exploit vulnerabilities before real attackers can?

True

False

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?

How do we select and onboard vendors?

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

Vendor Due Diligence

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

Do we review assessments/audits of our vendors?

Polling Question #4

Requesting penetration test reports from a vendor is the standard way of assuring that a vendor has implemented security controls?

True

False

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)
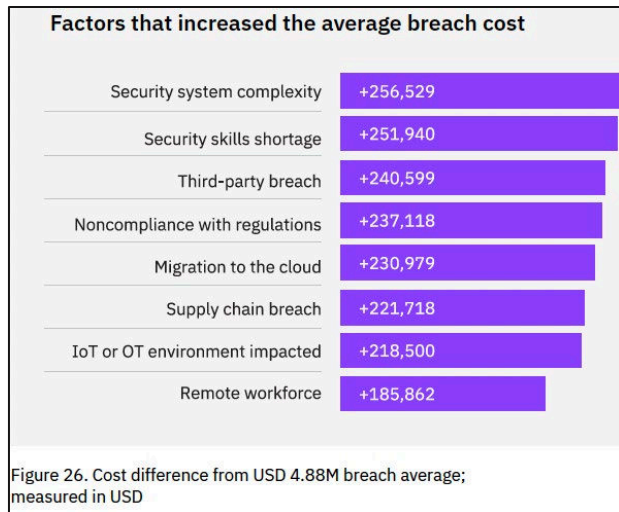
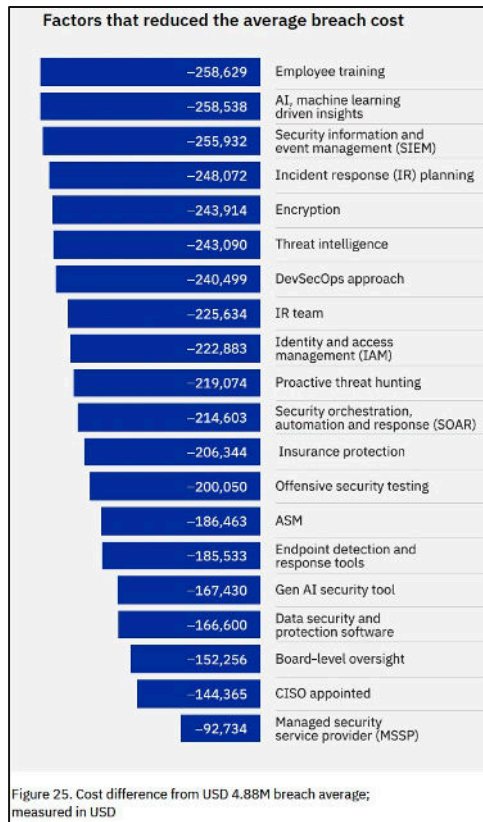A test plan should show scheduled testing for the current year

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

Incident Preparedness Cost Savings

Factors that increased the average breach cost

Factor	Cost
Security system complexity	+256,529
Security skills shortage	+251,940
Third-party breach	+240,599
Noncompliance with regulations	+237,118
Migration to the cloud	+230,979
Supply chain breach	+221,718
IoT or OT environment impacted	+218,500
Remote workforce	+185,862

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

Source: IBM Security Cost of a Data Breach Report 2024

Factors that reduced the average breach cost

Cost	Factor
−258,629	Employee training
−258,538	AI, machine learning driven insights
−255,932	Security information and event management (SIEM)
−248,072	Incident response (IR) planning
−243,914	Encryption
−243,090	Threat intelligence
−240,499	DevSecOps approach
−225,634	IR team
−222,883	Identity and access management (IAM)
−219,074	Proactive threat hunting
−214,603	Security orchestration, automation and response (SOAR)
−206,344	Insurance protection
−200,050	Offensive security testing
−186,463	ASM
−185,533	Endpoint detection and response tools
−167,430	Gen AI security tool
−166,600	Data security and protection software
−152,256	Board-level oversight
−144,365	CISO appointed
−92,734	Managed security service provider (MSSP)

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!

Andy Lee, CPA
Principal – Higher Education
267-419-1122
andrew.lee@CLAconnect.com

Zoran Jovic
Manager – Cybersecurity
813-384-2728
zoran.jovic@CLAconnect.com

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS

Resources

- CLA Cybersecurity Services:

  o https://www.claconnect.com/en/services/information-security

- CLA Digital Services:

  o https://godigital.claconnect.com/

- IBM Annual Data Breach Report

  o https://www.ibm.com/reports/data-breach

- Center for Internet Security – Critical Controls Resources

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

Cyber Security Services at CLA

Information Security offered as specialized service offering for over 25 years

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

Penetration Testing

CLA has been providing penetration testing and vulnerability assessment services for over 25 years. These services rely on a combination of tools that are developed internally by CLA cybersecurity professionals, as well as open-source and commercially available software. Our professionals are constantly on the lookout for new tools and tactics to continually enhance their capabilities. Engagement projects can range from highly collaborative to Red Team assessments designed to mimic true adversaries to assess response capabilities.

Penetration Test Goals	Examples
Penetration Testing, executed in a collaborative manner, to identify exploitable vulnerabilities in the environment and gauge the impact the vulnerabilities have to the organization.	Application / API Penetration Test External Penetration Test Internal Penetration Test Social Engineering Wireless Network Penetration Test
Penetration Testing used to evaluate logging and monitoring capabilities; or used to evaluate your ability to recognize, react, and respond.	Purple Team collaborative assessments Red Team covert assessments
Penetration Testing used to satisfy regulatory or compliance requirements.	Various compliance frameworks and regulatory bodies require or recommend penetration testing, including GLBA, FFIEC, FTC, HIPAA, and PCI.

"Penetration Testing is a process. It can be applied to any system, application, or network. What's important is to define the organization's goals and objectives."

Contact us to learn more:

https://www.claconnect.com/en/services/information-security/

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS

Announcements

Upcoming ACUA Webinars – Save the Date!

Month	Date & Time	Presenter	Topic
July 2025	7/24/25 – 1:00 PM EDT	Workiva	Tech Meets Talent in Internal Audit

Do you have an idea for a webinar? Contact the VLC director at wshinsato@calstate.edu

ACUA
Association of College
& University Auditors

Get Involved

Become a Volunteer	Nominate your Colleagues for an ACUA Award	Submit a Conference Proposal
Present a Webinar	Become a Mentor	Write an Article for the College & University Auditor
Write a Kick Starter	Post on Connect ACUA	Share, Like, Tweet & Connect on Social Media

Join us for an upcoming webinar