We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Cybersecurity Trends – Impacts on Controls and Audits

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.

Jim Kreiser, Principal – CRMA, CISA, CFSA

CLA – National Leader, State and Local Government, IT and Risk Services

Ashley Budd, Senior – CISA, CCSFP, CHQP

Learning Objectives

- Current Cybersecurity Landscape
- Review Trends
- Explain Ransomware, Data Exfiltration, and Other Attacks
- Cyber Security Preparedness and Controls
- Describe Controls and Risk Management strategies
- Importance of Vendor Risk Management
- Discuss Auditing Impacts and Related Risk
- Closing Remarks

Current Cybersecurity Landscape

Cybersecurity Landscape in 2025

- Governments are a top target for cybersecurity threats and breaches. According to a study from the Advanced Cybersecurity Management Institute (ACSMI), Government is a top 3 affected industry of cyber attacks.

- Municipal and state level agencies are the main government targets for politically motivated or financially driven bad actors. Systems such as voting systems, licensing portals, and emergency service networks are known to run legacy software and require inter-agency coordination for remediation efforts.

- Study from the Federal Bureau of Investigation shows a 33% increase in losses from internet crimes from 2023 to 2024.

Cybersecurity Data Breach – By the Numbers

2025 Cost of a Data Breach study conducted by the Ponemon Institute noted:

$10.22m	**Average cost of a data breach in the United States** ➢ Global average $4.44
1-in-6	Number of breaches involving AI-driven attacks
+$131,212	Additional cost per breach (avg.) due to remote workforce
53%	Breaches that included records containing Customer PII ➢ Average cost of $160 per record

Headlines

Microsoft SharePoint exploits – incident involved zero-day attacks on on-premises SharePoint servers. Ransomware was deployed and sensitive information was accessed. Included U.S. federal and state agencies.

TeleMessage breach – flaw involved missing end-to-end encryption, allowing attackers to intercept information on the messaging platform used by U.S. government officials. Included breaching content on national security.

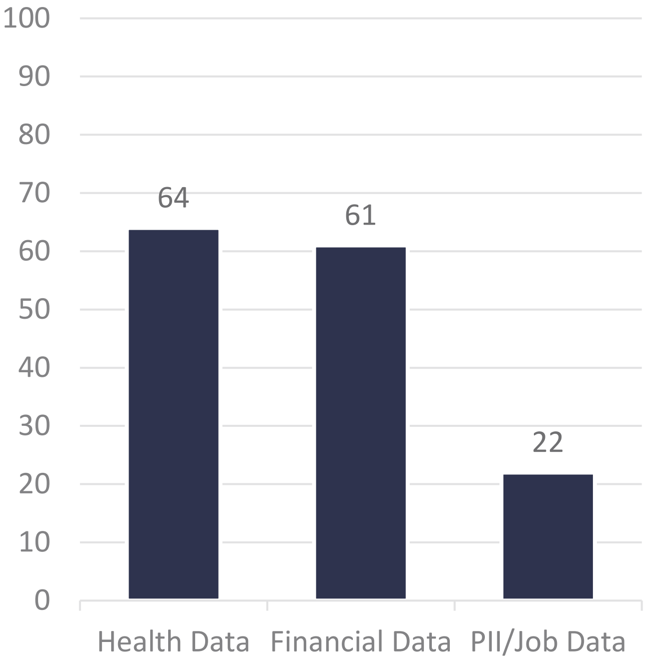
Cleo Communications breach – zero-day vulnerabilities exploited, affecting users of the file transfer platform, including Hertz. Credit card, driver's license, social security numbers, passport, and Medicaid/Medicare information was breached. Affected over 3,000 Maine residents.

What About These Headlines?

- **Rhode Island** – RIBridges System hit with ransomware. Went undetected for 6 months until Brain Cipher posted stolen data on their leak site.
- **Minneapolis Park and Recreation** – Ransomware after initial access through phishing and credential theft. Caused system-wide phone outages. Still working to determine what data may have been impacted.
- **Hoboken, New Jersey** – Ransomware attack forced the closure of City Hall and suspended all online municipal systems. PHI and PII stolen. Full scope still under investigation.
- **White Lake Township, Michigan** – Cyberattack likely occurred due to business email compromise (BEC) or vendor impersonation. Portion of the $29 million in infrastructure bond funds was compromised. New financing needed to be pursued.
- **Pennsylvania Office of Attorney General** – Cyber incident due to Citrix vulnerability. Website went offline and email and land lines were disabled. Data loss or breach is unconfirmed.

Virtual Culture

- The Pew Research Center states that 64% of users accessed information about their health conditions on a mobile device. In addition, 61% use mobile devices for online banking, while 22% have submitted a job application on their smartphone.



Mobile Apps – The Risk

Data – For many of us, our phone contains the most information about us.

Banking, credit cards, healthcare, social media, email, photos, etc.

Size – A smartphone can be easily lost or stolen. Even though mobile operating systems require setting a password by default, some users choose not to have one.

Privacy – Phones are clearly more than just phones with GPS, 4k cameras, digital assistants listening, and connections to your whole life.

Ex: Third-party keyboards - Apple/Google cannot control what the keyboard developers do with keystroke data.

Trends and Analysis

What Do We Know?

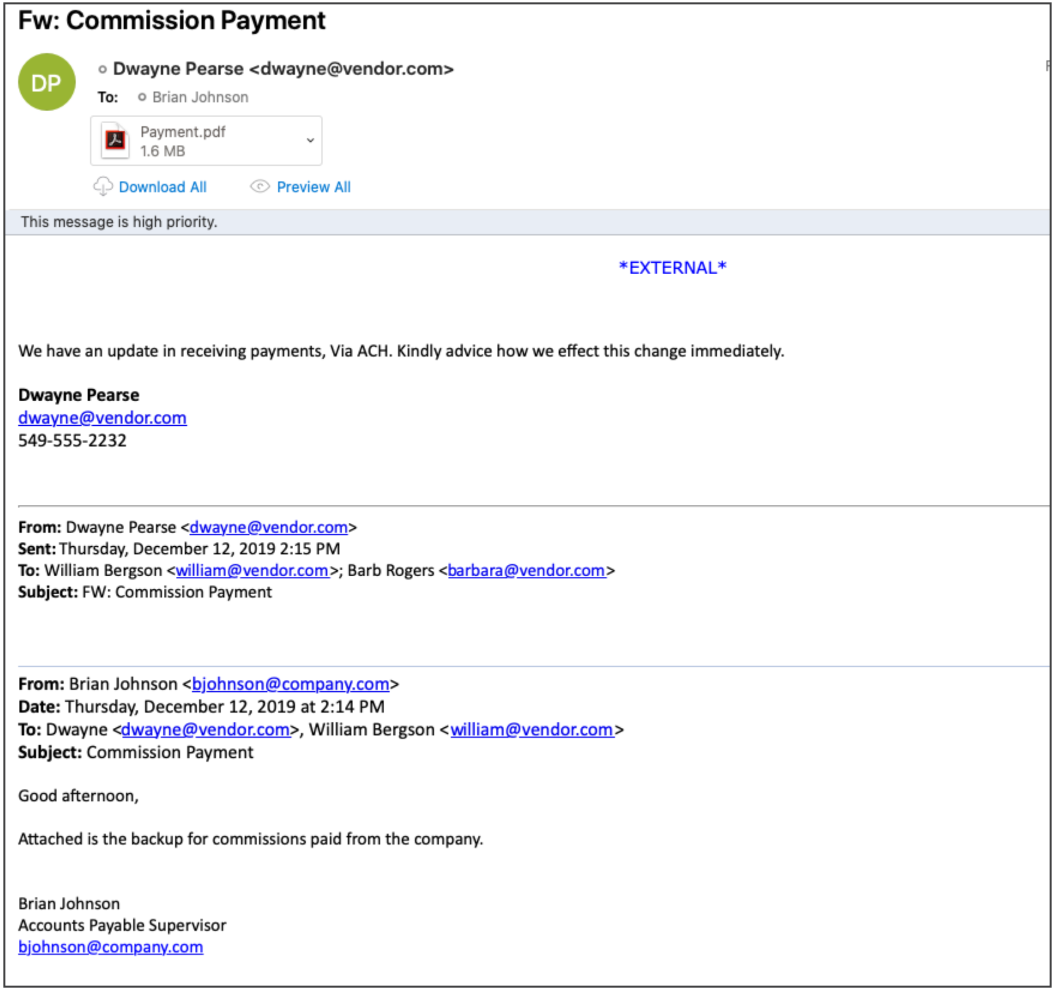
- It is reported in several studies, that as much as 34% of state and local government organizations were victims of ransomware attacks. Most studies put governments as a top 3 target of cyberattacks, and one of the largest growing sectors of breaches and attacks.

- Of attacks on “public sector” (nonprofit and government), 66% or more are reported to be a result of phishing attacks (Verizon DBIR).

- Cybercrime is increasing at an alarming rate. Many studies report different metrics and rates of growth. Cost of recovery from attacks nearly doubled in 2024, with average costs reaching $2.83 million (Sophos).

Business Email Compromise (BEC)

- Fraudsters impersonate employees or vendors via email to steal money or data
  - Fake vendor invoice
  - Exec asks staff to “buy gift cards”
  - Update direct deposit account
  - Etc.
- Malware often not needed
- Mainly a form of social engineering
- IC3 reported $2.9 billion in losses in 2023 alone



Fw: Commission Payment

Dwayne Pearse <dwayne@vendor.com>

To: Brian Johnson

This message is high priority.

EXTERNAL

We have an update in receiving payments, Via ACH. Kindly advice how we effect this change immediately.

Dwayne Pearse
dwayne@vendor.com
549-555-2232

From: Dwayne Pearse <dwayne@vendor.com>
Sent: Thursday, December 12, 2019 2:15 PM
To: William Bergson <william@vendor.com>; Barb Rogers <barbara@vendor.com>
Subject: FW: Commission Payment

From: Brian Johnson <bjohnson@company.com>
Date: Thursday, December 12, 2019 at 2:14 PM
To: Dwayne <dwayne@vendor.com>, William Bergson <william@vendor.com>
Subject: Commission Payment

Good afternoon,

Attached is the backup for commissions paid from the company.

Brian Johnson
Accounts Payable Supervisor
bjohnson@company.com

Ransomware

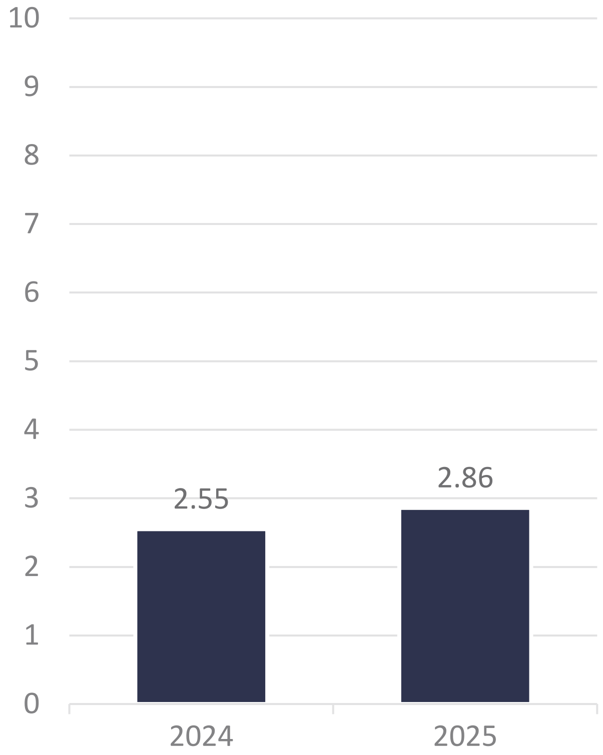
- Attack on the **availability** of data
- Payments are often in Bitcoin
- Cyber criminals attempt to delete backups
- Newer variants also demand payment not to publish stolen data (DOUBLE TAP)

Recent Sophos Study

- 59% of companies were hit with ransomware
- 50% paid the ransom

Breach Identification and Containment

- Global average is 277 days
  - 207 days to identify a breach
  - 70 days to contain the attack
- Average cost to recovery from a breach for the public sector (government) is $2.86 million



Behind the Statistics

Hackers can do a lot in and to your network in 207 days (Global Average)

- Learn everything about your business
- Find you crown jewels and take them
- Disable backups and security systems
- Create numerous back doors

Labeling ransomware as the top threat creates a false narrative

- Ransomware is usually coupled with other acts and just the most visible part of the attack
- Ransomware is a version of malware. The vector/delivery is the same/similar.
- Ransomware is coupled with data exfiltration
- Resuming operations is just the first step
- Legal and business ramifications of a data breach can persist

Control Practices

How do we start taking actions and steps to mitigate?

Preparedness

What can organizations do to prepare themselves for a potential cyber attack?

- What standards will we follow? NIST, ISO, CMMC
- Is there an IT Risk Assessment and Threat/Vulnerability analysis?
- Incident response plan?
- Action plans to harden and implement controls/tools
- Training and communication

Awareness

What is the importance of user education and testing?

- What does your organization do? Phishing? What follow-up? Email blasts? Are these effective?
- Remember stats? 66% through phishing – that's us!
- Phishing, testing, and awareness are critical. We all are the front line – and stats show we are failing.

Simple Fixes

- Are we willing to take additional steps as an organization?
- No local administrator rights
- Personal email and web filtering restrictions
- Privileged user account separations/logging
- Restrict USB drives
- Prevent zip file attachments

- *IT can implement quickly and for little cost. Are we willing to adjust and adapt?*

Securing Your Remote Workforce

Organization Connectivity

- Ensure the connection is secure (i.e. disallow use of public Wi-Fi)
- Restrict remote access to only those **needed timeframes** (business hours or current network time restrictions)
- **MFA** required on any type of access
- Monitoring capability for remote access communications as well as the ability to **disable quickly** if an issue arises
- Capability to log remote access communications (including date, time, user, user location, duration, and activity), analyze logs in a timely manner, **updated IDS and firewall alerts**, and follow up on anomalies.
- Strong **encryption** on all communications (SSL or TLS 1.2 or higher)

Securing Your Remote Workforce

Organization-owned Devices

- Company owned devices should be encrypted if they can contain sensitive data
- Application **whitelisting** on company-owned devices
- Ensure support/functionality for all other in-office security/technology like patch management including antivirus/antimalware updates, vulnerability scanning, event logging/collection, etc.

Trends to Consider

Mice and Keyboards Vulnerable to "MouseJack“

- The path can be used to gain administrative privileges

Visitors to hotels, coffee shops and malls often connect to the free WiFi on offer, but various studies have shown that care is not always taken when connecting.

- Hackers can easily set up fake WiFi access points, often using the name of the establishment in the SSID name.
- Everything users do could be monitored by cybercriminals.
- May have a stronger WiFi signal, which may see more people connect to it but it is an “evil twin” through which man in the middle attacks occur.
- One study indicated more than a third of WiFi hotspot users take no precautions when accessing WiFi hotspots.

Incident Response Preparedness

- Unfortunately, data breach can still occur despite implementing all the best security precautions

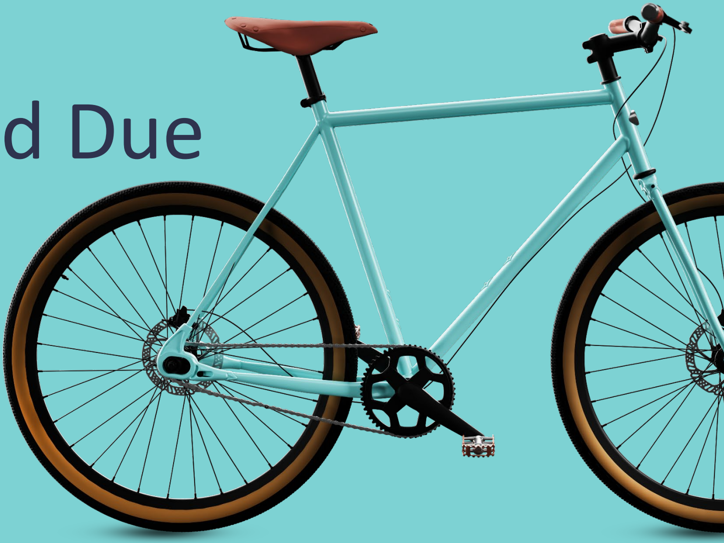
- When that occurs, organizations need to ensure they are ready to respond to a data breach.

Have a plan, practice the plan, prove the plan

Incident Response Planning

- Develop an incident response plan
  - Include the appropriate procedures
  - Ensure points of contact are included
  - Keep the plan update to date
- Establish relationships with key incident responders
  - Breach Counsel
  - Forensic provider
  - Public relations

Risk Assessment and Due Diligence Practices



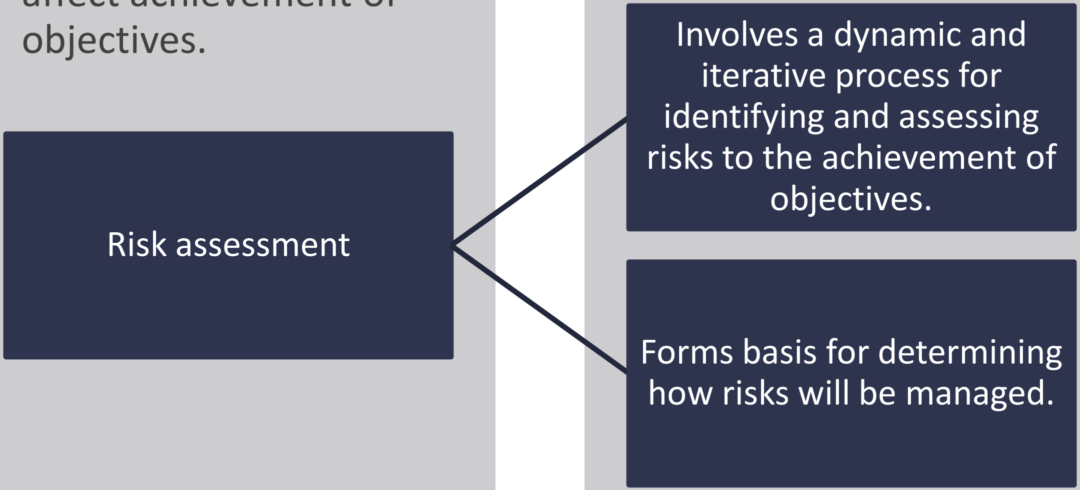
What is Risk Assessment?

Risk

- Possibility that an event will occur and adversely affect achievement of objectives.

Precondition to risk assessment

- Establishment of objectives, linked at different levels of the entity.



Risk assessment

Involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives.

Forms basis for determining how risks will be managed.

Vendor Contract and Reporting Considerations

- **Performance Clauses**
- Protection Clauses
- Scope
- Subcontractors
- Duration
- Fees
- **Right to Audit**
- Compliance
- **Confidentiality and Security**
- **Business Continuity**
- Insurance
- Warranties
- Indemnification
- Modification
- **Termination**

Vendor Due Diligence/Risk Assessment

How to use a SOC report to gain insight into a potential vendor:

- If the vendor is processing any data or storing any data on your behalf – request a SOC report.
- Look for “carve-outs” to determine what they are outsourcing.
  - May need to request additional SOC reports.
  - Example: Managed IT solutions outsourcing their Data center
- Determine the period covered (Type 1, Type 2)
- Make sure your specific service is covered.
  - Application Service Providers (ASPs) have many software solutions but may not include them all in their SOC report

Vendor Performance Clauses - Example

Service Level Agreements / Key Performance Indicators

- Example: Vendor will achieve and maintain a customer satisfaction rating of not less than 75% each calendar quarter

Availability

- Example: Product/service will be fully functional not less than 98% per day/month/quarter excluding standard maintenance periods

Reporting

- Outline all reports needed from vendor (e.g. SOC, monthly metrics, etc.).
- Include type and frequency of reports needed (performance, security, business continuity, etc.) and specific information to be included.

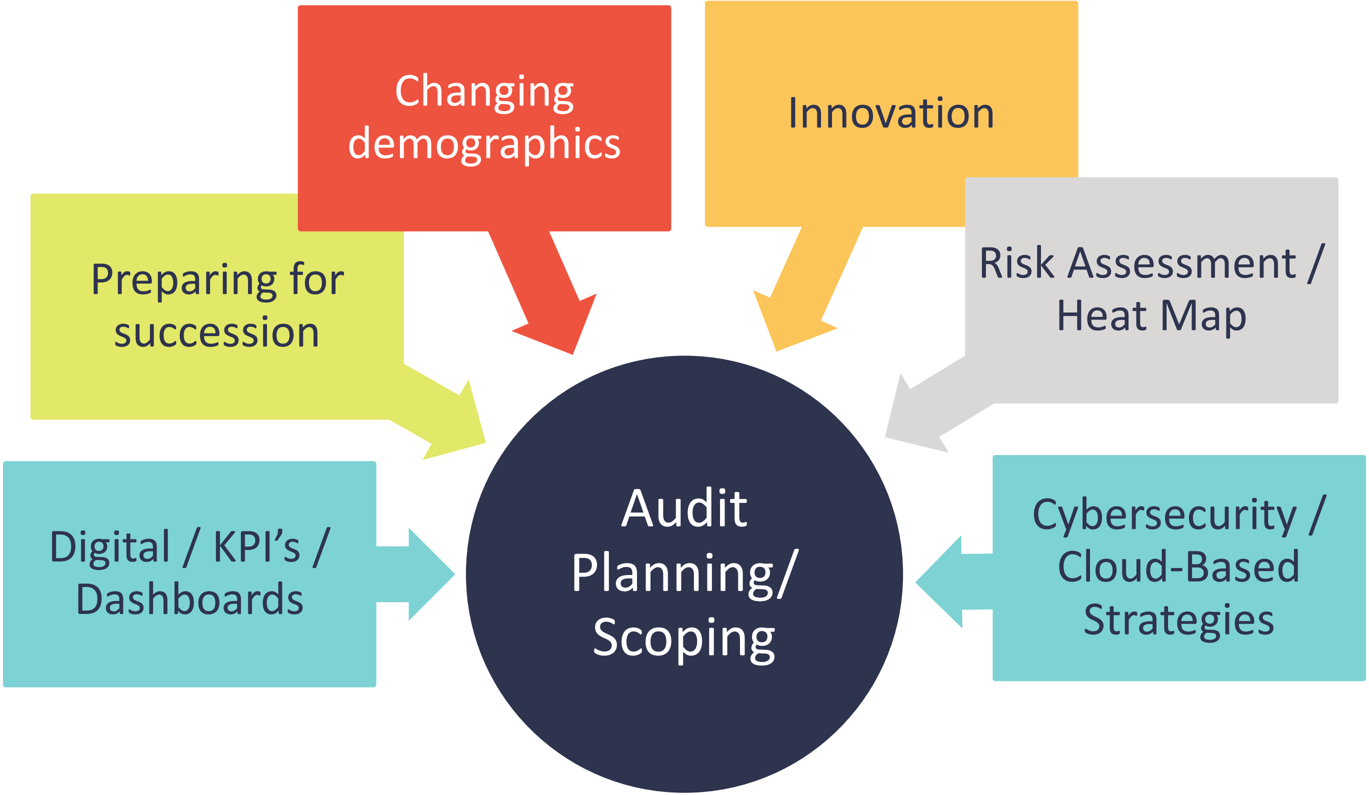
Compensation

- Damages for failure to meet SLAs usually are in the form of a % credit of fees with right to terminate for repeated failures.

Do We Have Proper Knowledge, Process and Tools?

- Software/hardware inventories
  - We don’t know what we don’t know.
  - Essential to any efforts to consolidate, streamline, standardize, etc.
- Rationalization & Redundancy
  - Are software, licenses, and tools routinely analyzed and reviewed? What opportunities are noted? Is hardware and software duplicated across various departments? What cost and efficiency is lost?
- Inefficient/duplicative contracts - Maximize vendor performance/services
- Standardization of Process and Procedures
  - Many cost containment issues with support, training, resources, etc. for disparate systems, applications, tools, and products
- Are we aware of how responsive, scalable, adaptive we want IT to be?
  - Goes back to question of knowing our goals and vision.

Risk Input and Integration



Changing demographics

Innovation

Preparing for succession

Risk Assessment / Heat Map

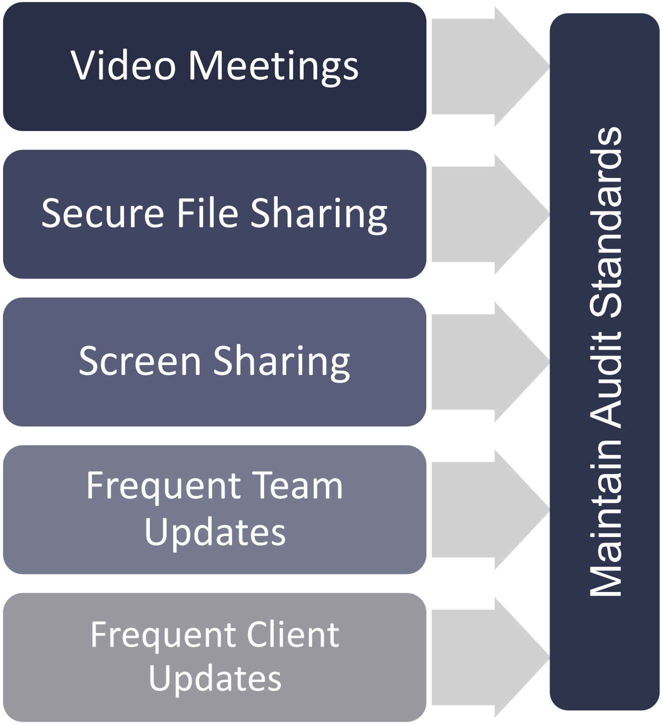
Digital / KPI's / Dashboards

Audit Planning/ Scoping

Cybersecurity / Cloud-Based Strategies

Audit Impacts

Remote Auditing


Video Meetings

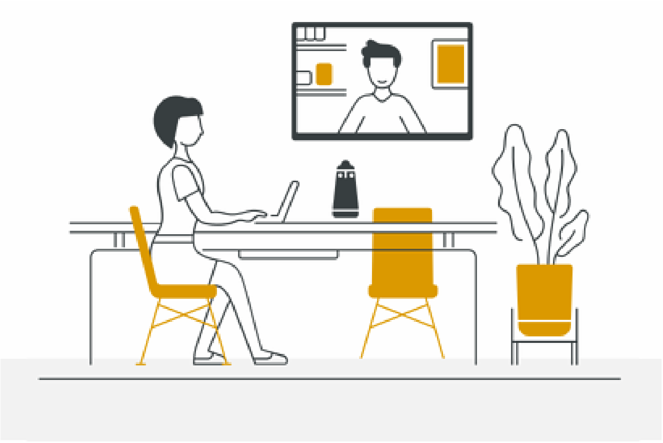
Secure File Sharing

Screen Sharing

Frequent Team Updates

Frequent Client Updates

Maintain Audit Standards



Encryption

Encryption scrambles the data so that it's unreadable in the hands of someone without the key (password).

- Are the auditors securing their data, evidence, reports, etc.?
- How is data shared with the auditor? Do auditors establish encrypted ways to send/received data?

❑ You should encrypt your mobile devices such as laptops - If a laptop is lost or stolen, the data is irretrievable. Have we assessed auditor devices?

Insurance underwriters react favorably to end-point encryption. In fact, it's one of the more significant "boxes to check"

Cyberinsurance

Easy to misunderstand, and few brokers well versed on the topic.

- ❑ Many of the coverages are not applicable.
- ❑ Cost to notify, public relations, credit monitoring services.
- ❑ **Cost to restore systems, loss of revenue**, employee theft.

- **Are auditors working consultatively and collaboratively with management on these areas? Are staff experienced/versed to review coverages, impacts, etc.?**
- **May want to coordinate with broker during the assessment and underwriting. Insurance companies now do significant due diligence quite often with these policies. Is the audit staff engaged/aware?**

Audit Updates?

- Have audit manuals/procedures been updated based on remote work/electronic formats, etc.?
- Have risk assessments truly been updated to reflect trends, evolving risks, etc.?
- Are virtual meetings encrypted? Do we use screen sharing that could be at risk? What about accessing from personal devices? Risk of recording (PHI, HIPAA, other compliance issues)?
- How do we audit certain activities? Can these be done virtually?
    - Inventory; Physical Controls; Access to “hard copy” records; etc.??
    - Interviews – can we read body language? Are cameras even on?

Security = Culture!!

*Security is a **BUSINESS** issue, NOT a technical issue!!*

- *Objectives:*
  - *Confidentiality*
  - *Integrity*
  - *Availability*
- *Strategy:*
  - *Administrative Policies / Procedures*
  - *Physical Access Controls*
  - *Technical Security Controls*

Questions?

Thank you!

Jim Kreiser, CRMA, CISA, CFSA
Principal – State & Local Government Risk Services Leader
Risk Advisory Services
James.Kreiser@CLAConnect.com
717.857.2613

Ashley Budd, CISA, CCSFP, CHQP
Senior – Risk Advisory Services
Ashley.Budd@CLAConnect.com
617.221.1949