We'll get you there

CPAs | CONSULTANTS | WEALTH ADVISORS

Cybersecurity – Trends, Risks, and Solutions

September 28, 2026

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.

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 an analysis conducted by DeepStrike, Government remains a top 10 affected industry of cyber attacks.
- Internet facing systems, legacy technology, identity gaps, and service-provider dependencies made the public sector exposed to external threats.
- Study from the Federal Bureau of Investigation shows a 26% increase in losses from internet crimes from 2024 to 2025

Cybercrime and Government – By the Numbers

2026 analysis conducted by DeepStrike noted:

- **65%** **Increase in ransomware attacks on government bodies in 2025**
- 50% Breaches involving third-parties (vendors, contractors, suppliers)
- $1.00m Average ransom for governments
- 20% Federal incidents caused by imposter/phishing

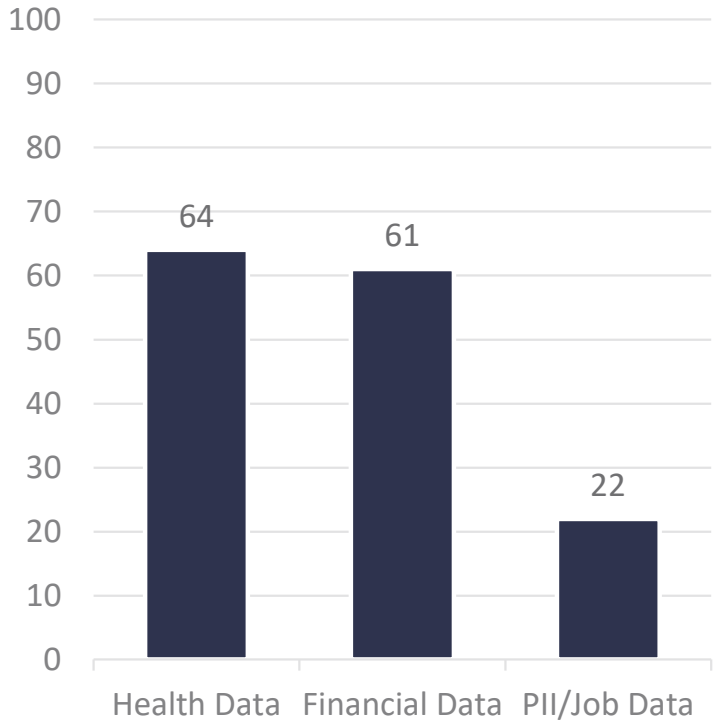
Cybercrime and AI – By the Numbers

2026 Cost of a Data Breach report conducted by IBM noted:

- **$4.99m** **Average cost of a data breach globally**
  - 12% increase from prior year
- 56% Increase in AI-driven attacks
- $6.00m Average cost of an AI model inversion attack
- 92% Share of organizations that reported an AI-related breach and lacked proper AI access controls

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.

Headlines – **Change Healthcare**

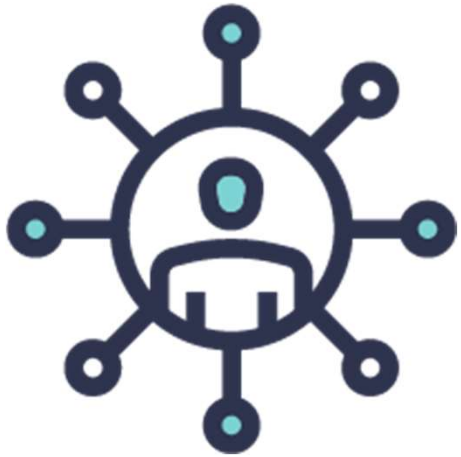
- **Largest US Healthcare Breach Recorded**
  - Access gained through Citrix remote access portal used by employees
    - No MFA enabled.
  - Nine-day delay between initial access and detection
  - $22 million ransom paid
    - data published on dark web anyway

Headlines – **Oracle E-Business**

- **2025 Ransomware Attacks**
  - Unpatched zero day vulnerability
    - Access gained through compromised emails, default password reset functions, etc.
  - Oracle E-Business Suite users extorted
    - Harvard University
    - Washington Post
    - Logitech.
    - Etc.

Headlines - **Aflac**

- **2025 Social Engineering Breach**
  - User accounts compromised
    - Human vulnerability
  - 13 million individual's info exposed
    - PHI
    - SSN
    - Etc.



What About These Headlines?

- **Rhode Island** – RIBridges System hit with ransomware. Went undetected for over 5 months until Brain Cipher posted stolen data on their leak site.
- **Nevada** – Ransomware attack due to download of a malware-laced system admin tool promoted via Google Ads. 26 accounts and 26,000 files accessed, and services across multiple agencies affected.
- **White Lake Township, Michigan** – Cyberattack assumed to be due to business email compromise (BEC). Portion of $29 million bond funds was compromised. New financing needed to be pursued.
- **City of St. Paul, Minnesota** – Backup server was compromised in July 2025 and bad actors were able to disrupt online payment portals, public wifi and internal networks. State of Emergency was declared which prompted a broader network shutdown. PII for over 12,000 individuals was stolen and posted.

Trends and Analysis

Ransomware

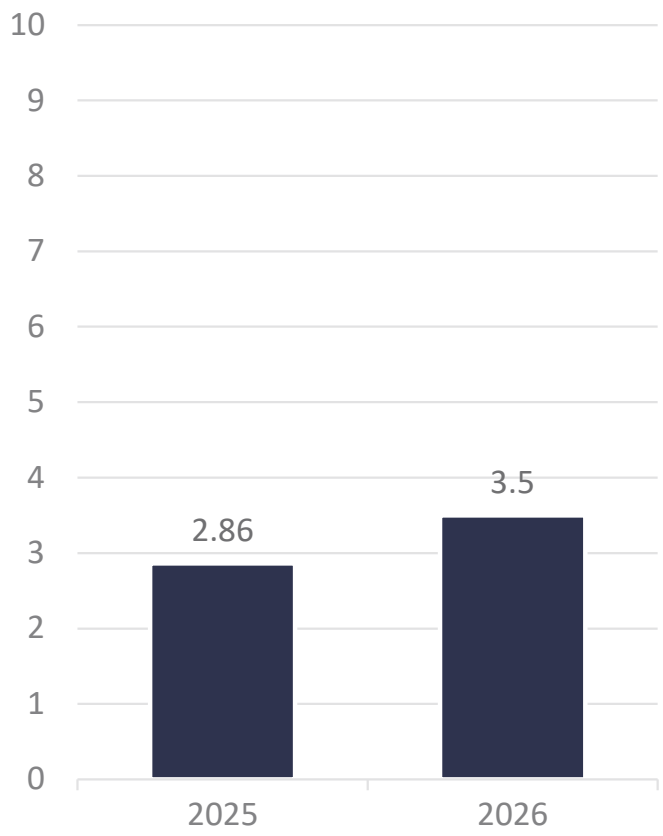
- Attack on the **availability** of data
- Payments are often in Bitcoin
- Cyber criminals attempt to delete backups
- Newer variants also demand payment not to publish stolen data (DOUBLE TAP)

Recent Sophos Study

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

Breach Identification and Containment

- Global average is 247 days
  - 183 days to identify a breach
  - 64 days to contain the attack
- Average cost to recovery from a breach for the public sector (government) is $3.5 million



Behind the Statistics

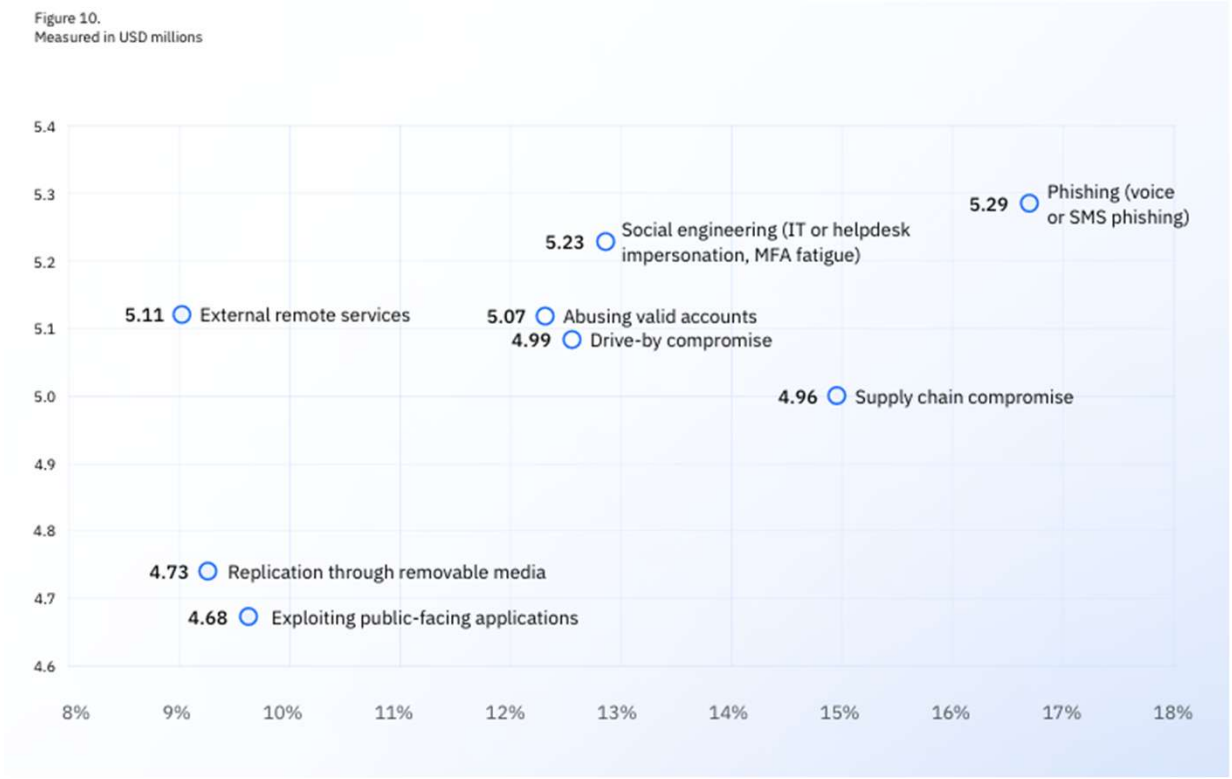
Hackers can do a lot in and to your network in 183 days

- Move across the environment
- Learn everything about your business
- Exfiltrate data
- Disable backups and security systems
- Create numerous back doors

Data Breaches and Our Impact

Attack Vectors and Root Causes

- Human error is the main cause of cyber attacks and data breaches



Source: IBM Cost of a Data Breach Report 2026

Social Engineering

- Exploit human psychology – attackers rely on trust, authority, urgency, and curiosity as a means of manipulation

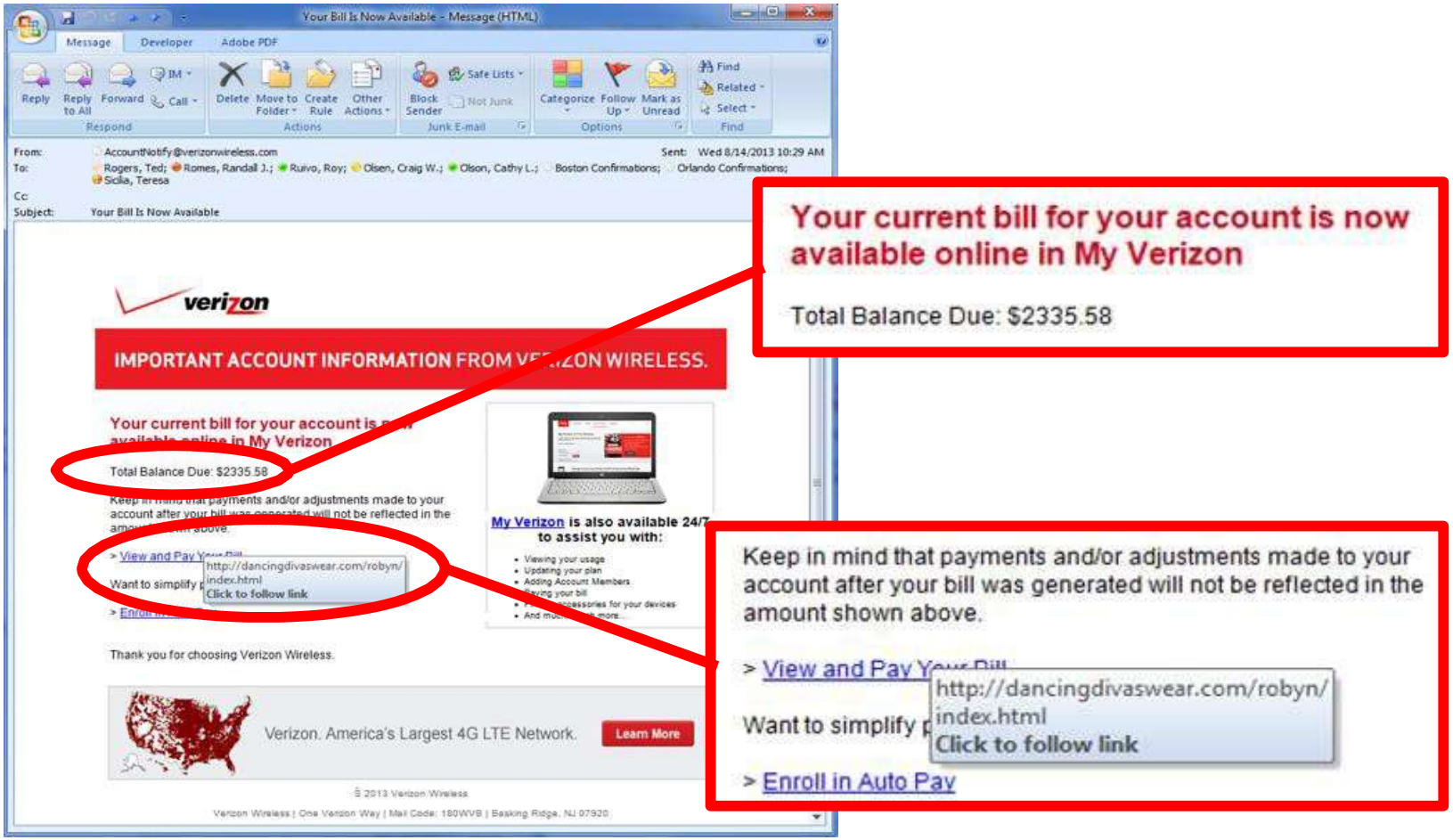
- Real World Examples:
  - AI Deepfake – employee in Hong Kong transferred $25 million after joining a video call with senior executives who were all AI-generated
  - IT Helpdesk Breach – MGM Resorts breached after attackers called the IT helpdesk impersonating and employee and gaining access to internal systems
  - Tailgating – woman bypassed Secret Service at Mar-a-Lago by pretending to be a family member of the President

Phishing

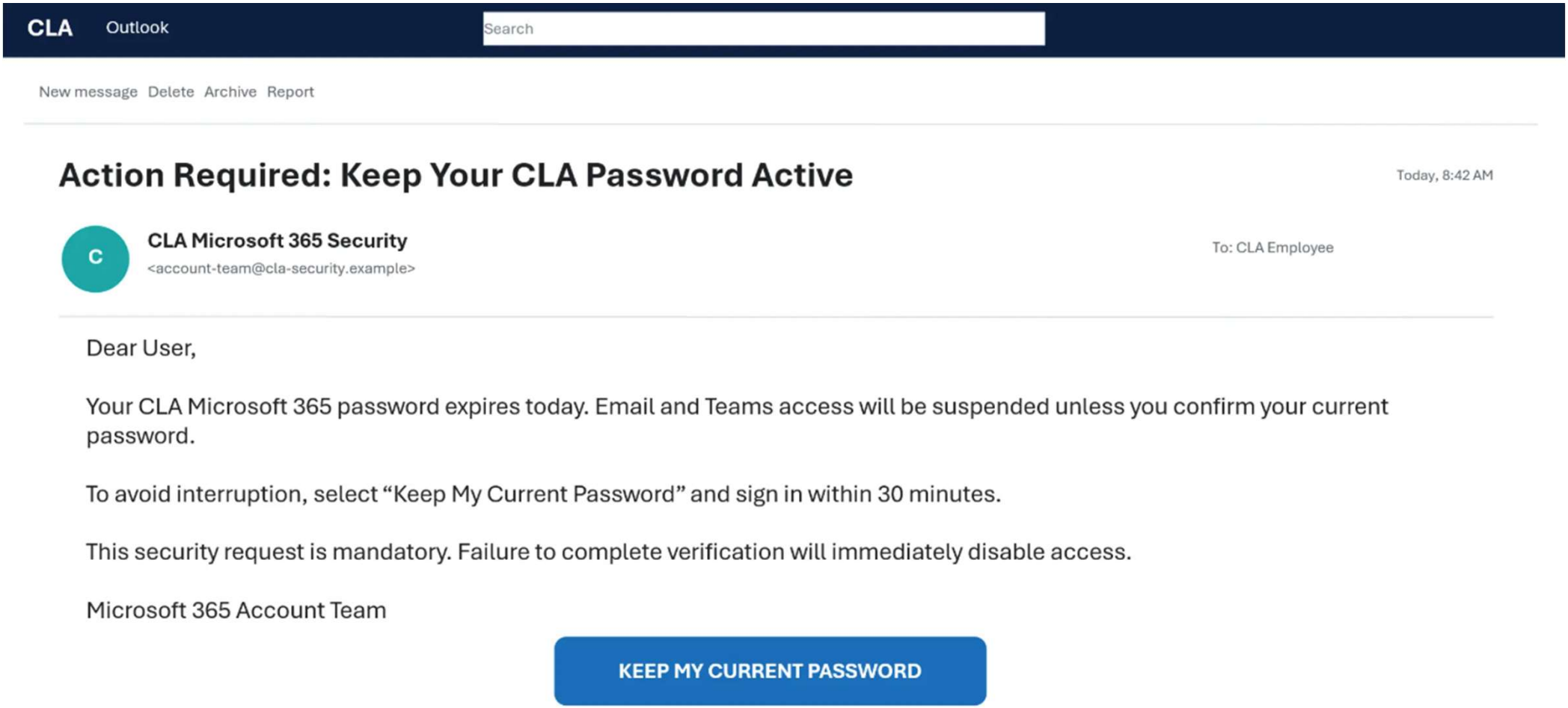
- Most common form of social engineering
- Deceptive messages that appear legitimate
- Email phishing
  - Mass fraudulent emails sent to many recipients
- Spear phishing
  - Targeted attack aimed at specific individuals
  - Whaling – targets high profile individuals (i.e. CEO)

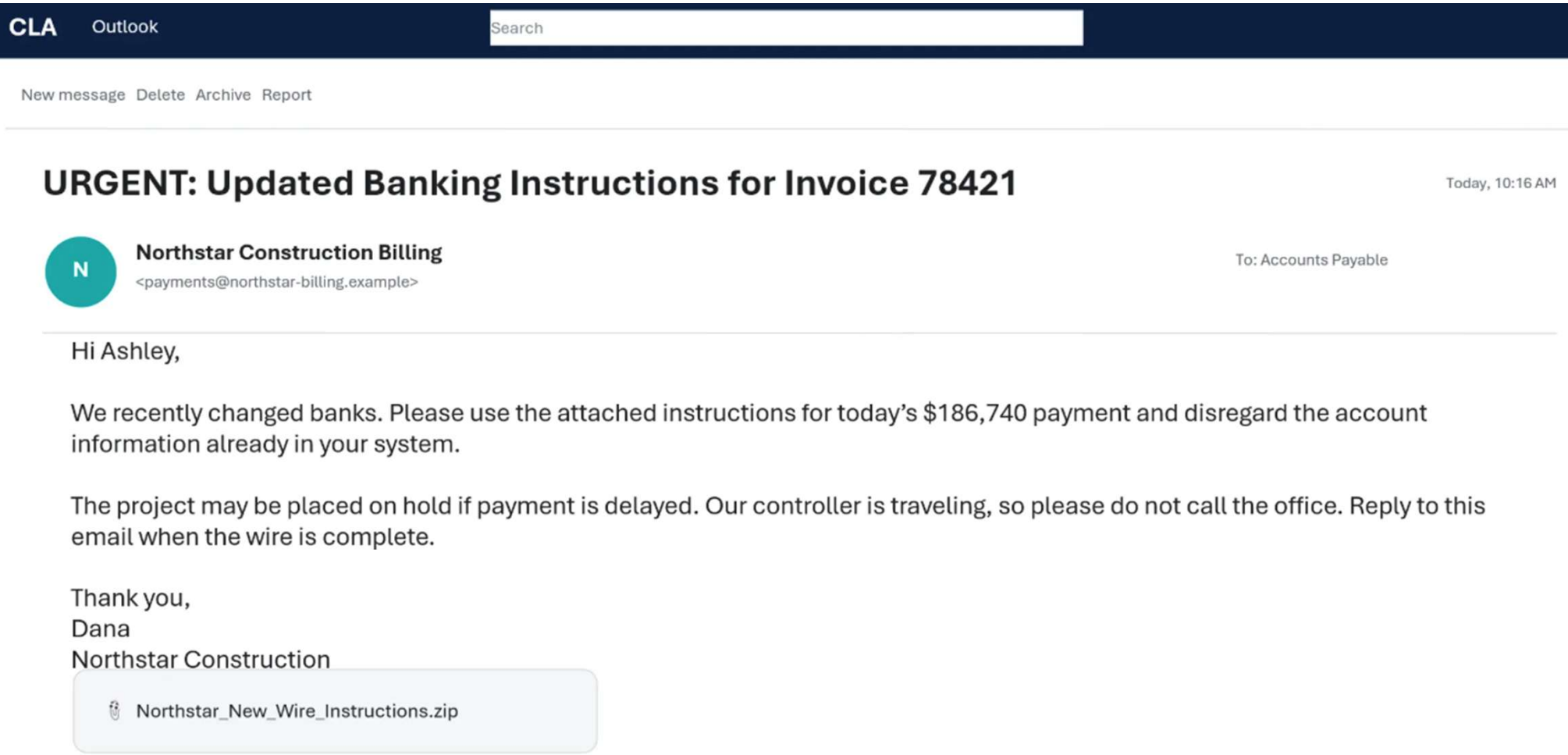
Business Email Compromise (BEC)

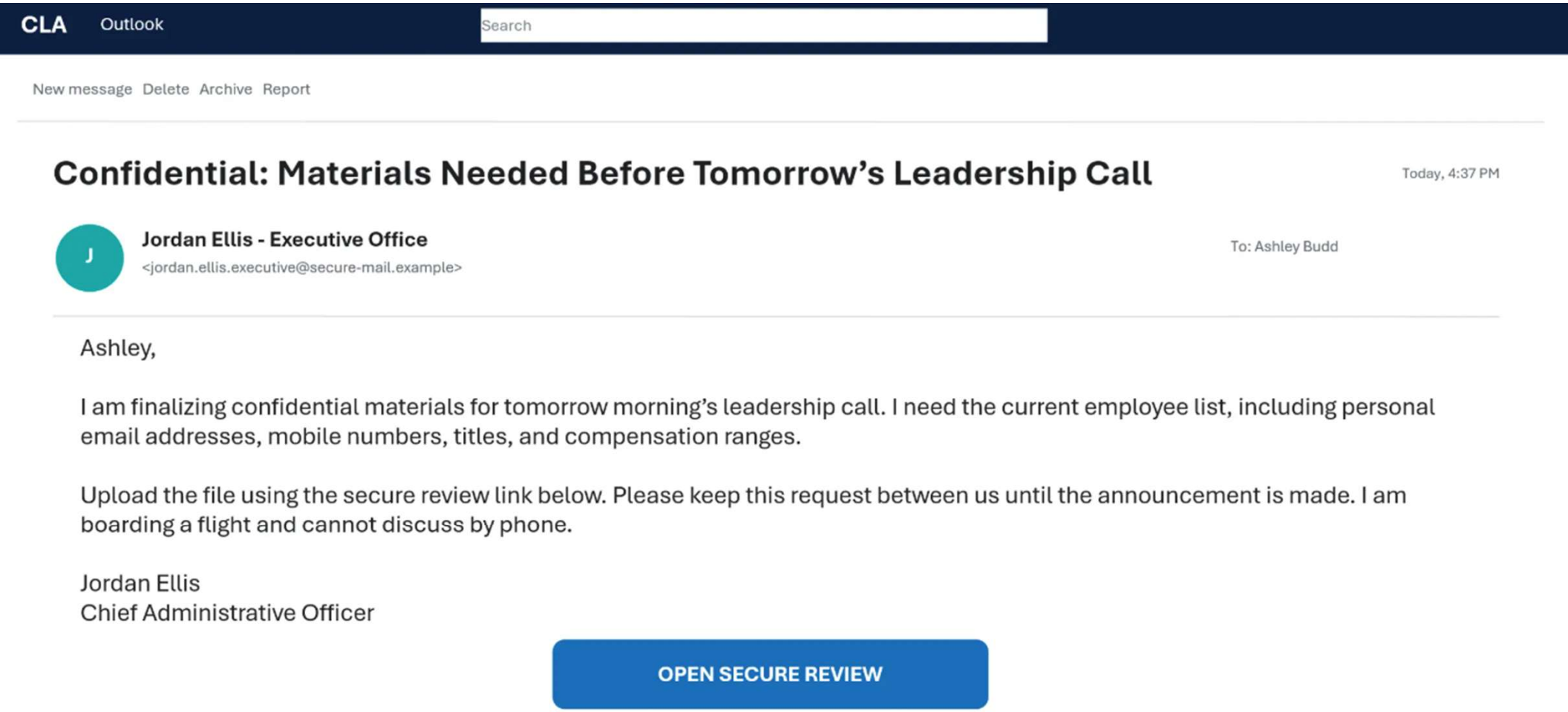
- Specialized form of spear phishing – relies on trust and urgency
- Fraudsters impersonate employees or vendors via email to steal money or data
  - Fake vendor invoice
  - Exec asks staff to “buy gift cards”
  - Update direct deposit account
  - Etc.
- Malware often not needed
- Mainly a form of social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



Activity – Identifying Phishing Warning Signs







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 data do we handle and standards should we follow/align with?
- NIST as a baseline cybersecurity framework

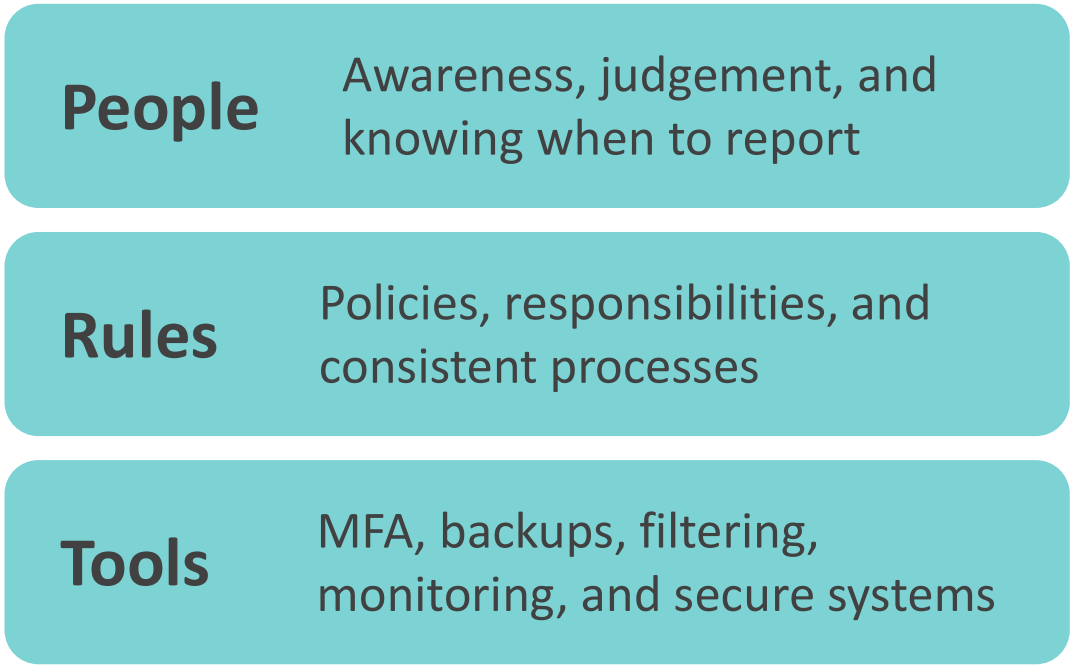
Data Type	Common Frameworks
Protected Health Information (PHI)	HIPAA
Financial customer information	GLBA
Payment card data	PCI DSS
Criminal justice information	CJIS
Student records	FERPA
Personally Identifiable Information (PII)	NIST Privacy Framework, state privacy laws

IT Risk Assessment

- What should be prioritized/where do we start?
  1. Set Scope: define key objectives, systems, etc.
  2. Identify Critical Assets: Build an inventory of assets and map criticality to business operations
  3. Identify Potential IT Risks: Internal and external threats and assess likelihood and impact
  4. Prioritize: Identify most critical impacts to business
  5. Identify Risk Treatment Options: Align actions with risk appetite
  6. Identify Remediation: What controls can be implemented?
  7. Implement and Monitor: Monitor for control effectiveness
  8. Reassess: Repeat process periodically (annually, after major changes)

Good Security Uses Layers

- No single tool, policy, or person can prevent every incident
- Layers reduce the chance that one mistake becomes a major event



Employee Training and Awareness

Human Error = Biggest Attack Vector

- What does your organization do? Security Training? Phishing? What follow-up?
- Phishing, testing, and awareness are critical. We all are the front line – and stats show we are failing.

Passwords

- An analysis of over 19 billion leaked passwords in 2025 found that **94% of passwords** were either weak, default, simple, or reused across multiple accounts
- Old Rules (NIST – 2005?)
  - Length (8+characters)
  - Complexity (Aa4@)
  - Forced expiration (every____)
- New Guidance (NIST – 2018)
  - Long passwords
  - No expiration
  - Especially important for administrative accounts (CIS 4)
- MFA on all external systems

Pass Phrases	
Password24	Unforgiveable
Summer24	Terrible
N*78fm/1	Painful
Wallet Painting lamp	Good
The Packers always beat the Bears	Best

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.

Incident Response Planning

- Develop an incident response plan
  - Include the appropriate procedures
    - Preparation
    - Detection and analysis
    - Containment
    - Eradication
    - Recovery
    - Lessons learned
  - Ensure points of contact & responsible parties are included/outlined
  - Keep the plan update to date

Disaster Recovery Planning

How do we recover systems after a disruption (attack, outage, etc.)?

- Inventory of assets and results of risk assessment are crucial
  - Where are critical data elements (“the crown jewels”) stored and processed?
  - What supports critical business processes?
- **Business impact analysis** with definition of recovery point objectives
- Disaster recovery is periodically practiced
  - Need to make sure it works the way you expect

Cybersecurity Insurance

Role in the Control Environment = Risk Transfer

- Helps fund covered response and recovery costs after a cyber event
- It does *not*:
  - Prevent an attack
  - Replace incident readiness
  - Guarantee complete coverage
- Understand your policy options

Third Party Risk and Due Diligence Practices

Vendor Risk: Exposure Extends Beyond Your Network

Why it Matters

- **Data** Vendors may process, transmit, or store sensitive information
- **Access** Remote support and integrations can create entry paths
- **Operations** Outages can interrupt essential services and recovery
- **Compliance** Contractual and regulatory obligations remain with you

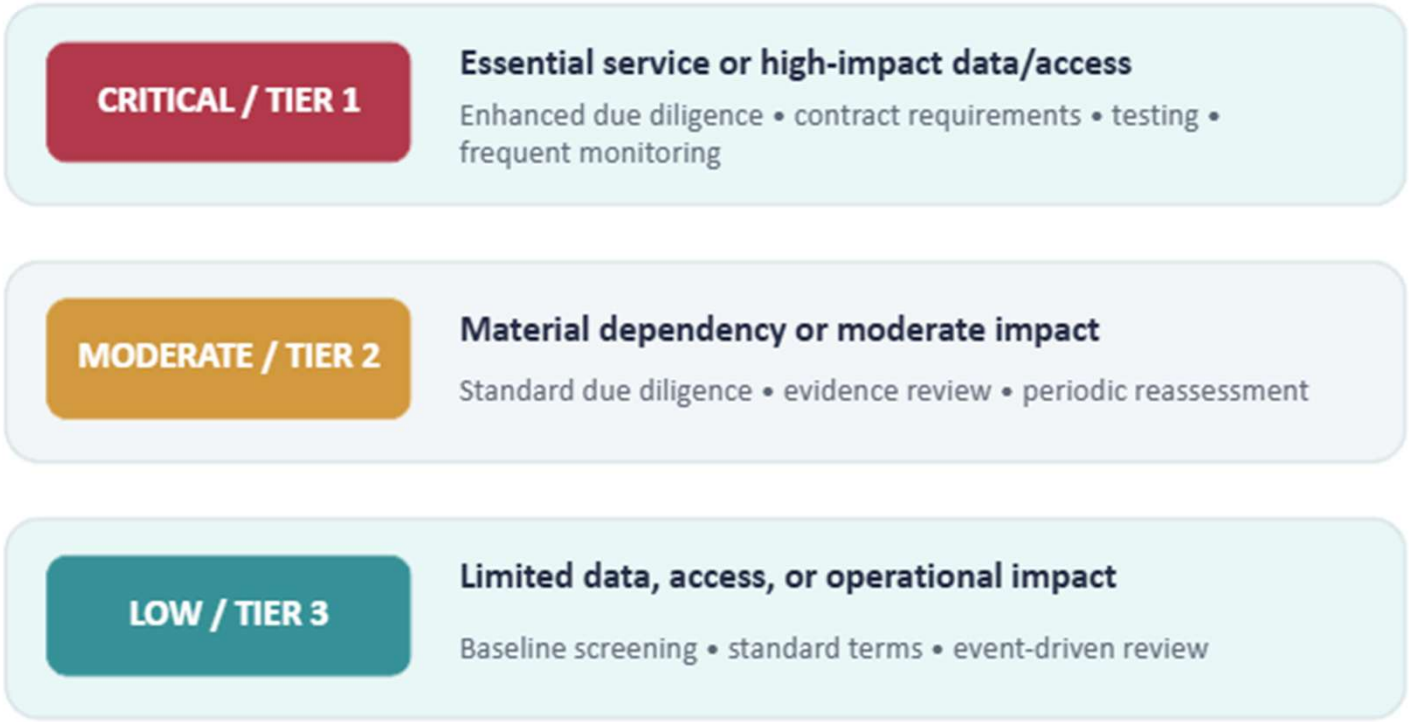
Vendor Risk Management Policy

- Establish Accountability!!
  - Set consistent expectations for selecting, assessing, contracting, monitoring, and terminating vendor relationships

- Basic Policy Elements
  - Scope
  - Roles & Responsibilities
  - Tiering
  - Due Diligence
  - Contracts & Monitoring
  - Termination

Risk-Based Vendor Tiering

Not all vendors are the same



Vendor Due Diligence: Match Review to Risk

- Due diligence should validate whether the vendor's controls and commitments are appropriate for the assigned risk tier

Tier 1 - Critical

- Detailed security questionnaire
- SOC report
- Incident response and recovery evidence
- Penetration test summary
- Annual risk assessment

Tier 2 - Moderate

- Standard security questionnaire
- SOC report, if available
- Reviewed every 2 years

Tier 3 - Low

- Basic vendor onboarding/screening
- Contract review
- Reassess when services change

We'll get you there

CPAs | CONSULTANTS | WEALTH ADVISORS

Questions?

Thank you!

Ashley Budd, CISA, CCSFP, CHQP
Manager – Business Risk Services
Ashley.Budd@CLAConnect.com
617.221.1949