We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Understanding Your Benefit Plans' Cybersecurity Requirements and Options

July 22, 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.

Session CPE Requirements

- You need to attend 50 minutes to receive the full 1 CPE credit.
- There will be 4 polling questions throughout the presentation. You must respond to a minimum of 3 to receive the full 1 CPE credit.

Both requirements must be met to receive CPE credit

Speakers

Doug Bertossi
Principal, Employee Benefit Plans
doug.bertossi@CLAconnect.com
612-376-4693

Randy Romes
Founding Principal, Cybersecurity
randy.romes@CLAconnect.com
612-397-3114

Agenda

Why cybersecurity is a critical consideration for EBP

Our adversaries (threat actors) and their motivations

What we need to defend against

Strategies to safeguard our plan assets

Learning Objectives

1

Recognize the latest developments in cybersecurity

2

Identify where to focus valuable risk mitigation resources

3

Recall how-to develop and refine a framework of knowledge to plan ongoing security efforts and response strategies

Current Employee Benefit Plan Cybersecurity Environment

Why Cybersecurity Is Critical for EBP

- Plans operate in a highly electronic environment
- Large amounts of sensitive data that may be shared with multiple third parties
- Many times, plans fall outside the scope of a plan sponsor's cybersecurity planning for their organization
- Plan sponsors and administrators may incorrectly believe that their service organization SOC 1 reports address cyber risks at the service organization

Why Cybersecurity Is Critical for EBP

- In 2021, Government Accountability Office (GAO) issued a warning about increased risk to ERISA fiduciaries related to cyber breaches
- Data involved can be valuable
- Plan assets
- Court cases exist regarding:
  - Participants having their retirement plan accounts hacked and drained
  - Breaches at third-party service providers with losses of hundreds of thousands of sensitive data points in a single incident

Department of Labor Cybersecurity Guidance

- Employee Benefit Security Administration issued cybersecurity guidance for employee benefit plans in April 2021
  - Updated guidance in September 2024 confirmed guidance is for all plans, not just retirement plans
  - Tips for hiring third-party service providers with strong cybersecurity practices
  - Cybersecurity program best practices
  - Online security tips for employee benefit plan participants

Activities Being Done by Plans

- Assessments of third-party vendors
  - Questionnaires
  - Interviews
  - On-site visits
- Supplementing service contracts with cybersecurity and privacy terms and agreements
- Reviewing SOC 2 or other data security testing results

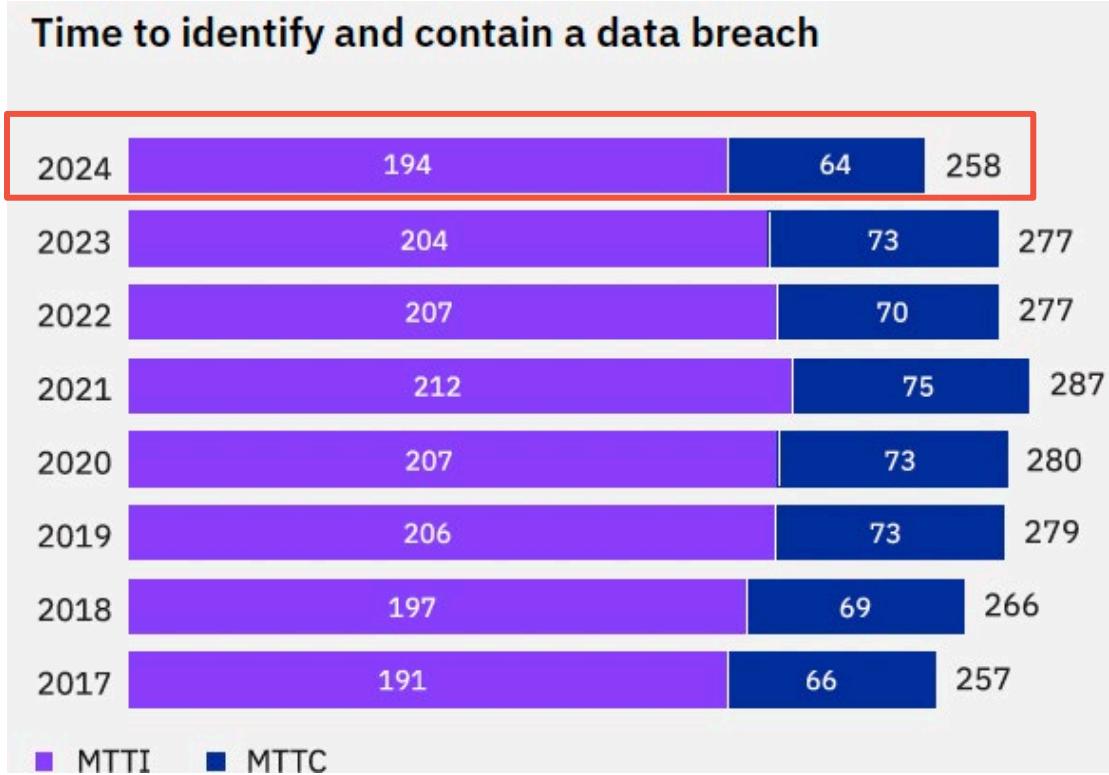
Polling Question 1

- What activities has your organization performed to address the DOL Cybersecurity Guidance?
  - Assessments of third-party vendors
  - Supplementing service contracts with cybersecurity and privacy terms and agreements
  - Reviewing SOC 2 or other data security testing results
  - Other activities
  - No activities at this time

Sun Tzu: “Know Your Enemy”

The Current Threat Landscape

IBM – Average Days to Identify and Contain a Data Breach



Source: IBM Security Cost of a Data Breach Report 2024

Global average is

258 days

- 194 days to identify a breach
- 64 days to contain the attack
- IMPROVEMENT!

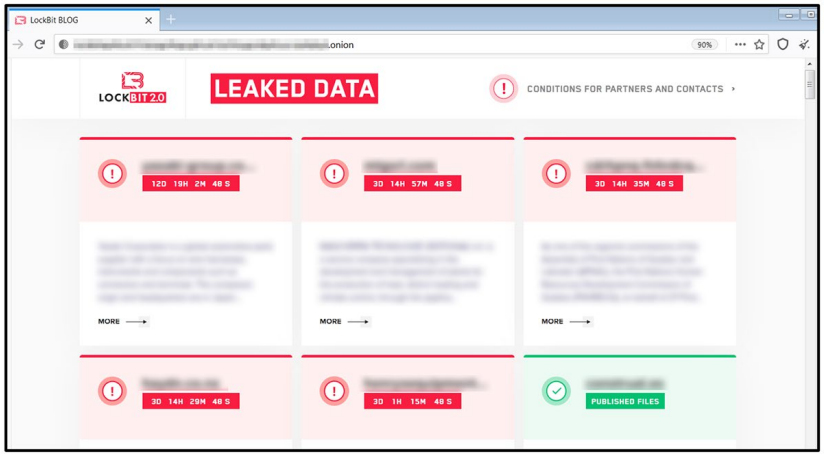
What are the bad actors doing for 194 days?

Cybercrime and Black-Market Economies

- Black-market economy to support cyber fraud
  - Business models and specialization
  - Underground Marketplace (The Dark Web)
- Most common cyber fraud scenarios we see affecting our clients
  - Theft of information
    - Log in Credentials
    - ePHI, PII, PFI, account profiles, etc.
    - Credit card information
  - Ransomware, interference w/ operations and extortion
- Monetization of access…

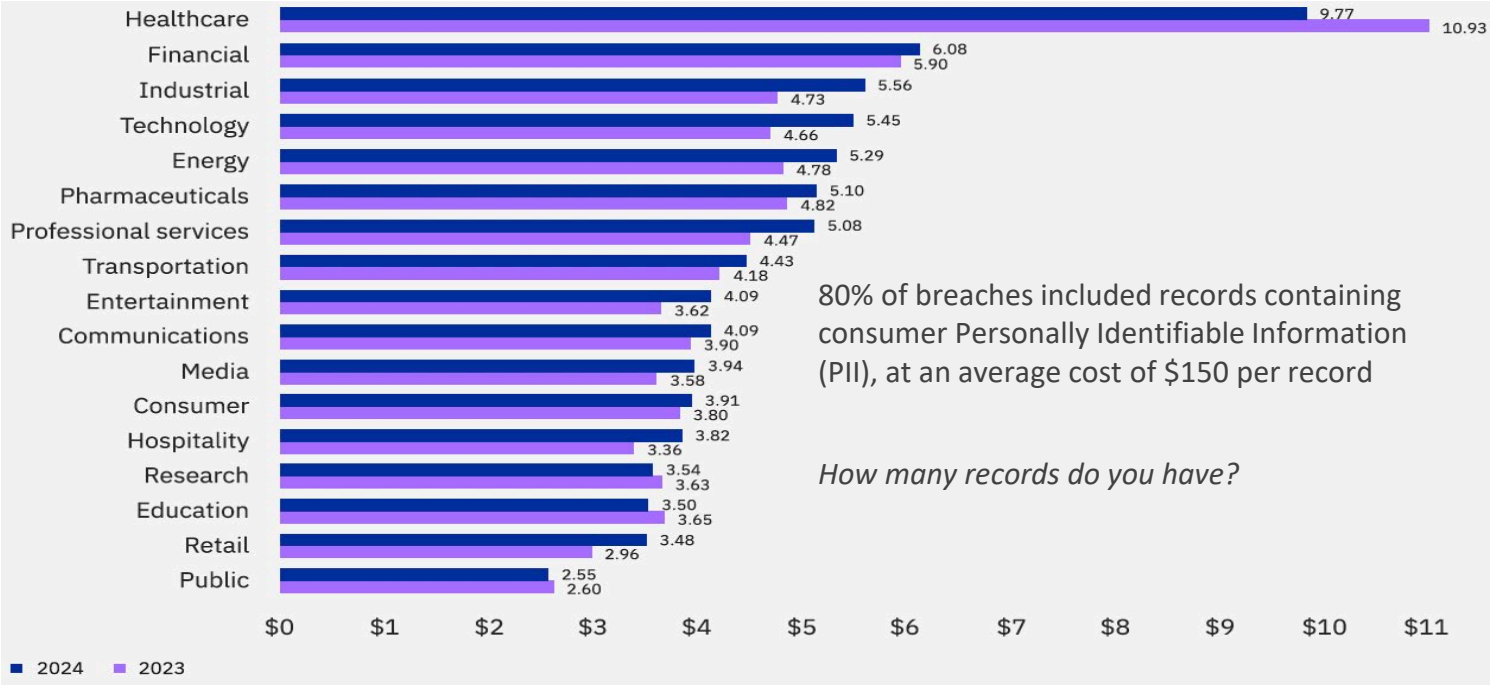
They will hit you with any or all of the following:

1. Email Spear Phishing Attacks
2. Password Guessing and Business Email Account Takeovers
3. Payment and Funds Disbursement Transfer Fraud
4. Data exfiltration
5. Ransomware
6. Extortion to avoid breach disclosure



IBM - Cost of a Data Breach

Average cost in 2024 is $3.5M



80% of breaches included records containing consumer Personally Identifiable Information (PII), at an average cost of $150 per record

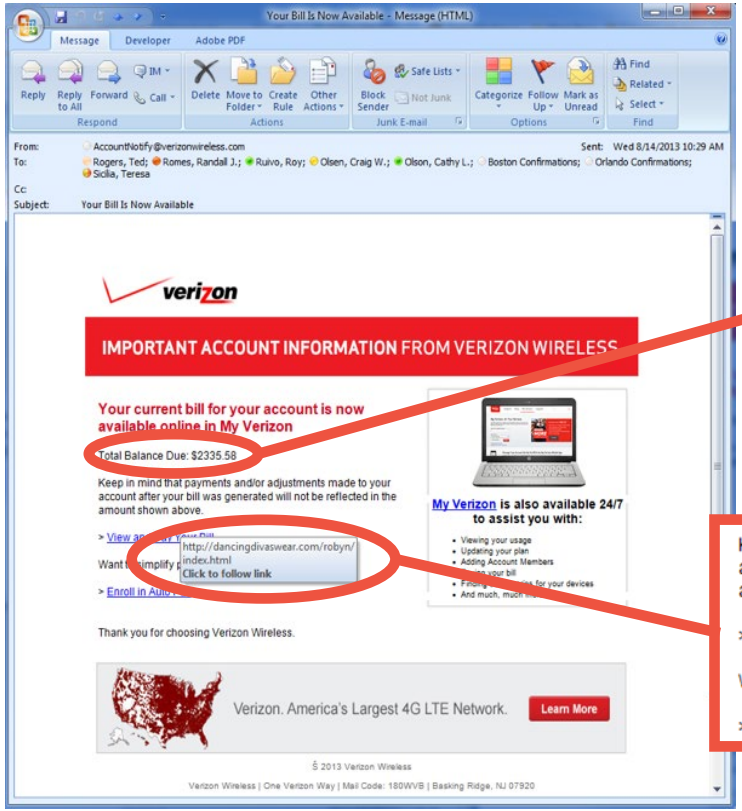
How many records do you have?

Source: IBM Security Cost of a Data Breach Report 2024

Email (Spear) Phishing

The Root Cause For Most Breaches

Spear Phishing



Your current bill for your account is now available online in My Verizon

Total Balance Due: $2335.58

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

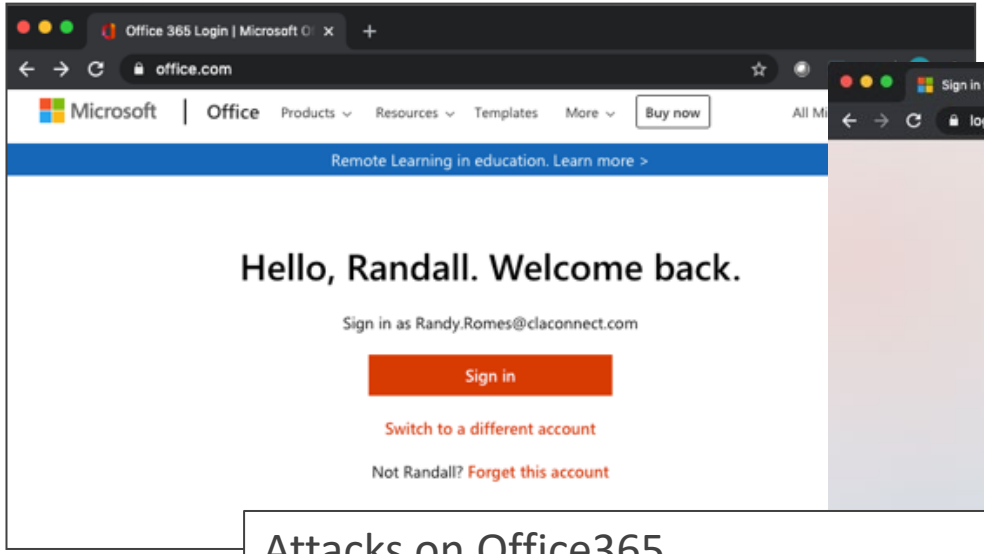
> View and Pay Your Bill

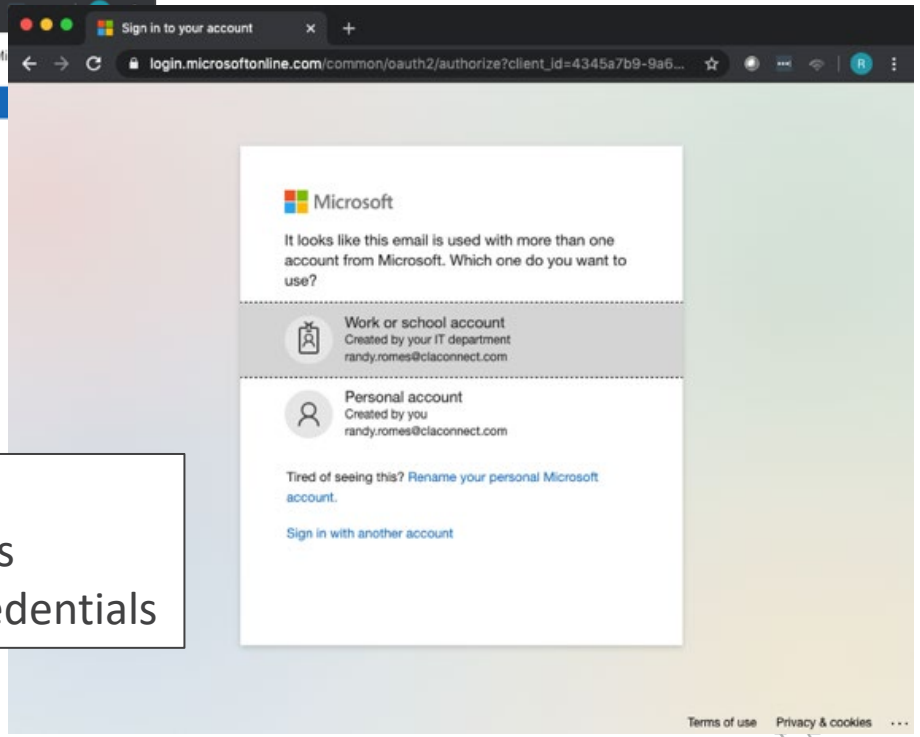
http://dancingdivaswear.com/robyn/index.html
Click to follow link

Want to simplify p

> Enroll in Auto Pay

Credential Harvesting and Password Guessing:





Attacks on Office365

- Password guessing attacks
- Phishing that harvests credentials

Case Study

BEC, Payment Diversion, and Data Loss

Overview

- CFO sent email to HR to process an updated bonus
- HR verified the legitimacy, identified request was fraudulent
  - CFO did *NOT* send it
- IT Security team “reviewed”, identified logins from outside the USA, found no other fraudulent emails/requests, and changed password for user
- Three months later, risk committee heard about incident and asked for independent investigation
  - Log retention for many systems was default (30 days)

Analysis

1. Email that was sent from CFO to HR was sent using CFO's actual email account
2. Log in came from Ukraine
3. Three weeks of failed logins prior to success
4. Numerous successful logins over 10 days before invoice request, including…

Analysis

- Analysis of email showed controller had documents with users' social security numbers and bank account information
  - 13,499 email addresses
  - 87,844 bank routing and account numbers
  - 51,071 Social Security numbers

Preventative Measures / Mitigating Controls

- Improve monitoring
- Improve password security requirements
- Enforce multi-factor authentication on all forms of remote access
- Implement geo-restrictions to M365
- Enable email retention settings
- Enhance log retention settings

Passwords

- Old Rules (NIST)
  - Length (8+ characters)
  - Complexity (Aa4@)
  - Forced expiration (every…)
- New Guidance (NIST)
  - Password tools
    - MFA
    - Password managers

Password Audit	Total
Number of passwords audited	855
Passwords cracked	794
Passwords that were all letters	63
Passwords that were all numbers	5
Passwords that were an English word	20
Passwords that were a word with numbers appended to it	200
Passwords that were the same as the username	6
Passwords that do not meet Windows complexity	584

Password Strategies:

- Multi-factor authentication on ALL external systems
- Password management tools
- Pass phrases – ***long*** natural language
  - Password21 = Unforgiveable!
  - Summer21 = Terrible
  - N*78fm/1 = Painful
  - Wallet Painting lamp = **GOOD**
  - The Packers always beat the Bears! = **BEST**

Polling Question 2

- Are you planning to invest in AI and digital solutions in the next six months?
  - 5 = Highly likely
  - 4 = Likely
  - 3 = Neutral
  - 2 = Unlikely
  - 1 = Highly Unlikely

Attacking the Supply Chain:

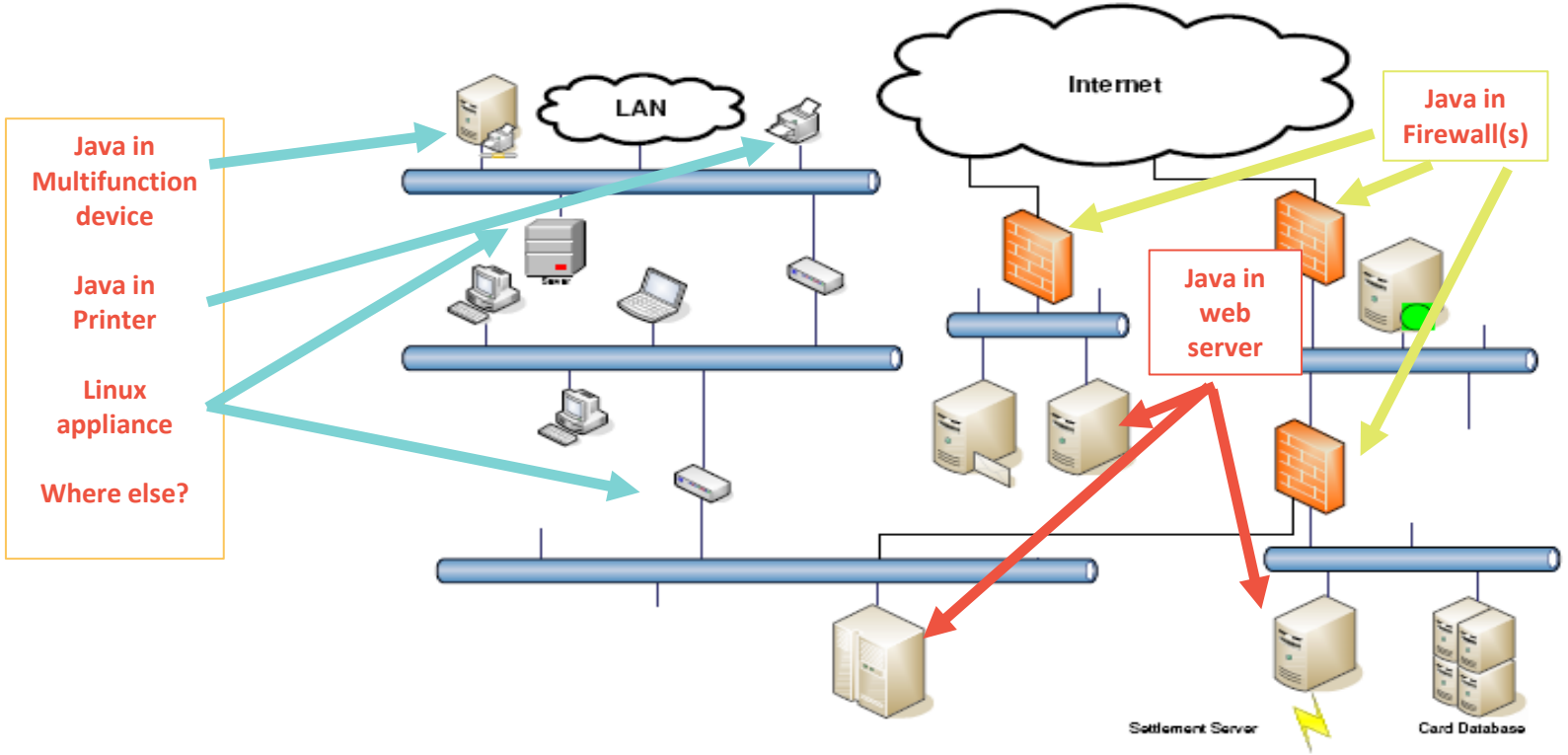
Software Vendor/Supply Chain Risk Management

Recent Significant Issues:

- Common software components with exploitable vulnerabilities
- Recent examples include
  - "**Log4j**" Java vulnerabilities…
  - **Pkexec** - CVE-2021-4034 (PwnKit)
  - **Python** – CVE-2007-4559
    - September 2022
    - 15-Year-Old Python Flaw Slithers into software worldwide
    - An unpatched flaw in more than 350,000 unique open source repositories leaves software applications vulnerable to exploit

Google:
Log4j vulnerabilities

Java Software and Log4j



Software Vendor/Supply Chain Risk Management

- All software products have bugs/vulnerabilities
- Key questions:
  - Do we have accurate system and data inventory?
  - What does this software application have access to?
  - What user account/privileges are given to it?
  - What do we need to do for our due diligence?
  - What impact does this software have on the institution…
    - If it is hacked/breached?
    - If it is down for… 2 hours? 2 days? 2 weeks? 2 months?

Pick your hosted software vendor:

1. CrowdStrike
2. Trellance
3. MoveIT
4. Kronos
5. Solarwinds
6. MS Exchange
7. _____

Operational Stability

Ransomware is not going away.

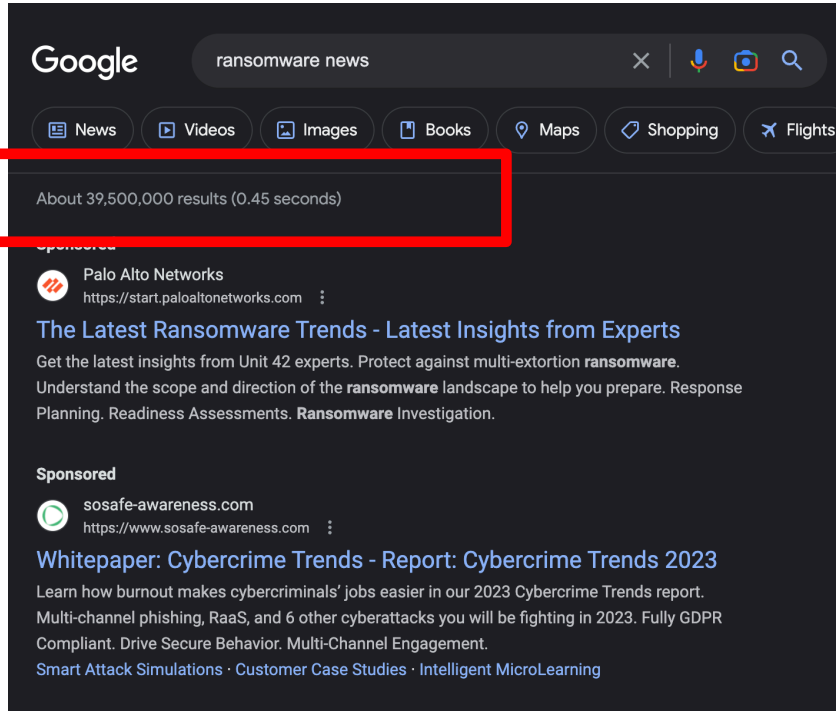
How much would you pay to restore access to your plan?

Ransomware

- Ransomware bursts on the scene more than eight years ago
- Hollywood Presbyterian decided to pay after ___
- Why did they wait to pay?

Ransomware

- Interfere with operational up time
  - This costs $
- Extortion:
  - Pay to release data and systems
  - Pay to avoid exposure
  - Threaten those whose data has been stolen
- Be Prepared
- Have you performed a ransomware readiness/resilience test?
- Can IT operations restore? From bare metal up? In the heat of the moment?
- Are you confident your hosted vendor is prepared?
  - Change health care?



Preventative Measures / Mitigating Controls

- Network segmentation
  - e.g. Isolation
- Admin credential hygiene
- Strong patch management
- Antivirus/endpoint controls
- Logging and monitoring
- **Secure (isolated) backups**
- Cybersecurity insurance

Polling Question 3

- As an organization, do you believe you are prepared for a cybersecurity incident?
  - Yes
  - No
  - Not sure

Standards Based Operations
“People, Rules, and Tools”

Peace of Mind - It Starts with Policies and Standards

- Security is not a product
  - There is no sliver bullet
- People, Rules and Tools
  - What do we expect to occur?
  - How do we conduct business?
  - Who is responsible for what?

- Standards based operations from a framework:
  - GLBA, DOL, HIPAA, State Laws --- Regulatory
  - PCI – DSS, CMMC --- Contractual
  - CIS Critical Controls, NIST CSF --- Operational standards

Department of Labor Requirements

These requirements tightly aligned with other governance and compliance frameworks. (**Foreshadowing**…)

They can save you $... (**Foreshadowing**…)

Where should you start?

- Readiness and Gap Assessment
- Risk and Security Assessment(s)
- Build or update your program
- Develop a process for continuous improvement
- Practice and Test - Be Prepared (for the worst)

EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

CYBERSECURITY PROGRAM BEST PRACTICES

ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employee Benefits Security Administration has prepared the following best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plans' service providers should:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf

Standards Based IT and Cyber Operations

CIS Critical Controls – Version 8

- Vendor/Product/Industry agnostic
- 20 years of improvement
- Prioritized
- Scalable

- Check lists, benchmarks, reporting and tracking tools and resources
  - Cloud implementations
  - Operating systems and software
  - Hardware/devices

- Best “plain English” framework

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

1. ”Have a formal, well documented cybersecurity program”

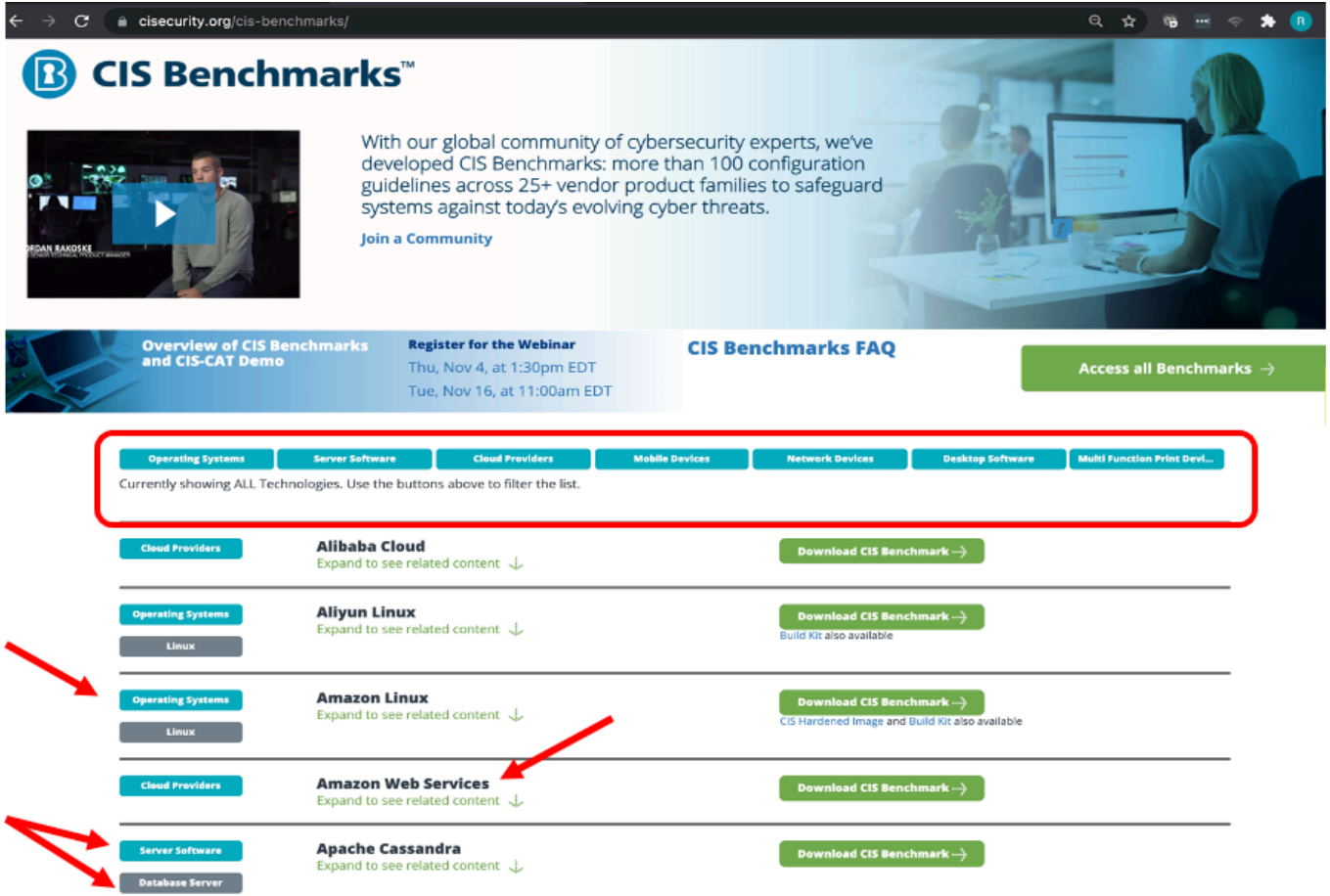
6. Ensure that any assets or data stored in a cloud…

11. Implement Strong Technical Controls….

CIS Benchmarks

Checklists and How-to guides for just about everything

- Operating Systems
- Server Software
- Network Devices
- Cloud Implementations
- Etc…



Secure Office 365

NOT fully secure by default

- Needs to be secured:
  - ➢ Enable/Turn On security features
  - ➢ Harden (email) security
  - ➢ Fine tune logging, monitoring and alerting
  - ➢ Enforce retention periods

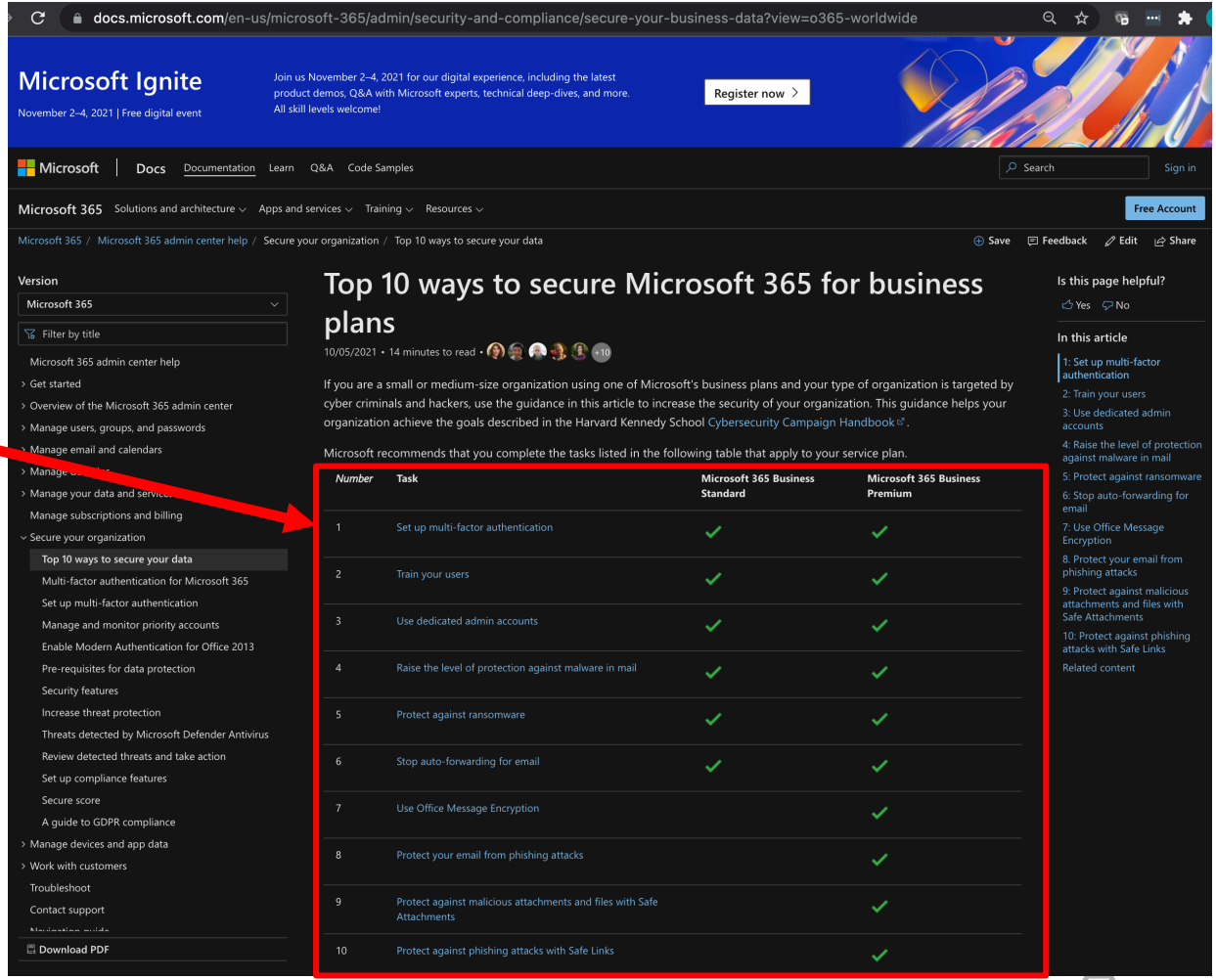
6. Ensure that any assets or data stored in a cloud…

11. Implement Strong Technical Controls….

CIS Benchmarks

Checklists and How-to guides for just about everything

- Operating Systems
- Server Software
- Network Devices
- Cloud Implementations
- Etc…



Incident Response Preparedness

- Unfortunately, data breach can still occur despite implementing all the best security precautions → Think WHEN… NOT IF
- Have a plan – implement the plan – practice the plan
- Develop an incident response program and 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

12. Appropriately respond to any (past) cybersecurity Incidents

Are you prepared to respond to any (or all) of the following:

1. Email spear phishing attacks
2. Password guessing and business email account takeovers
3. Payment and funds disbursement transfer fraud
4. Ransomware
5. Extortion to avoid breach disclosure

Incident Response, Disaster Recovery Business Continuity

- Inventory of assets and results of risk assessment are crucial
  - Hardware, software and critical data elements (“the crown jewels”)
  - Data classification and retention
- Business impact analysis with definition of recovery point objectives
  - Defines criticality and priority for restoration
- Incident response planning and procedures are well defined
  - Playbooks…
  - Standards based (eg. NIST 800-61 or similar)
- Know how the vendors fit into and support the plan
  - Contractual SLAs

Practice the Plan

- IT and operations needs to PRACTICE – prove they can restore in the heat of the moment
- Tabletop exercises- simulations where participants walk through the incident and response procedures
- Simulated adversarial breach exercises:
  - Red team penetration testing
  - Spear phishing tests and other social engineering tests

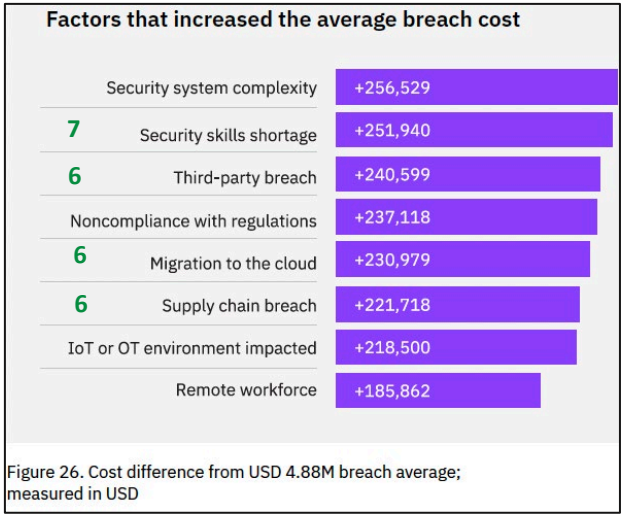


Figure 26. Cost difference from USD 4.88M breach average; measured in USD

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

Maturity leads to Cost Savings

3. Have reliable annual third party audit of security controls
4. Clearly define and assign information security roles and responsibilities
5. Have strong access controls…
6. Ensure any assets or data stored in a cloud or managed by a third-party…
7. Conduct periodic cybersecurity awareness training
9. Have an effective business resiliency program…
10. Encrypt sensitive data
12. Appropriately respond to any past cybersecurity incidents

“Chance Favors the Prepared Mind”

Are you confident you’ve done enough to secure your employee benefit plan?

Do you have appropriate governance and visibility into your service providers and TPAs

Are they doing enough of the right thing?

Are you prepared for…???

Be Prepared…

Prepare

Operate

Test

- IT Operations – Digital – Cybersecurity Readiness
- Risk Assessments at least annually
- Standards Based Operations and Exception Management
  - Daily Operational DNA
- Regular/periodic risk assessment:
  - Daily Business as Usual
- Monitor and fine tune:
  - Continuous improvement
- **Practice and Test**
  - Audit your operations controls (against a framework)
  - Review Office 365 (O365) security (periodically)
  - Schedule IR Tabletop and Disaster Recovery exercises
  - Test new systems and after significant change
  - Test your people periodically

Polling Question 4

- I would like someone from CLA to contact me to discuss these services:
  - Penetration Testing and Vulnerability Assessment
  - IT/Cyber risk, audit and compliance (DOL, HIPAA, CIS, NIST, CMMC, etc.)
  - PCI-DSS Readiness and Compliance Assessments (PCI-DSS)
  - Independent security consulting
  - Nothing at this time

Thank you!

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

Doug Bertossi, CEBS, CPA
Principal – Employee Benefits Plan
doug.bertossi@CLAconnect.com
612.376.4693

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/
- Center for Internet Security – Critical Controls Resources
  - https://www.cisecurity.org/controls
- IBM Cost of a Data Breach
  - https://www.ibm.com/reports/data-breach
- Department of Labor Cybersecurity Guidance
  - https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices
  - https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf

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 (DOL, HIPAA, GLBA, NIST, CMMC, CIS, State Laws, 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

PCI Security Standards Council®

HITRUST Authorized CSF Assessor

AICPA SERVICE ORGANIZATIONS SOC aicpa.org/soc Formerly SAS 70 Reports®

CLA Cybersecurity Helps Clients

Governance, Risk, & 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