Cybersecurity and Your Employee Benefit Plan

October 26, 2021

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Disclaimer

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Agenda, Learning Objectives & Speakers

Agenda

- Our adversaries (threat actors) and their motivations
- What we need to defend against
- Strategies to safeguard our plan assets

Learning Objectives

- Describe the latest cyber threat developments
- Identify where organizations can focus valuable risk mitigation resources
- Identify how to develop and refine a framework of knowledge to plan future security efforts and response strategies

Speakers

Beth Auterman
Principal, Employee Benefit Plans

Beth.Auterman@CLAconnect.com
217-373-3125

Randy Romes
Principal, Cybersecurity

Randy.Romes@CLAconnect.com
612-397-3114

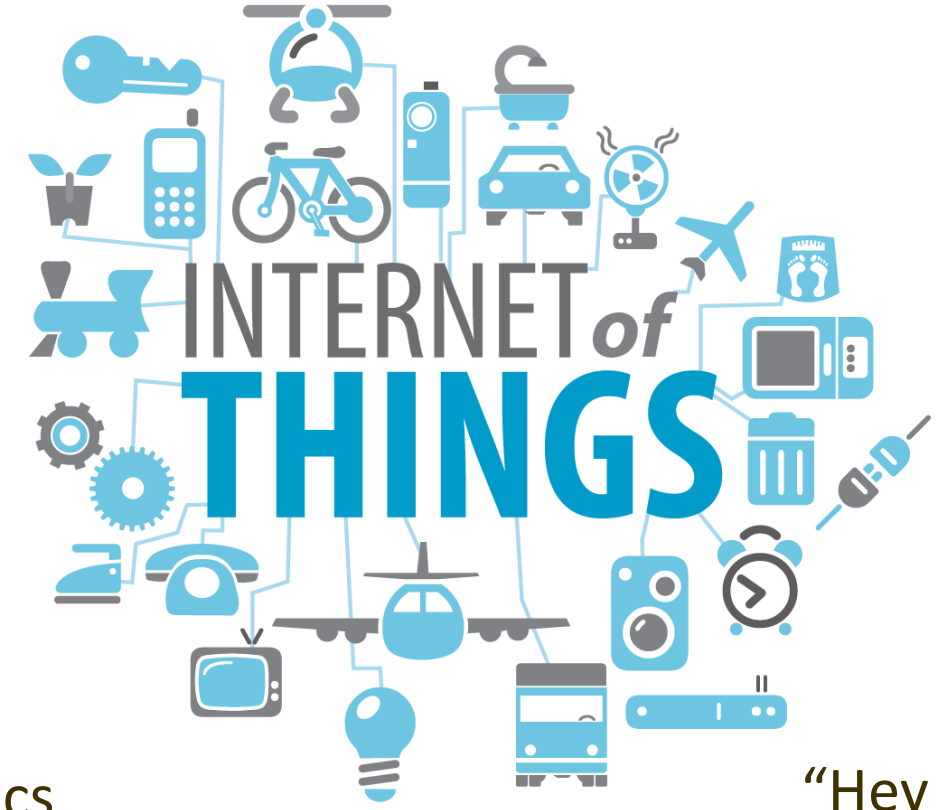
Cyber Security Services

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 (NIST, HIPPA, DOL, CIS, etc…)
- **PCI-DSS Readiness and Compliance Assessments**
- Incident response and forensics
- Independent security consulting
- Internal audit support

Raise Your Hand if You Work for a Tech Company

- Security Cameras
- Motion Sensors
- HVAC
- Print Vendors
- Smart TV Displays
- Temperature and Humidity
- Digital Assistance
- Cloud Applications & Analytics
- Logistics Monitoring/Tracking
- ➢ **“Presence”**



Security cameras

Garage door

Home thermostat

Cable TV remote

Smart TV

Sleep number bed

Roomba

“Hey Siri, what’s my balance?”

“Presence”

Sun Tzu:
"*Know your enemy and know yourself and you can fight a hundred battles without disaster*"

Why do cybercriminals like employee benefit plans?

Plans contain data hackers can use to withdraw funds and sell employee data.

Cybercrime and Black-Market Economies

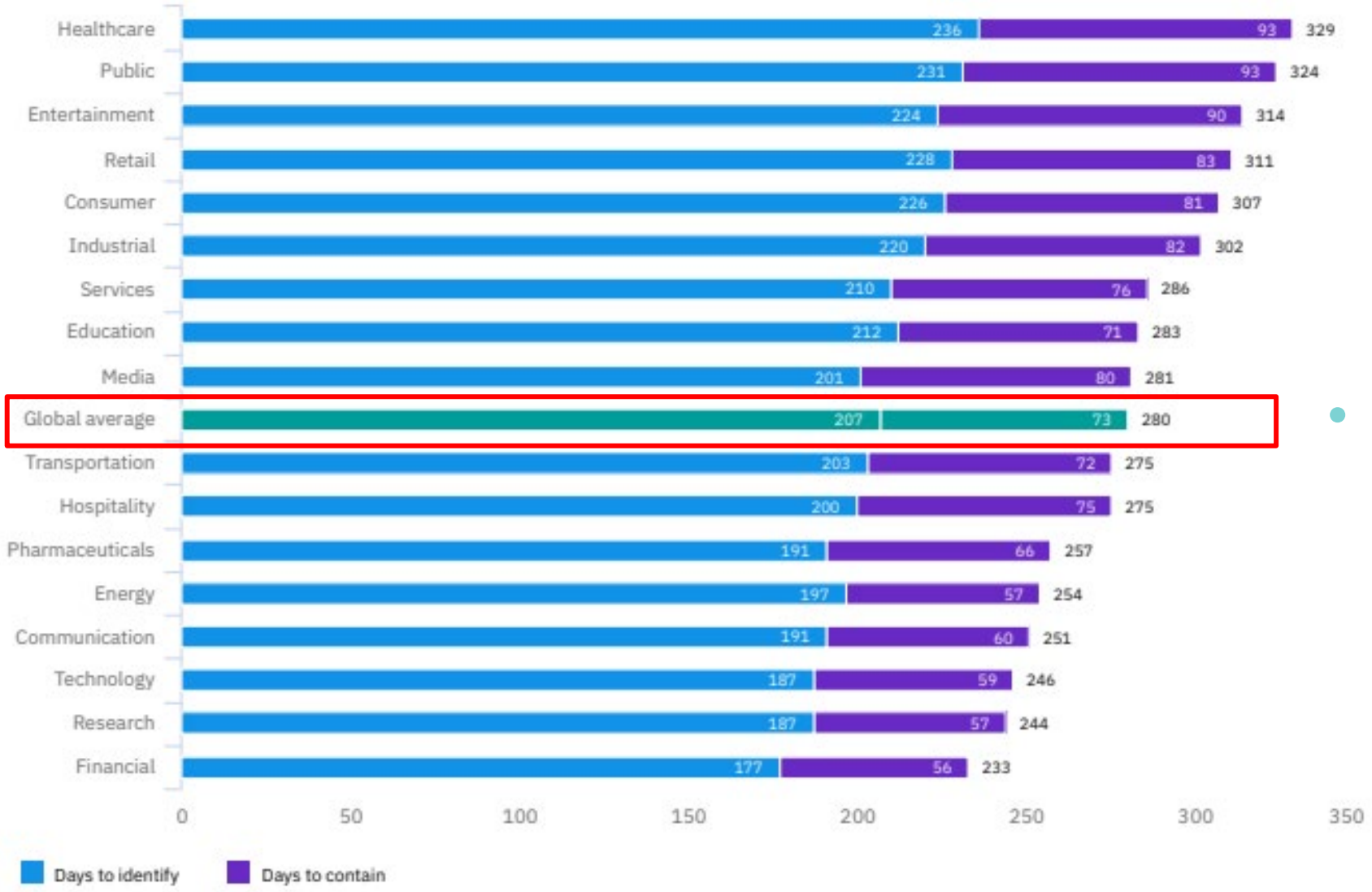
- Black market economy to support cyber fraud
  - Business models and specialization
  - Underground Marketplace (The Dark Web)

- Most common cyber fraud scenarios we see affecting our clients
  - Theft of information
    - Credit card information
    - PII and PFI
    - Log-in Credentials
  - Ransomware and interference w/ operations
  - To the Hackers, we all look the same…

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. Ransomware
5. Extortion to avoid breach disclosure

Average Days to Identify and Contain a Data Breach



- Global average is 280 days
  - 207 days to identify a breach
  - 73 days to contain the attack

Source: IBM Security Cost of a Data Breach Report 2020

A recent 2020 research on the Cost of a Data Breach conducted by Ponemon Institute and sponsored and published IBM Security noted:

Hackers can do a lot in 200 days…

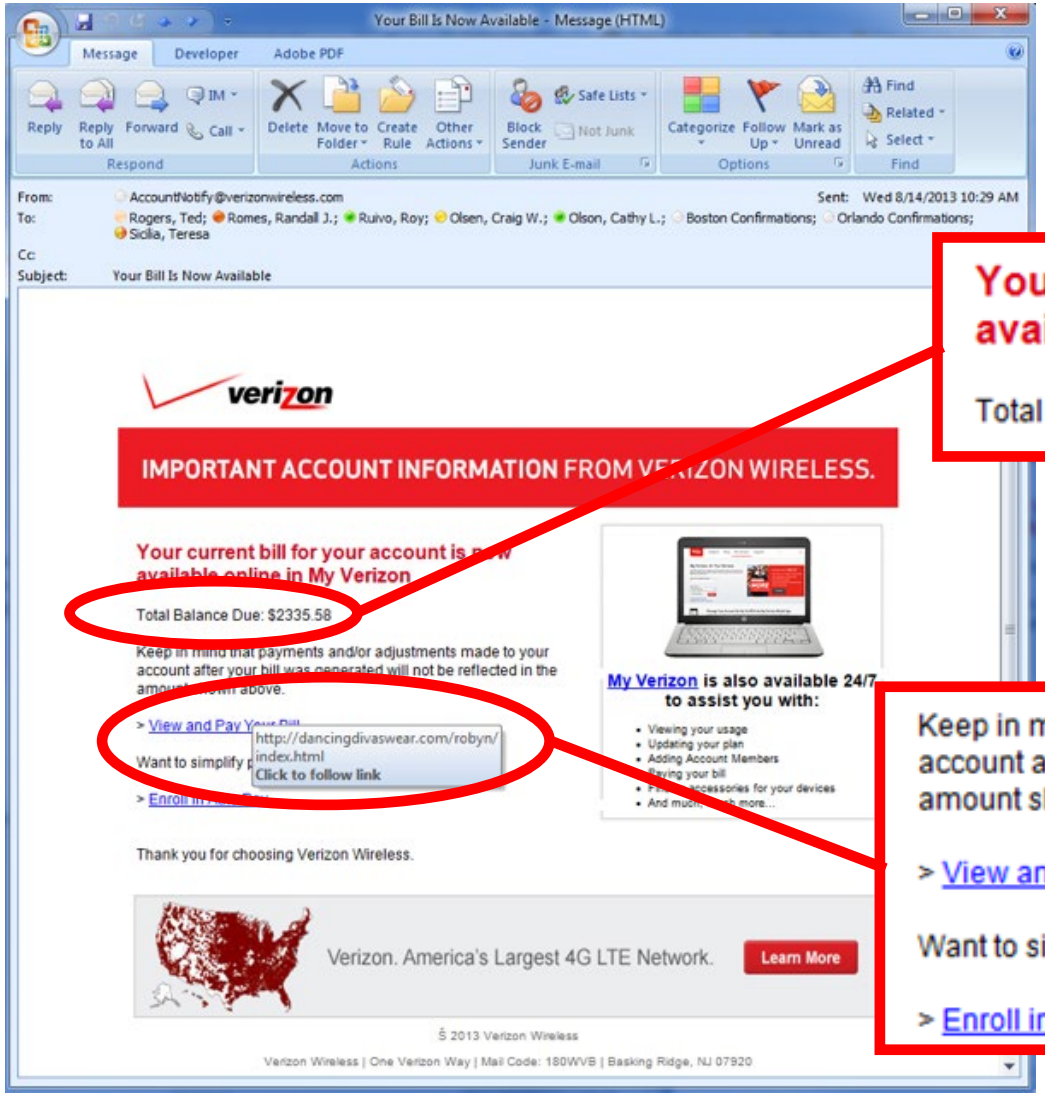
By the numbers:

- $8.64m – Average cost of a data breach in the United States
- 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?*

Your employee benefit plan just got hacked. Now what?

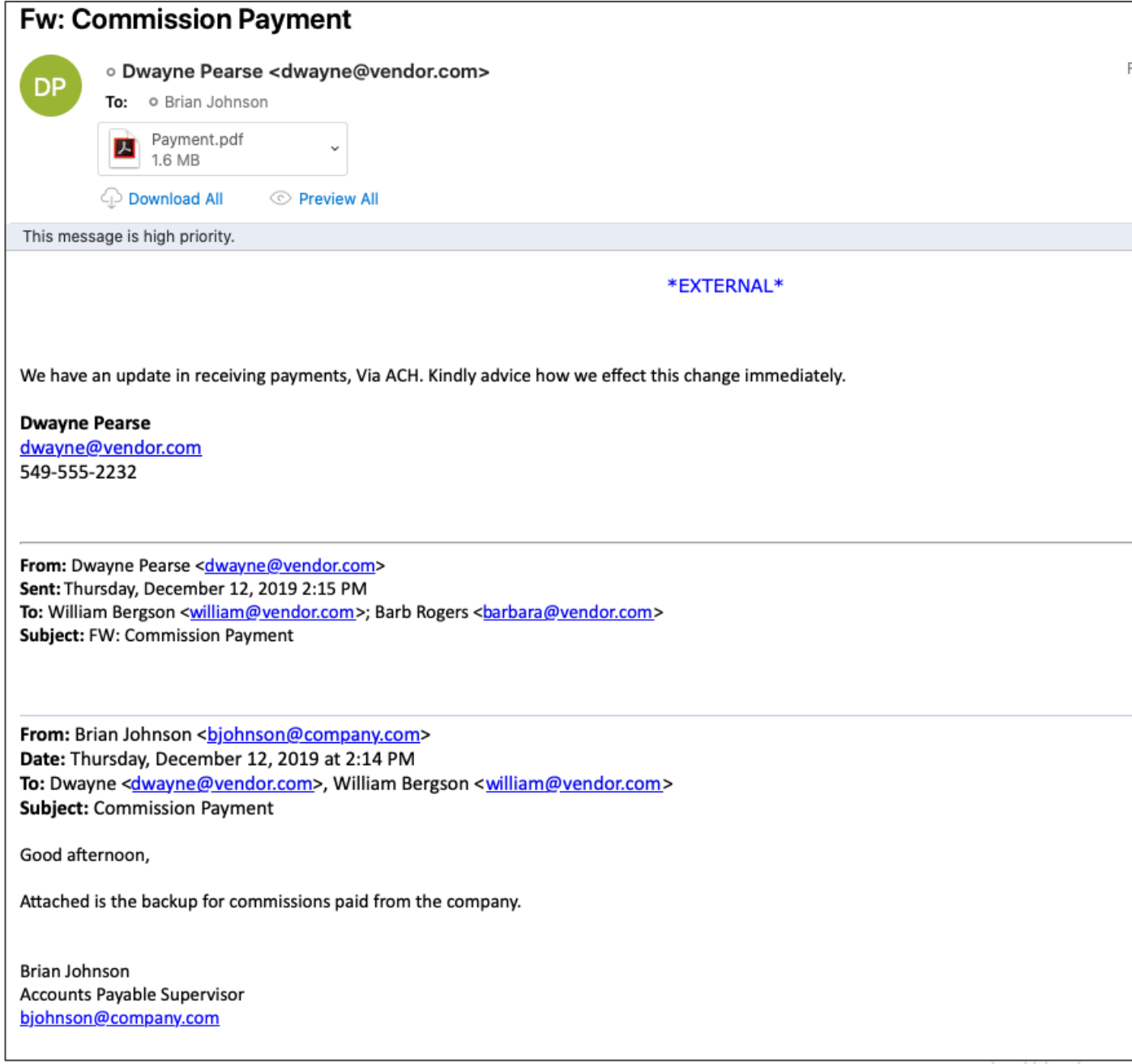
Like anything that lives online, any plan can be hacked.

Phishing?



Business Email Compromise

- Fraudsters impersonate employees, service providers, or vendors via email in an attempt to…
  - Steal or transfer $$$
  - Authorize a distribution
  - Impersonate an Executive asks staff to “buy gift cards”
  - Update direct deposit account



Fw: Commission Payment

DP

Dwayne Pearse <dwayne@vendor.com>

To: Brian Johnson

Payment.pdf
1.6 MB

Download All Preview All

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

Does Your Organization Already Use a Phishing Service?

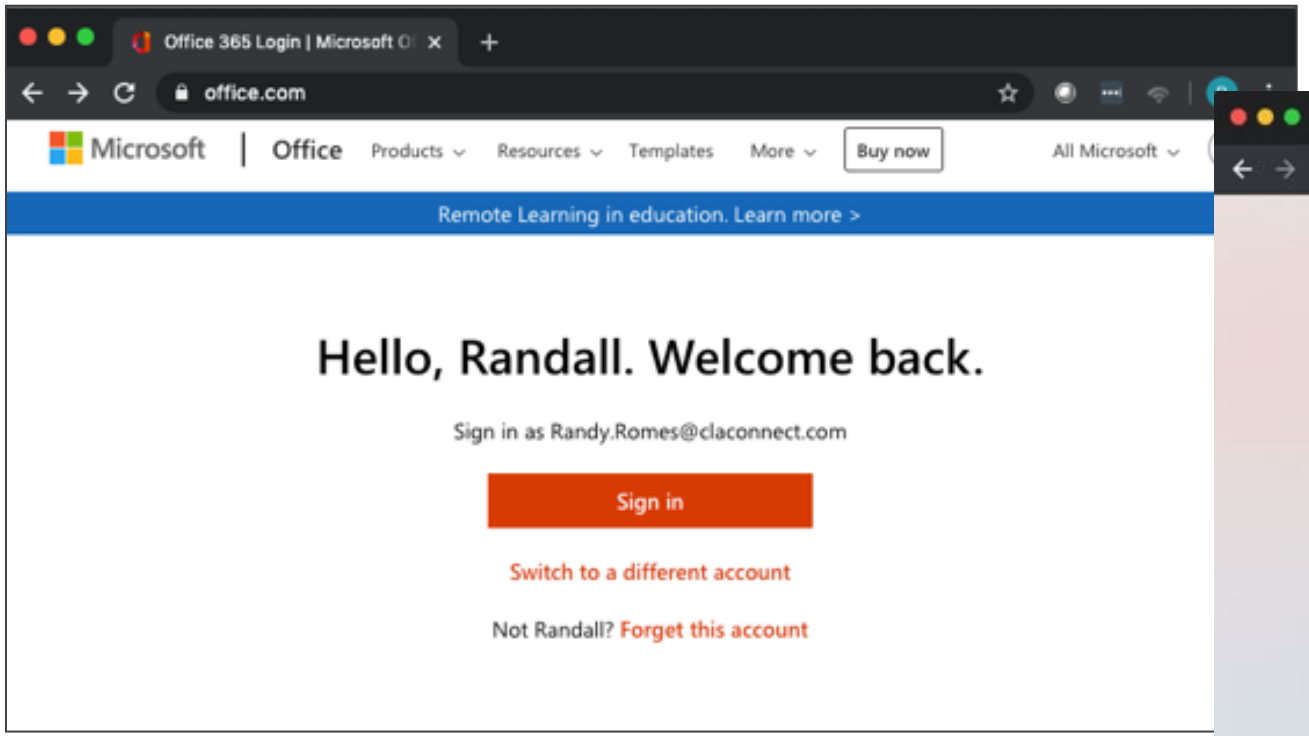
- "We already use _____"
  - "IT tests our people every ___"
  - "Click through rate is ___"
  - "Failures are required to take training…"
  - "We report results to the board quarterly…"

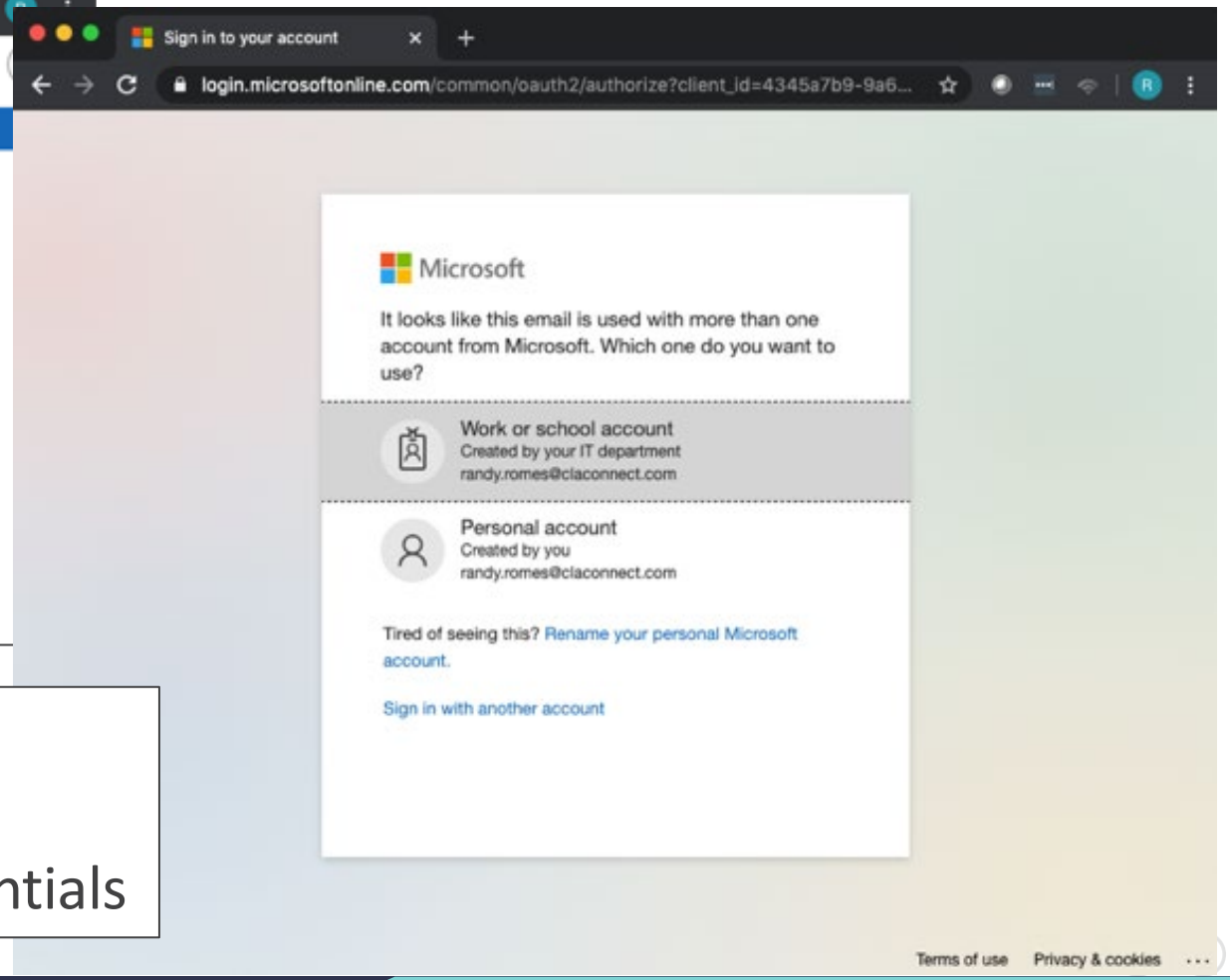
- These services are best categorized as training and training effectiveness measurement tools.
- They are NOT penetration testing…
- There is a "so what factor" that you may be missing…

Besides employees, who can access your EBP network?

Passwords are the keys to the kingdom…

Credential Harvesting and Password Guessing The Cloud is Ripe for the Picking





Attacks on Office365

- Password guessing attacks
- Phishing that harvests credentials

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 – Looooooong natural language**

Password21 <---------- ***Unforgiveable!***

Summer21 <---------- *Terrible*

*N*78fm/1* <---------- *Painful*

Wallet Painting lamp <-- GOOD

The Packers always beat the Bears! ← BEST

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

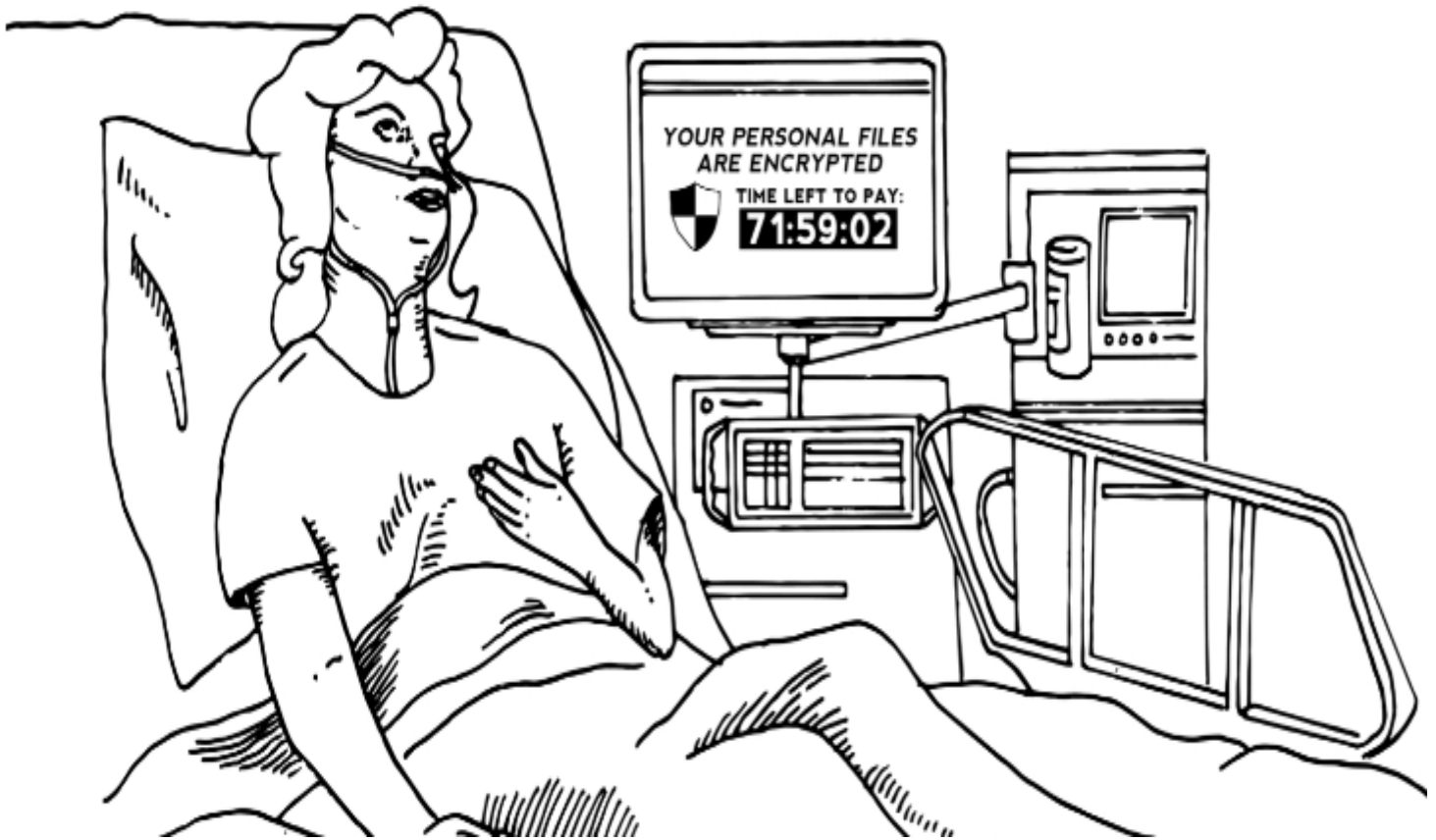
It’s a question you might have to answer if cybercriminals take your network hostage.

Ransomware

Ransomware bursts on the scene more than four years ago…

Hospital ransomware: A chilling wake-up call

Hollywood Presbyterian was forced to pay up, just like everyone else.



Latest Warnings / Ransomware / The Coming Storm — 76 comments

28 OCT 20 FBI, DHS, HHS Warn of Imminent, Credible Ransomware Threat Against U.S. Hospitals

On Monday, Oct. 26, KrebsOnSecurity began following up on a tip from a reliable source that an aggressive Russian cybercriminal gang known for deploying ransomware was preparing to disrupt information technology systems at hundreds of hospitals, clinics and medical care facilities across the United States. Today, officials from the **FBI** and the **U.S. Department of Homeland Security** hastily assembled a conference call with healthcare industry executives warning about an "imminent cybercrime threat to U.S. hospitals and healthcare providers."

The agencies on the conference call, which included the **U.S. Department of Health and Human Services** (HHS), warned participants about "credible information of an increased and imminent cybercrime threat to US hospitals and healthcare providers."

The agencies said they were sharing the information "to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats."

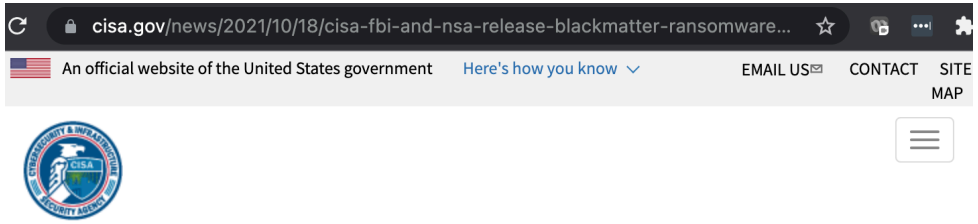
Late Last Year

Who will they set their sights on next?

https://krebsonsecurity.com/2020/10/fbi-dhs-hhs-warn-of-imminent-credible-ransomware-threat-against-u-s-hospitals/

Last WEEK!

Everyone has business operations at risk of denial of service and extortion.



CISA, FBI, AND NSA RELEASE BLACKMATTER RANSOMWARE ADVISORY TO HELP ORGANIZATIONS REDUCE RISK OF ATTACK

Original release date: October 18, 2021

WASHINGTON - The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) published a cybersecurity advisory today regarding BlackMatter ransomware cyber intrusions targeting multiple U.S. critical infrastructure entities, including two U.S. food and agriculture sector organizations. The advisory includes technical details, analysis, and assessment of this cyber threat, as well as several mitigation actions that can be taken to reduce the risk to this ransomware.

First seen in July 2021, cyber actors leveraged BlackMatter with embedded, previously compromised credentials that enabled them to access the network and remotely encrypt hosts and shared drives. When the actors found backup data stores and appliances on the network, not stored offsite, they wiped or reformatted the data. BlackMatter is a ransomware-as-a-service (Raas) tool, which means the developers are able to profit from cybercriminal affiliates (i.e., BlackMatter actors) who deploy it.

https://www.cisa.gov/news/2021/10/18/cisa-fbi-and-nsa-release-blackmatter-ransomware-advisory-help-organizations-reduce

Ransomware Attacks Continue to Evolve

- Earliest versions attack consumer availability
- 2nd generation attacked business availability & confidentiality
- Newest versions
  - Successful against all operating systems
  - Include Internet banking trojans (Zeus Sphinx Trojan)
  - Search for and encrypt back ups first
  - ➢ **FINISH with threat of data disclosure (DR is not enough…)**

➢ **If you have not tested your susceptibility to Ransomware…**

NOW… "STAND UP" (answer yes) if your company would be in a lot of trouble if you could not use your technology for TWO WEEKS

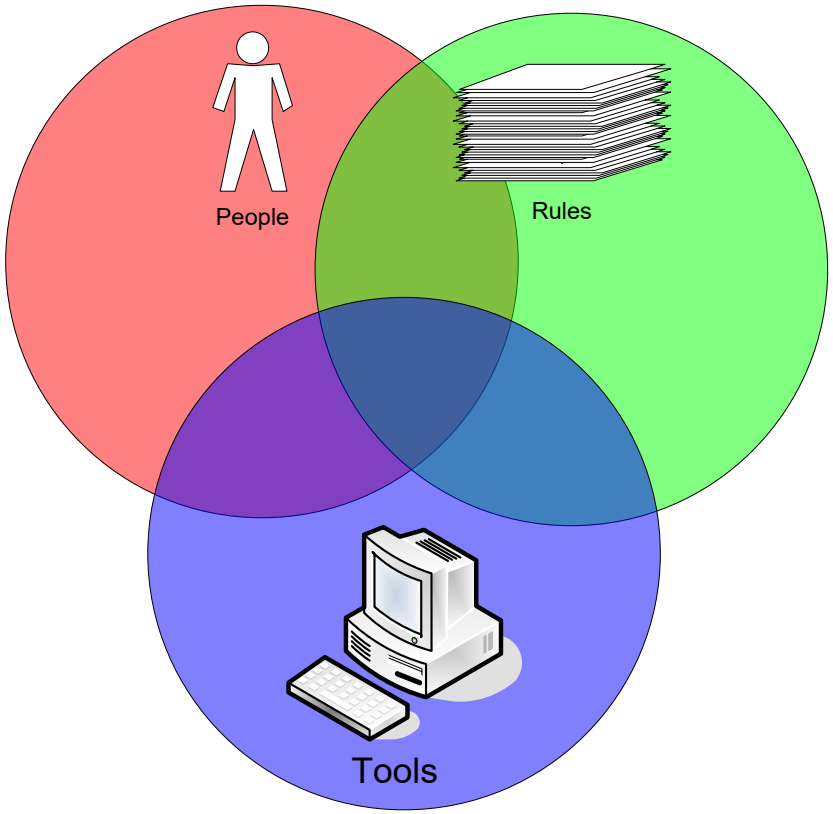
Is cybersecurity built into your employee benefit plan?

Plans without effective data security are easy pickings for cybercriminals. See what protection looks like.

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Policies and Standards

- 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 governance or compliance framework:
  - DOL, HIPAA, GLBA
  - PCI – DSS, CMMC
  - CIS Critical Controls, NIST

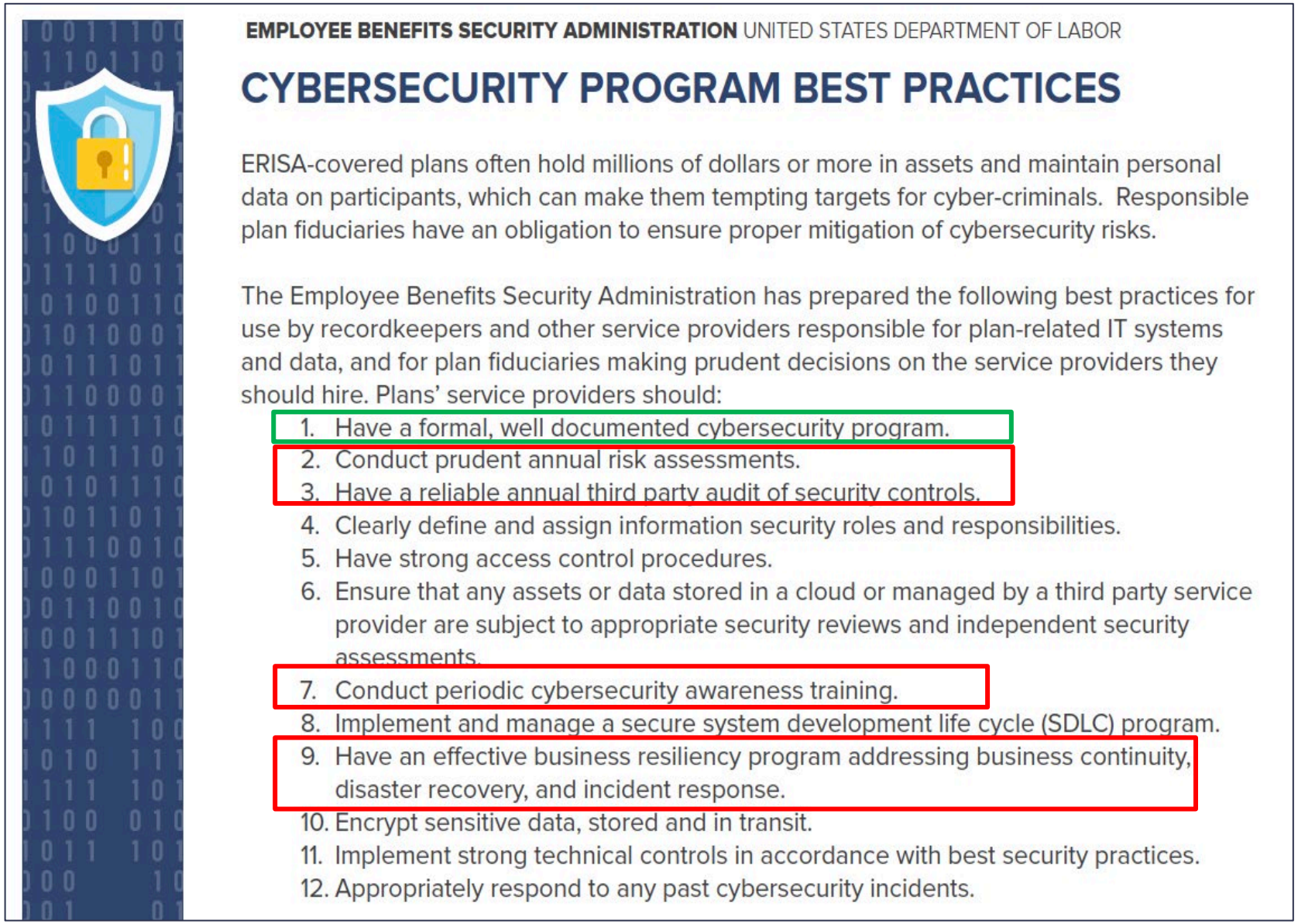
Department of Labor Requirements

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

CIS Controls™

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

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

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

Standards Based IT and Cyber Operations

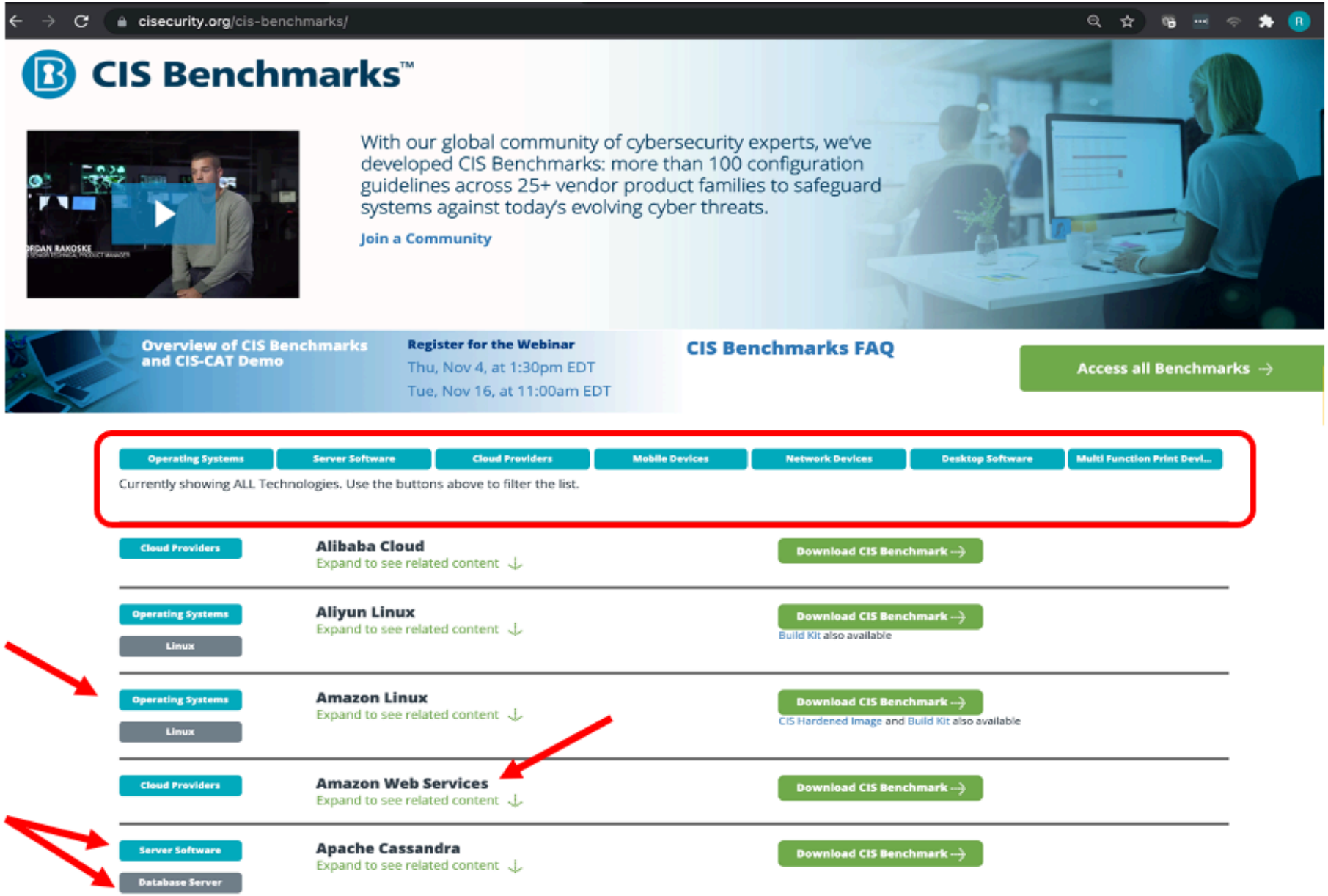
6. **Ensure that any assets or data stored in a cloud**

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

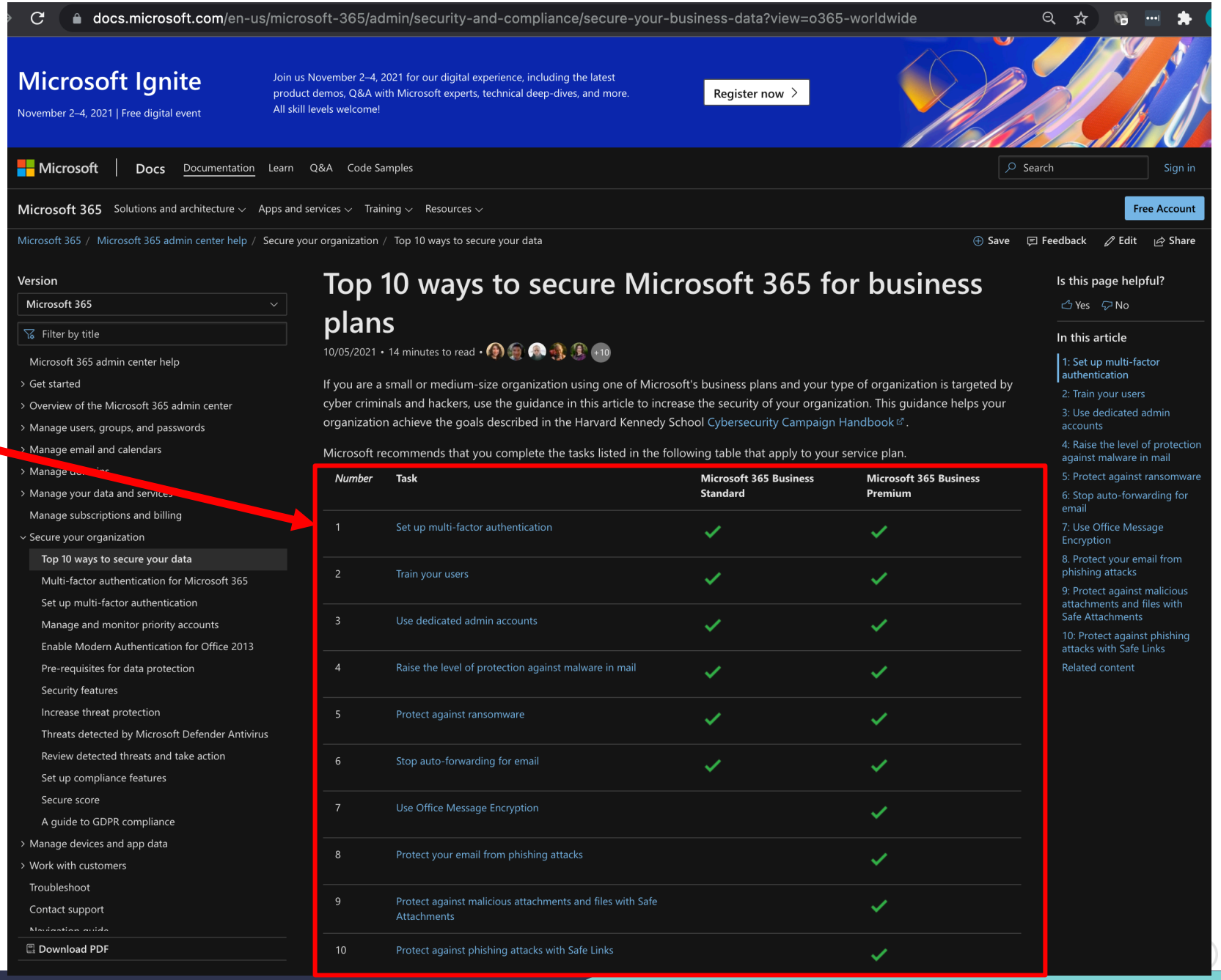
6. Ensure that any assets or data stored in a cloud

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…



The Boy Scouts Motto: *"Be Prepared"*

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

It's a question you might have to answer if cybercriminals take your network hostage.

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

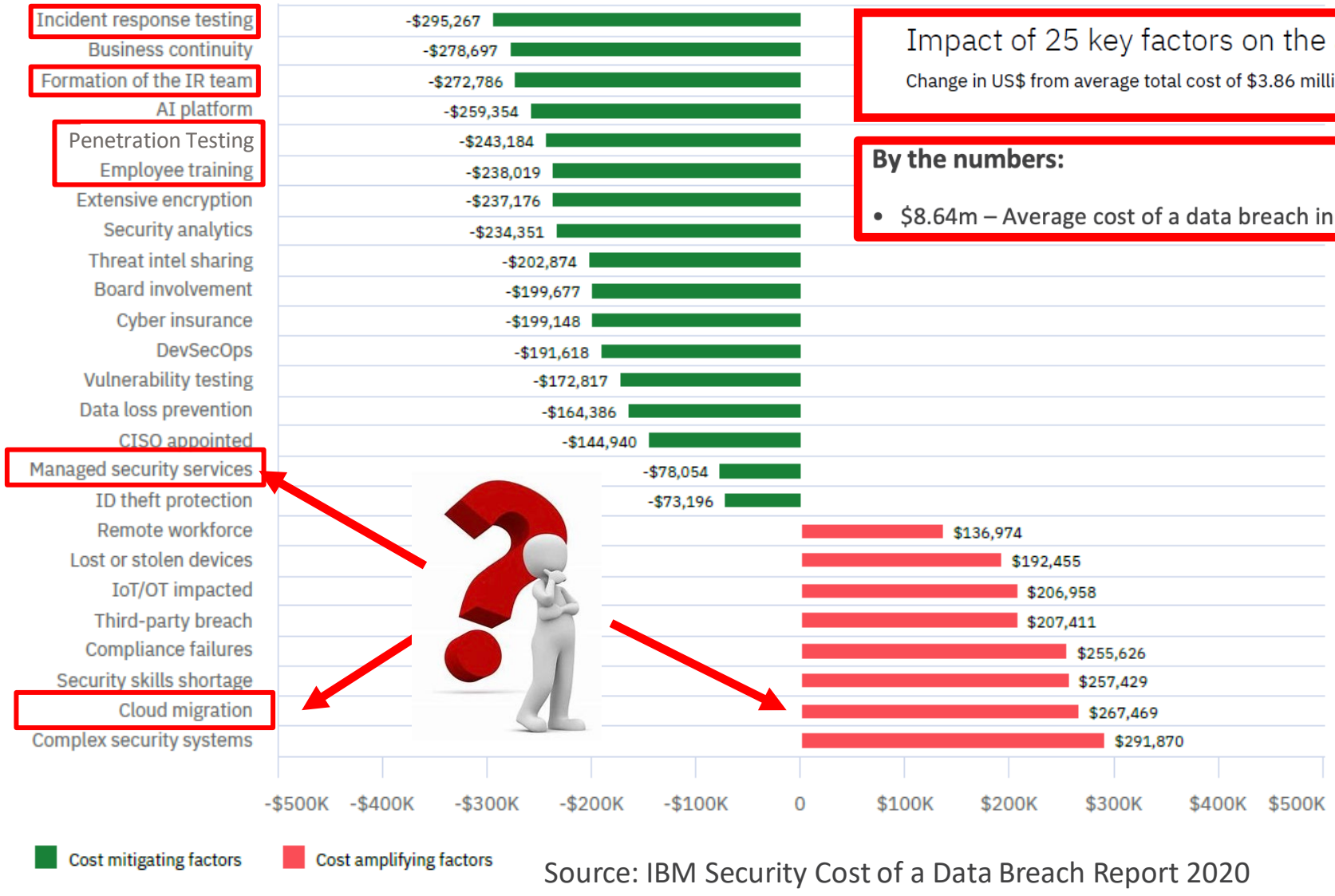
- Establish relationships with key incident responders
  - Breach Counsel
  - Forensic provider
  - Public relations

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 Preparedness- Cost Savings



By the numbers:

- $8.64m – Average cost of a data breach in the United States

Source: IBM Security Cost of a Data Breach Report 2020

3. Have reliable annual third party audit of security controls
4. Clearly define and assign information security roles and responsibilities
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…???

Boy Scouts Motto: Be Prepared…

Prepare

Operate

Test

- Risk Assessment at least annually
- Implement Standards Based Operations and Exception Management
- 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
  - Perform application testing
  - Engage independent penetration testing and vulnerability assessment (prove it)

Thank You!

Randy Romes, CISSP, CRISC, CISA, MPC, PCI-QSA
Principal – Cybersecurity Services
612-397-3114
Randy.Romes@claconnect.com

Beth Auterman, CPA
Principal – Employee Benefit Plans
217-373-3125
beth.auterman@CLAconnect.com