We'll get you there.

Data Breach Concerns
The Intersection Between Cyber & Financial Fraud

October 2023

CPAs | CONSULTANTS | WEALTH ADVISORS

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.

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 (HIPAA, GLBA/FFIEC, NIST, CMMC, CIS, etc.)
- PCI-DSS Readiness and Compliance Assessments (PCI-DSS)
- Incident response and forensics
- Independent security consulting
- Internal audit support

C:\whoami
> moth_man

- “Professional Student”
- Science Teacher / Self Taught Computer Guy
- IT Consultant - Project Manager → IT Staff/Help Desk → Hacker
- Assistant Scout Master (Boy Scouts)
- Boys Scouts Motto: Be Prepared

The Current Threat Landscape

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

- Phishing
- Account Take Overs
- Internet of Things
- Software Supply Chain Vulnerabilities
- Payment Process Controls
- Ransomware
- And finally… “Artificial Intelligence”

Cybercrime and Black-Market Economies

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

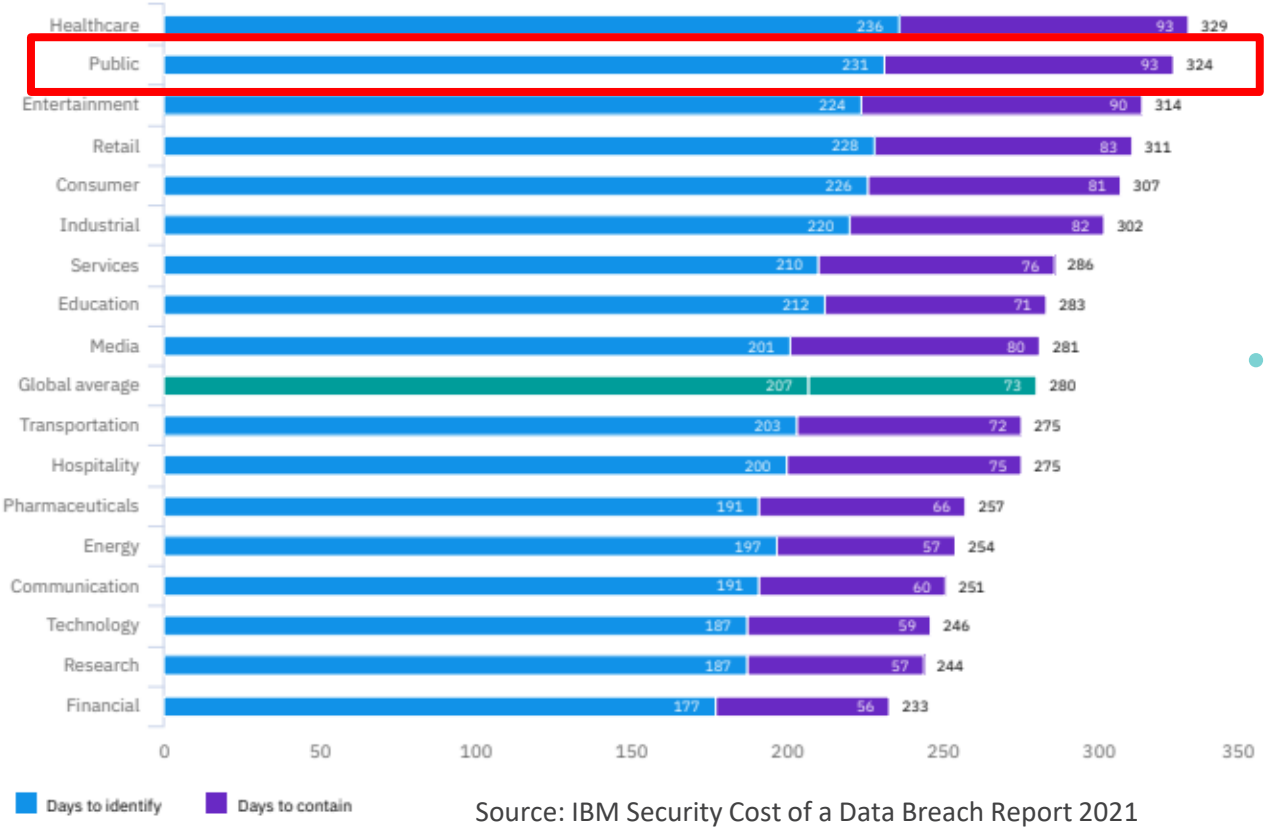
- Most common cyber fraud scenarios we see affecting our clients
  - Theft of information
    - Credit card information
    - ePHI, PII, PFI, account profiles, etc.
    - Log-in Credentials
  - Ransomware and interference w/ operations

➢ 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



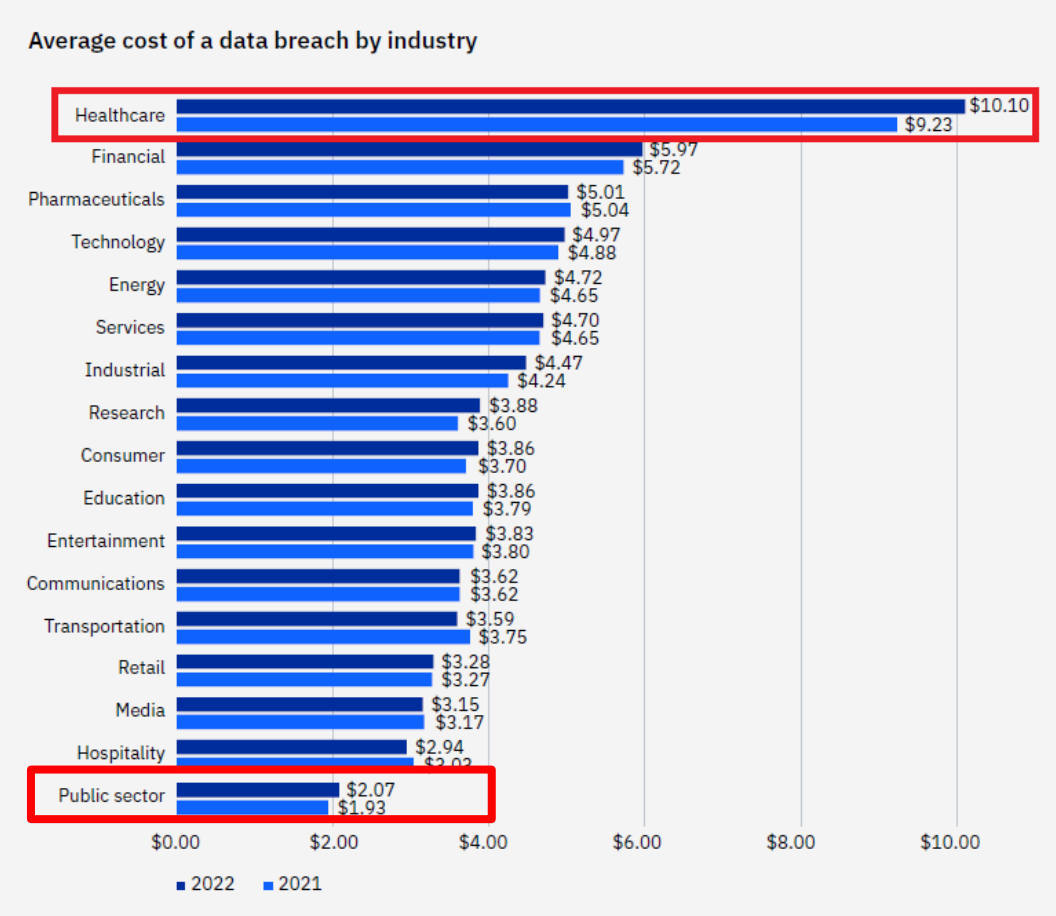
- Global average is 280 days
  - 207 days to identify a breach
  - 73 days to contain the attack

Source: IBM Security Cost of a Data Breach Report 2021

Behind the statistics

- ***What are they doing while they are inside for 231 days???***
  - Learn everything about your institution
  - Find your crown jewels and take them
  - Disable backups and security systems
  - Create numerous back doors

- Public portrayal of ransomware creates a **false sense of security**
  - Ransomware is usually coupled with other acts – Ransomware is simply the most visible part of the attack – it is usually “the last act”
  - Current ransomware attacks are coupled with data exfiltration
  - Resuming operations is just the first step
  - Legal and business ramifications of a data breach can persist



Measured in USD millions

Source: IBM Security Cost of a Data Breach Report 2022

2022 IBM Data Breach Study:

What does a breach cost?

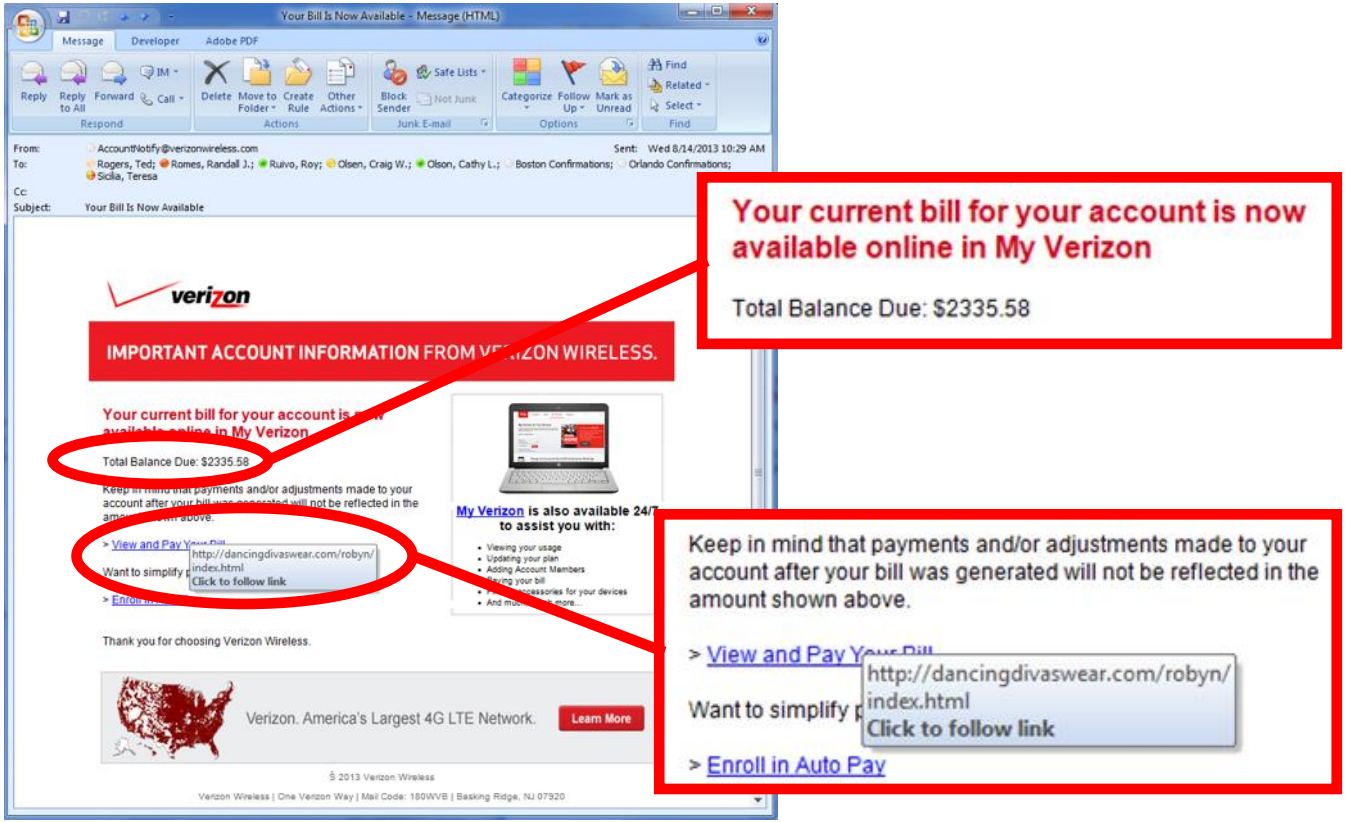
Email Spear Phishing

The Root Cause For More Than 85% of Breaches

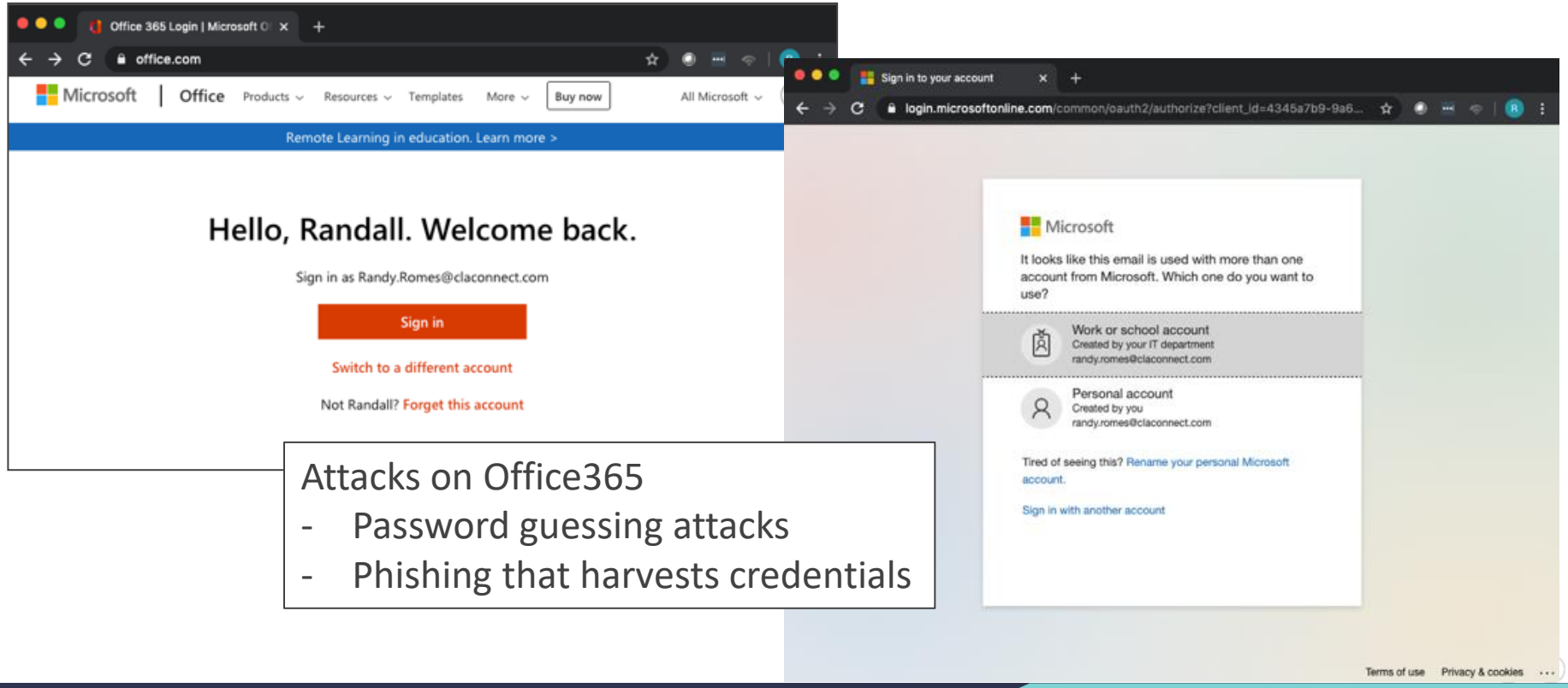
We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Spear Phishing



Credential Harvesting and Password Guessing:

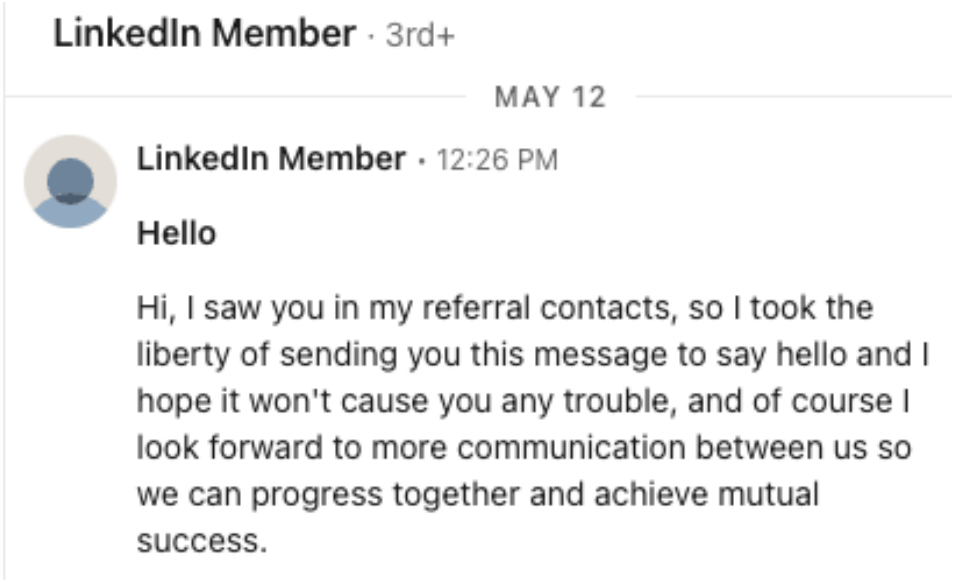


Attacks on Office365

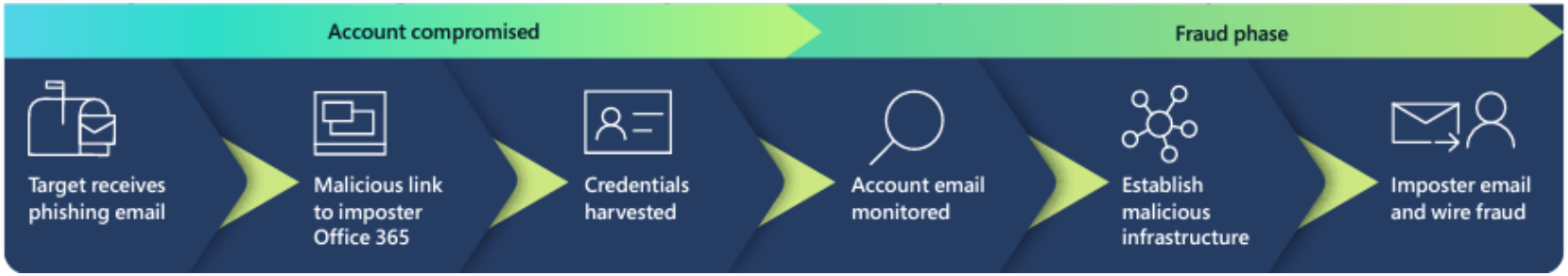
- Password guessing attacks
- Phishing that harvests credentials

BEC Lure

- Attacker starts a conversation with the victim to establish rapport
- Poses as a business colleague or business acquaintance
- Switches from LinkedIn to an introductory email (BEC lure)
- Phisher impersonates a legitimate sender to trick the recipient into clicking

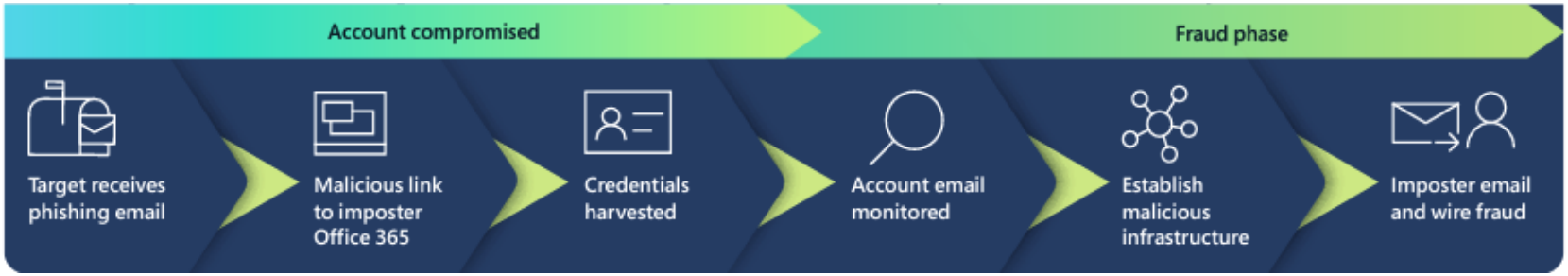


Phase 1 – Compromise of Credentials



- Credential leaks can be a result of phishing attacks or large data breaches
- The credentials are then sold or traded on the dark web

Phase 2 – Fraud Phase



- Attackers use compromised credentials to engage in sophisticated social engineering using homoglyph email domains

Homoglyph in Action

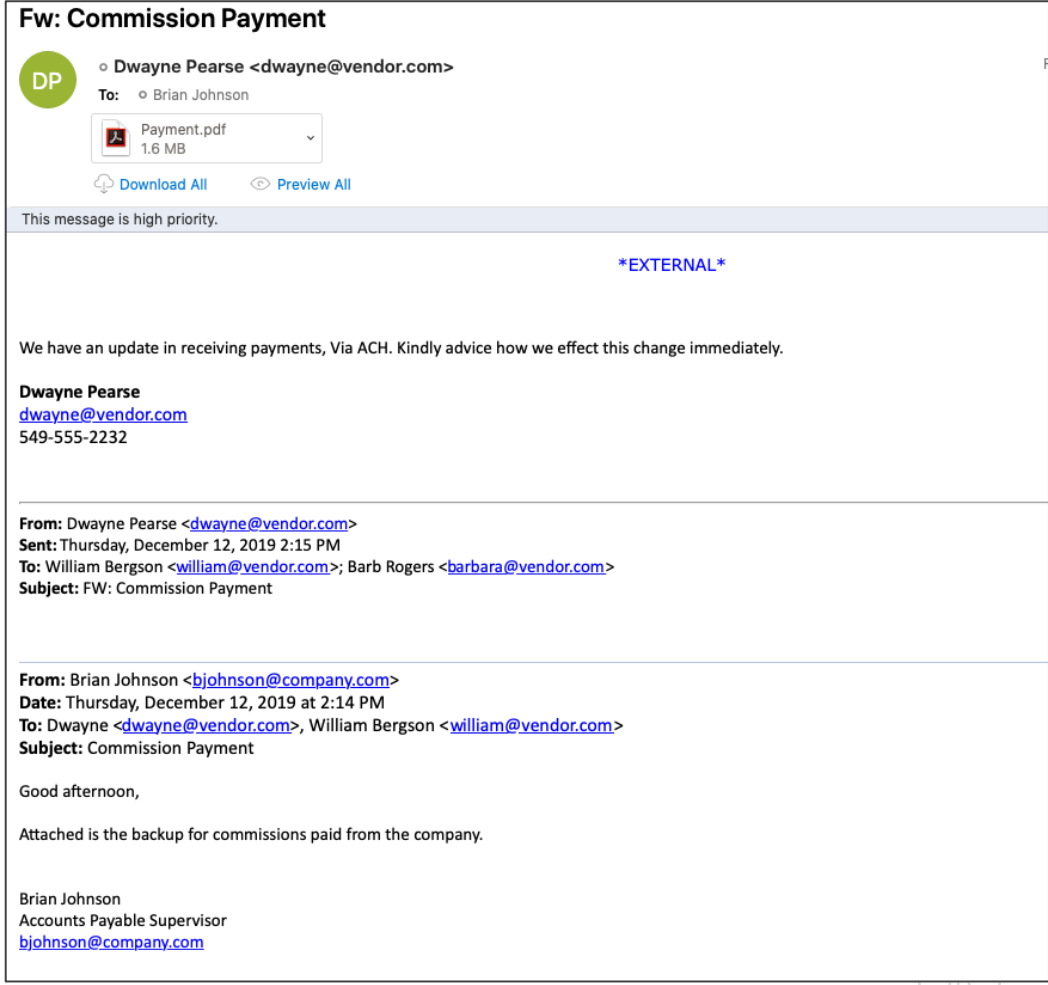
- A homoglyph domain that looks identical to a mail domain the victim recognizes is registered on a mail provider with a username that is identical
- Hijacked email is then sent from the hijacked domain with new payment instructions

Technique	% of domains showing homoglyph technique
sub l for I	25%
sub i for l	12%
sub q for g	7%
sub rn for m	6%
sub .cam for .com	6%
sub 0 for o	5%
sub ll for l	3%
sub ii for i	2%
sub vv for w	2%
sub l for ll	2%
sub e for a	2%
sub nn for m	1%
sub ll for I, sub l for i	1%
sub o for u	1%

Analysis of over 1,700 homoglyph domains between January–July 2022. While 170 homoglyph techniques were used, 75% of domains used just 14 techniques.

Business Email Compromise

- Fraudsters impersonate employees, service providers, or vendors via email in an attempt to…
  - EXAMPLE
    - Finance person phished
    - …gift cards…
    - IT staff “investigated…”
    - IT staff “shut it down”
    - We are good (right?)



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

Business Email Compromise - Examples

- FOUR EXAMPLES in the last 3 weeks…
- Finance person's email account is compromised….
  - Finance person phished
  - …gift cards…
  - IT staff "investigated…"
  - IT staff "shut it down"
  - We are good (right?)
- Issues
  - Retention time and data storage limits
  - IT is not equipped to perform incident response

Business Email Compromise and Payment Fraud

MANATEE COUNTY

Cyber criminals dupe Manatee County out of nearly $1 million

by: Trevor Sochocki
Posted: Apr 19, 2023 / 09:56 PM EDT
Updated: Apr 20, 2023 / 12:54 PM EDT

BRADENTON, Fla. (WFLA) — Nearly $1 million in taxpayer money is gone from Manatee County coffers this week after cyber criminals duped county officials into paying for what they thought was official business.

“There’s a lot of head-scratching that’s still going on,” said John Neal.

Neal is the president of Neal Land & Neighborhoods. He said his company built Fort Hamer Road in Manatee County years ago and the county has been paying him back in installments since then. But Neal Land & Neighborhoods expected another installment last Friday, it didn’t come.

“In our normal course of business, we reached out and we were informed that the payment had already been made,” Neal explained. “That’s how we became aware, and that’s really all that we know.”

The Manatee County Clerk’s Office had already sent the money to someone pretending to be Neal Land & Neighborhoods.

“It is roughly, for the last number of years,” Neal said. “About $800,000 a quarter to $1 million a quarter.”

In a statement, the clerk’s office said:

> *Late last week, we learned our county was the victim of a highly sophisticated fraud. It involved multiple entities at various stages of the payment process. As Comptroller, funds were delivered based on fraudulent information and documents for an authorized invoice. We are working with law enforcement, the county, and my cybersecurity consultant. We cannot provide specific details now, but we will when we are lawfully able, as this is an active criminal investigation.*
>
> - ANGEL COLONESSO, MANATEE COUNTY CLERK OF THE CIRCUIT COURT AND COMPTROLLER

But that money may be long gone.

“Once it’s wired to say, a bank in New York, and then a bank in New York wires it to a bank in Asia,” said Dr. Tom Hyslip. “Two, three steps, it’s gone. You’re not getting it back.”

Dr. Tom Hyslip is a cybersecurity expert and assistant professor of instruction at USF. He said hundreds of millions of dollars are lost every year to crimes just like this one.

BEC Example - Incident Timeline

- Controller leaves for planned vacation to Africa (off grid)
- Management discovers $488,200 payment to an unrecognized third party with a foreign bank account
- Note the payment was approved by the Controller but no other paperwork exists (they think she took the money)
- Management finds out there are 2.2 million in paid invoices
- Upon investigation there are deleted emails from, and suspicious devices logged in as CFO

Hacker Events

- Hacker uses breached email account from another non-vender business to phish CFO
- Hacker registers second phone number to maintain persistent access
- Hacker sets up auto forwarding rules to delete and hide emails from CFO

Hacker Events

- Using the CFO's email, hacker contacts Controller and says they are processing another batch of past due invoices and has a conversation about the next run

- Hacker then asks to Controller to register vendor "L and B investments LLC" and process $88,000 payment (5/26)

- Payment requests (8 in total) keep coming in every couple days escalated values into the 100s of thousands topping out at $488,000

Lessons Learned

- No lock down of Azure AD Join or MFA registration (can be done in conditional access)
- Policies to block Risky sign ins not enabled
- Users can register additional MFA and MFA is not phishing resistant
- No blocking or alerting on auto forward rules

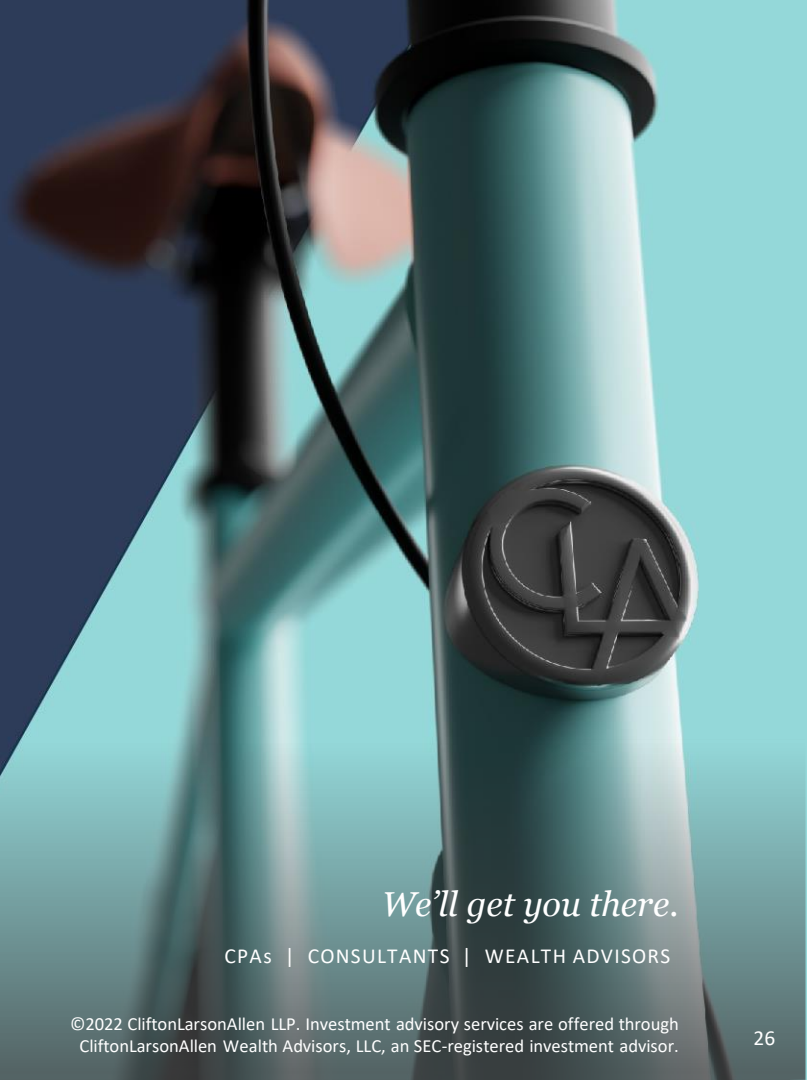
Does Your Organization Already Use a Phishing Service?

- "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…**

Attacking the Supply Chain Enterprise Software

SolarWinds Orion, Kronos, MoveIT

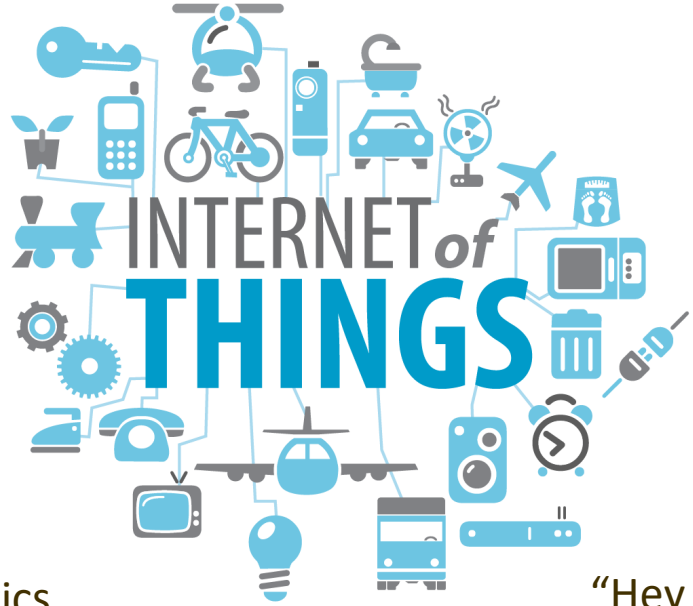


We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Raise Your Hand if You Work for a Tech Company

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



Security cameras

Garage door

Home thermostat

Cable TV remote

Smart TV

Sleep number bed

Roomba

“Hey Siri, what’s my balance?”

Apple Watch or FitBit

“Presence”

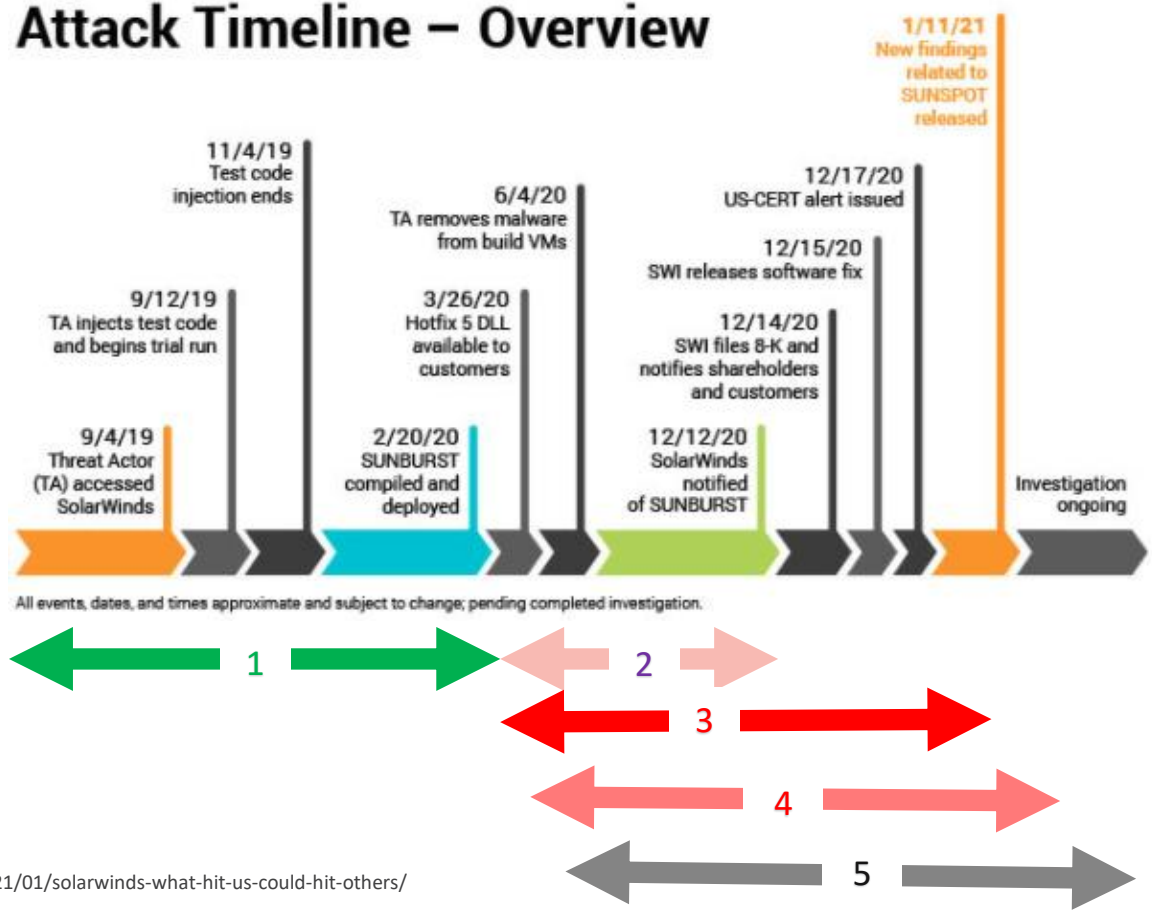
Are You Prepared?

Enterprise Software Platforms

1. Microsoft Exchange (in-house)
2. Microsoft Office 365 (email, Teams, OneDrive, etc…)
3. SolarWinds Orion
4. MoveIT
5. Kronos

Timeline of Events

Krebs On Security



https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/

Take-Aways and To-Dos (ie. on the fly IR)

1. Do we use SolarWinds Orion?
   - If ***NO*** → Go to 6
   - If YES → What version?
2. Is our version the affected version (see SW advisory)?
   - If ***NO*** → Go to 6
   - If YES → Continue
3. Have we created a timeline of potential exposure?
4. What logs do we have and how far back in time do they go?
5. What Indicators of Compromise (IOC's) have we searched for?
   - What resources/references have we used to identify known and potential IOC's?
   - Use 3 and 4 to search for IOC's
6. Do we have any third-party service providers with trusted access?
   - Who has remote access into our environment?
   - Who do we push our data out to?
   - Are there any persistent open connections to or from third parties?
7. Repeat 1-5 for those identified in 6

Software Vendor/Supply Chain Risk Management

- All software products have bugs/vulnerabilities
  - Key questions:
    - What does this software application have access to?
    - What user account/privileges are given to it?
    - What is the software vendor doing to provide us a level of comfort that they have done their due diligence?
    - 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?

The Supply Chain Exposing Us Embedded / Open-source Software

Log4j and Other Imbedded Software Components

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

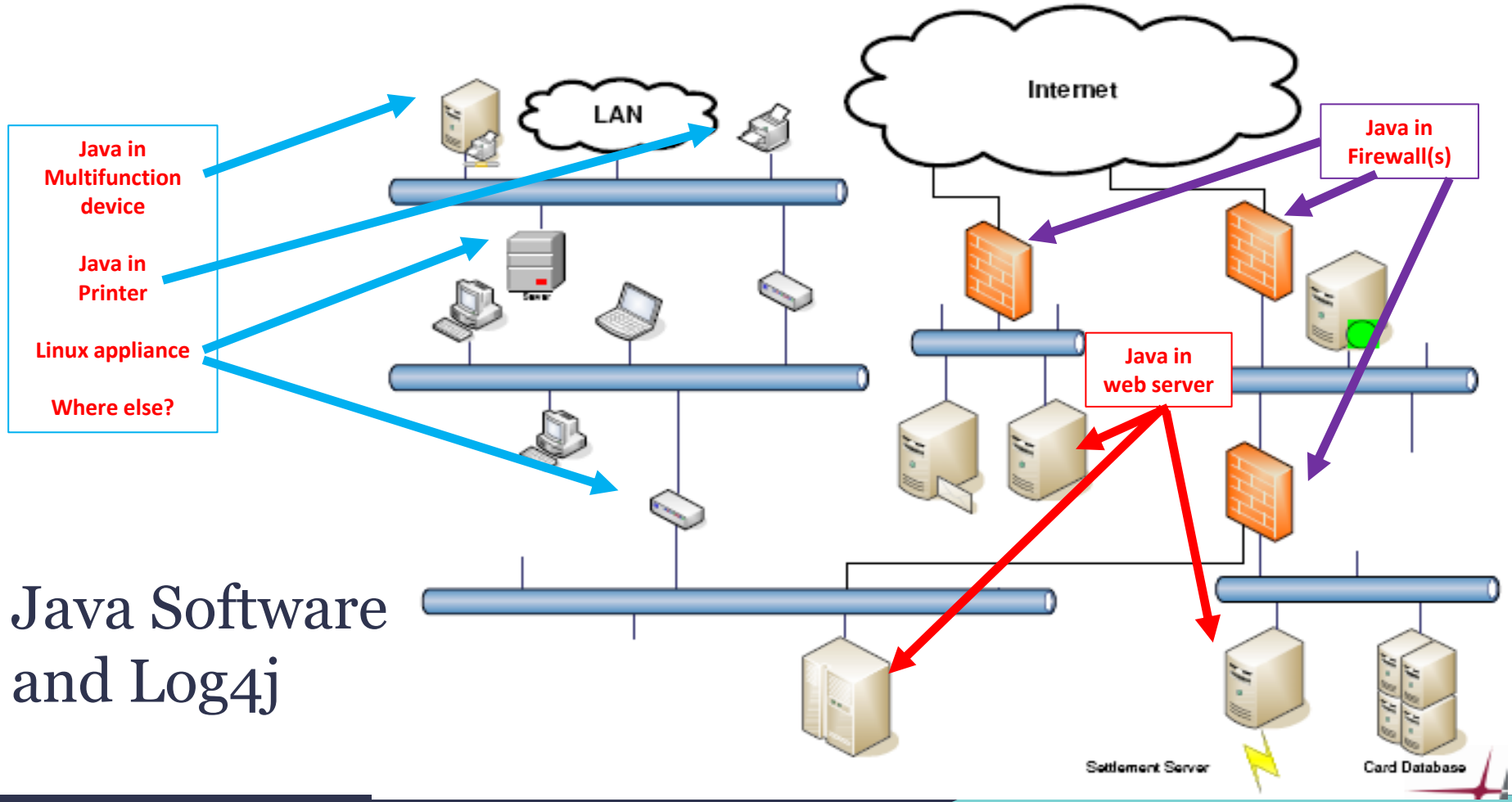
Software Vendor/Supply Chain Risk Management

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

- Inventory
- Controlled use of Administrative Access
- Secure Standard Builds
- Vulnerability Management
- Logging, Monitoring and Alerting

- Vulnerable API Interfaces and Web Services

Take-Aways and To-Dos (i.e., IR)

- Have a plan
  - Incident Response Play Book(s)
  - Disaster Recovery Plan and Procedures
  - Business Continuity Plan supported by Business Impact Analysis

- Know how the vendors fit into and support the plan
  - Service provider responsibility matrix

- Practice the plan
  - Tabletop exercises
  - Live exercises
  - Regularly review and update the Plan(s)

Interference With Operations & Extortion

Ransomware is not going away…

We'll get you there.

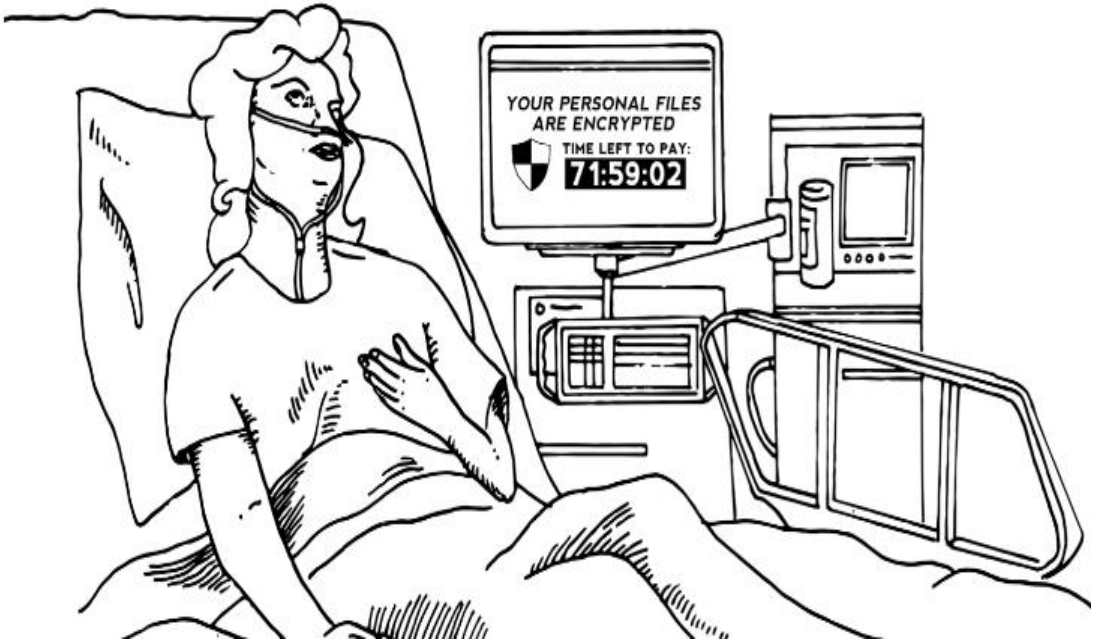
CPAs | CONSULTANTS | WEALTH ADVISORS

Ransomware

Ransomware bursts on the scene more than eight years ago…

Hospital ransomware: A chilling wake-up call

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



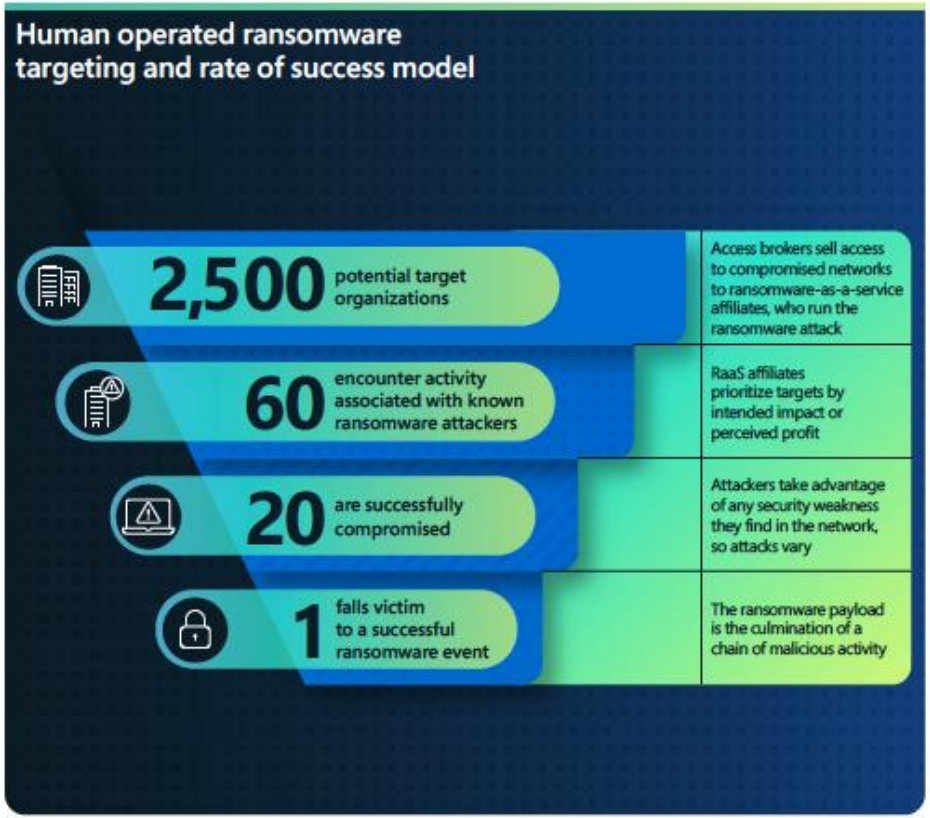
Ransomware Attacks Continue to Evolve

- Earliest versions attack consumer availability
- 2nd generation attacked business availability & confidentiality
- Newest versions
  - Successful against all operating systems
  - Search for and encrypt back ups first
  - Compromise data – attack all three of the CIA:
    - Confidentiality of data
    - Integrity of data
    - Availability of data

Ransomware

➢ **FINISH with threat of data breach disclosure (DR is not enough…)**

Human Operated Ransomware



Model based on Microsoft Defender for Endpoint (EDR) data (January–June 2022).

Human Operated Ransomware

- Attackers need credentials to succeed in their operations.

- The successful human operated ransomware infection of an entire organization relies on access to a highly privileged account.

Ransomware

Jackson County government gives in to hackers and pays $400,000

Paying up is cheaper than the alternative

By Isaiah Mayersen on March 10, 2019, 11:27 AM | 20 comments

Recap: A little over a week ago government computer systems in Jackson County, Georgia were hit with one of the most sophisticated ransomware attacks attempted in the US. After a week with their entire computer and internet network down, they've decided to cough up $400,000 to regain control of their systems and to retrieve stolen files.

Employees first noticed that government computers, websites and even email addresses had stopped functioning sometime on March 1. While fortunately 911 emergency calls were still operational, every internet connected device was inoperable and it is possible that the hackers were able to steal police and county records, too.

"Everything we have is down," Sherriff Janis Mangum told StateScoop. "[But] we've continued to function. It's just more difficult."

Ransomware

BOS chairman speaks about the county cyber attack

By Staff Reporter May 6, 2019 0

File photo

IMPERIAL COUNTY — "We apologize for the inconvenience and disruption associated with the recent cyber-attack," Board of Supervisor chair Ryan Kelley said in a recent press release.

The Imperial County network is operational, Kelley went on to say, and communications have been restored. A few information systems are experiencing hiccups that are being addressed daily.

"Believe me, we are not keeping secrets from the public, "Kelley said in the release. "At the advice of our cyber security firm in consultation with our insurance carrier, we did not share the ransom demand amount nor the ransom attack details. Once we made a decision to rebuild, we did not want the hackers to know and potentially cause further damage."

Kelley said it was safe to reveal the details of the ransom, saying the hackers demanded over $1.2 million dollars in bitcoin for a keycode to defragment the information. The ransom payment would require the same network rebuilt as being completed today to ensure the hacker group no longer had access to county systems. The release said the estimated cost of this option was $4 million.

"Our board decided to not pay the ransom demand and, instead, rebuilt our network," Kelley said in the release. "To date, the County of Imperial has expended $1.4 million dollars to rebuild the network, and additional costs are expected. The release said insurance coverage will provide reimbursement for the majority costs associated with the rebuild.

Over the past two weeks, federal law enforcement was able to share the Imperial County ransomware attack with other public and private agencies across the country, per the release. The county said it has released information when possible with the main purpose of protecting Imperial County from any additional attacks and any other agencies being targeted by this group.

"We have identified the county computer that initiated the spread of this attack; however, there is no need to identify the individual," Kelley said in the press release. "It is not fair to the individual or county employees to single out an individual for a sophisticated attack that could fool any of us."

The county said that the information services unit, in collaboration with specialized assistance, have done exceptional work to bring the county network back to the public and county employees. The unit has installed firewalls and intrusive detection systems to block any additional intrusions and will continue monitoring the system. In addition, Imperial County Information Services is building a training platform for staff education and identifying malicious emails.

Preventing Ransomware

1. Build credential hygiene
2. Audit credential exposure
3. Prioritize deployment of AD updates
4. Prioritize cloud hardening
5. Reduce the attack surface
6. Harden internet-facing assets and understand your perimeter
7. Reduce SOC alert fatigue

- **If you have not tested your susceptibility to Ransomware…???**
- **If you have not tested your recovery capabilities, from bare metal up…???**

Standards Based Operations

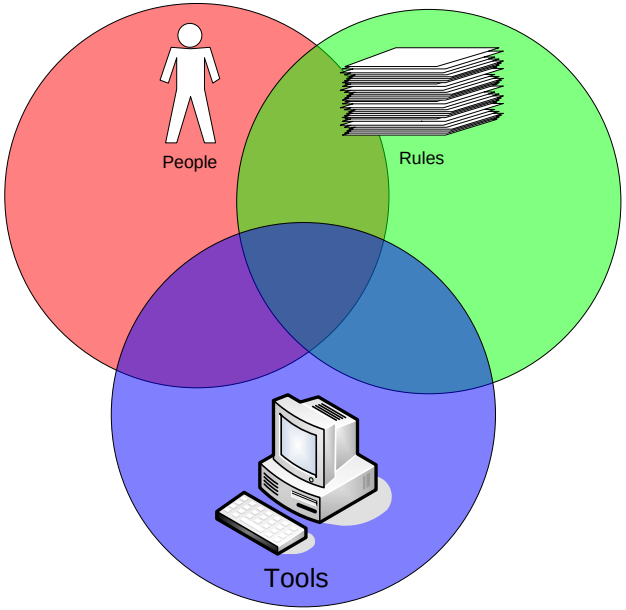
“People, Rules, and Tools”

We’ll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Policies and Standards

- Security is not a product
- 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:
  - HIPAA, GLBA, (State Laws?) ----- *Regulatory*
  - PCI – DSS, CMMC ----- *Contractual*
  - CIS Critical Controls, NIST ----- *Operational standards*



CIS Controls™ V7

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

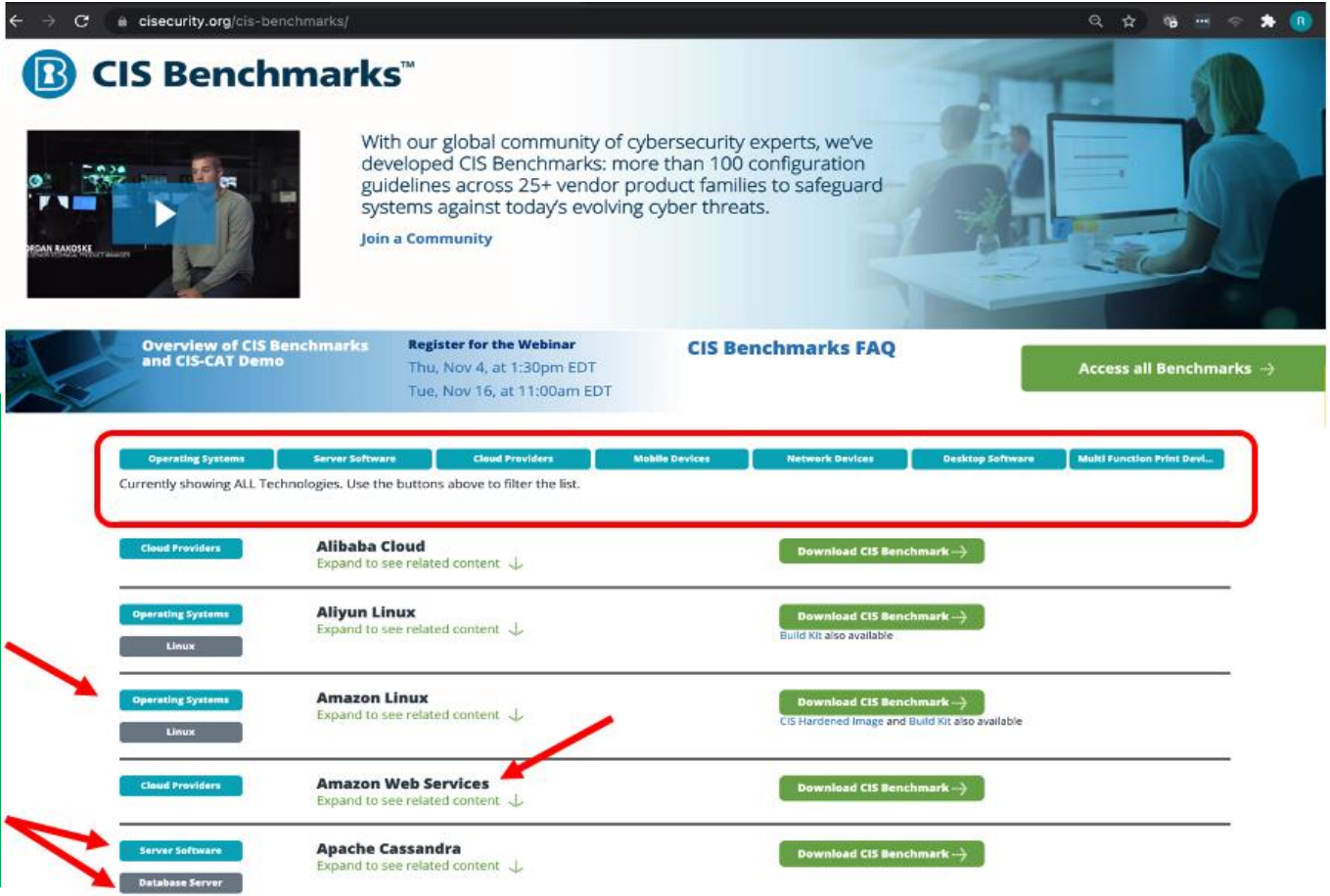
https://www.cisecurity.org/controls/

Standards Based IT and Cyber Operations

CIS Benchmarks

Checklists and How-to guides for just about everything

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



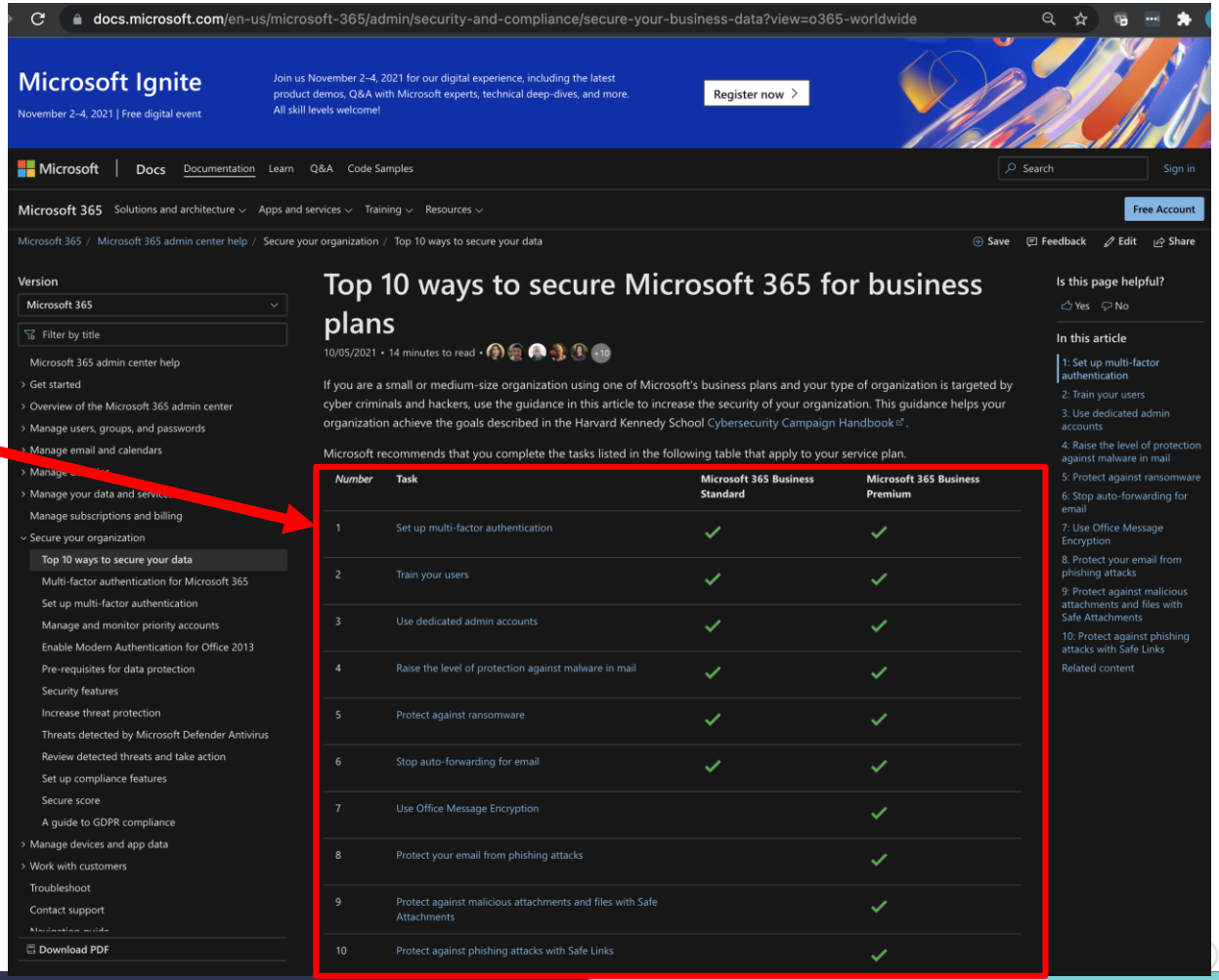
Secure Office 365

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

- ➢ Security configurations need to be periodically assessed.

- ➢ **Logging is based on license level.**



Operational Discipline

- Disciplined change management
- Consistent exception control and documentation
  - Should include risk evaluation and acceptance of risk
  - Risk mitigation strategies
  - Expiration and re-analysis of risk acceptance

Payment Process Discipline

- Say it with me: “Email is not secure…”
- Review and update your payment process
  - Payment requests
  - Change requests
  - White lists
  - Authorization process
  - Email should NOT be relied on as source of _____
- Say it with me: “Email is not secure…”

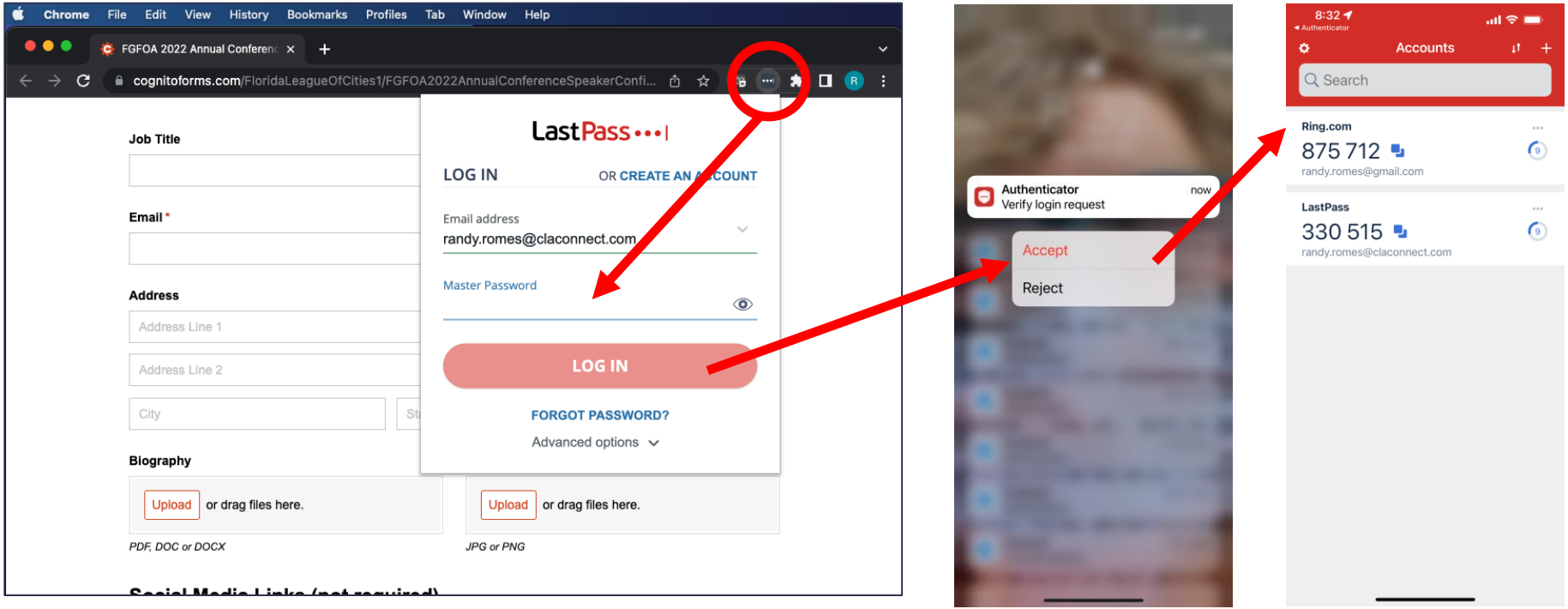
Passwords

- Old Rules (NIST – 2005?)
  - Length (8+ characters)
  - Complexity (Aa4@)
  - Forced expiration (every_____)
- New Guidance (NIST – 2018?)
  - Looooooooong Passwords
  - No expiration
  - Especially important for administrative accounts (CIS 4)

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:

- Password tools: MFA and Password Managers are needed



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
- Audit your passwords

Disaster Recovery & Business Continuity

- Inventory of assets and results of risk assessment are crucial
  - Hardware and software
  - Critical data elements (“the crown jewels”)
    - Data Retention policies and standards
    - Where is the data (if we know where it is, we know where to apply controls)
  - Critical business processes
- **Business impact analysis** with definition of recovery point objectives
  - This is another name for a specialized type of risk assessment
  - Defines priority for restoration
- Disaster Recovery is periodically practiced
  - Need to make sure it works the way you expect

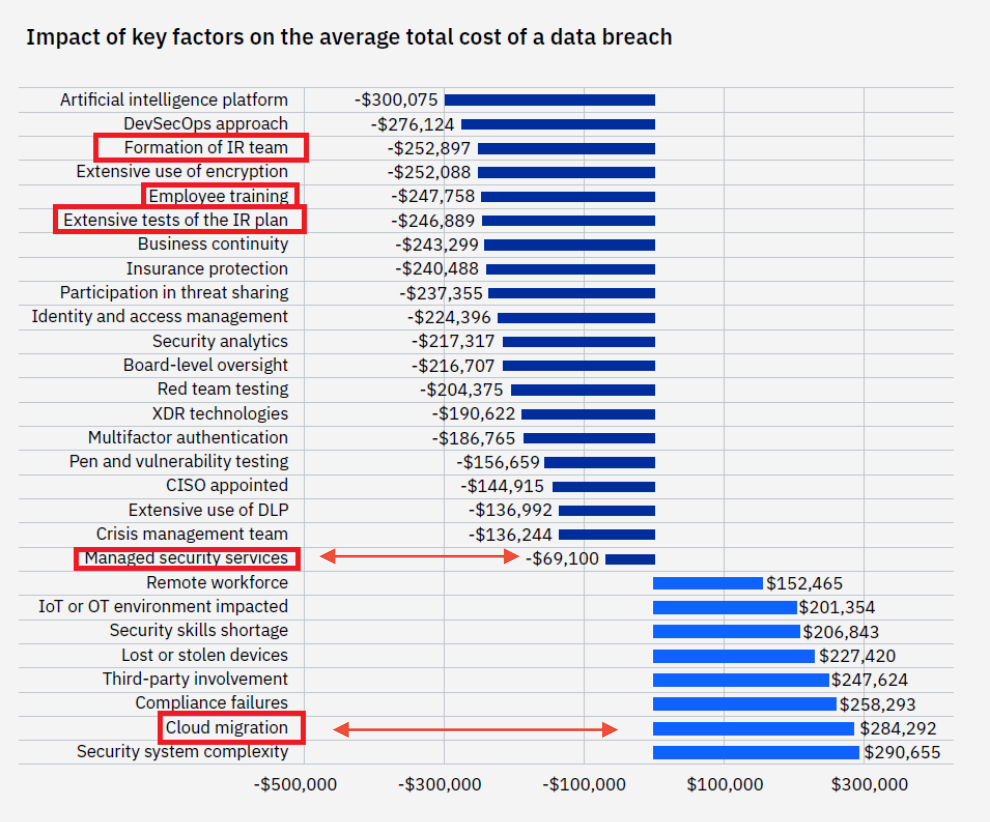
Practice the Plan

- Tabletop exercises- simulations where participants walk through the incident and response procedures

- Two types of tabletop exercises
  - Technical
  - Management
  - Both types should be conducted annually

- Spear phishing tests and other social engineering tests
- Red team penetration testing

Incident Response Preparedness- Cost Savings



The impact of 28 factors on the average cost of a data breach

$4.35 Million – The average cost of a data breach in the US

Source: IBM Security Cost of a Data Breach Report 2022

Boy Scouts Motto: Be Prepared…

Prepare

Operate

Test

- 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

  PROVE IT

Create Opportunities

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

CLA exists to
create opportunities —
for our clients, our people,
and our communities.