Modern Cyber Risks and Mitigation Strategies

Randy Romes, Principal
CliftonLarsonAllen LLP

ROCHDALE + VLI

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Modern Cyber Risks and Mitigation Strategies

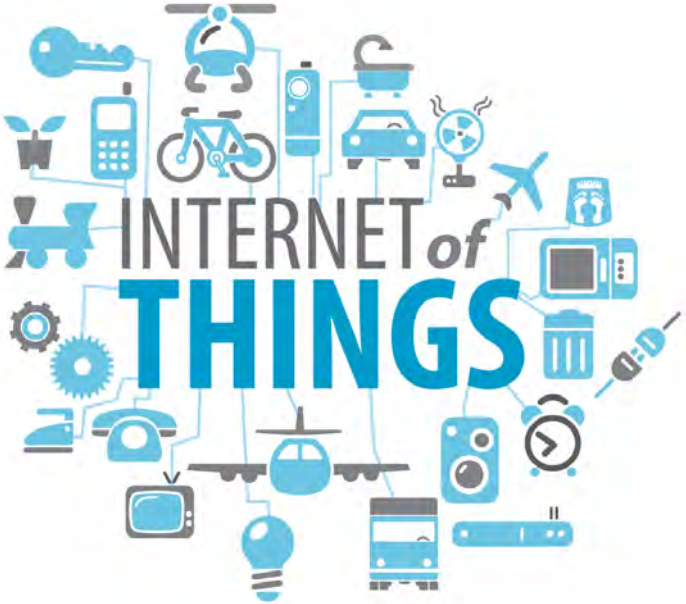
January 2026

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.

Raise Your Hand if You Work for a Tech Company

- Security Cameras
- Motion Sensors
- Logistics/GPS Tracking
- Print Vendors
- Smart TV Displays
- HVAC
- Digital Assistance
- Core Data Processing
- Cloud Applications & Analytics
- Hosted Application Processing



Security cameras

Garage door

Home thermostat

Cable TV remote

Smart TV

Sleep number bed

Roomba

Apple Watch or FitBit

“Hey Siri, what’s my balance?”

Raise Your Hand if….

C:\whoami
> m0th_man

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

Sun Tzu: “*Know Your Enemy*”
BSA Motto: ”Be Prepared”

The Current Threat Landscape

IBM - Average Days to Identify and Contain a Data Breach

Global average is

241 days

- 181 days to identify a breach
- 60 days to contain the attack
- IMPROVEMENT!

What are the bad actors doing for 181 days?

Source: IBM Security Cost of a Data Breach Report 2025

Cybercrime and Black-Market Economies

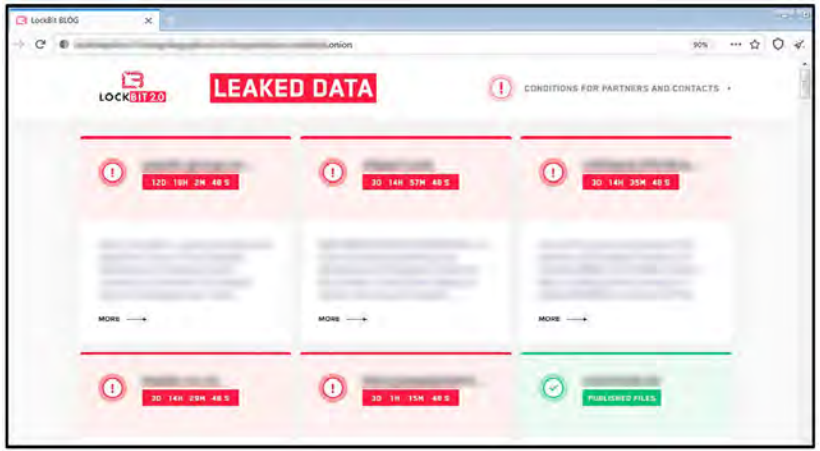
- Black market economy to support cyber fraud
  - Business models and specialization
  - Underground Marketplace (The Dark Web)

- 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…

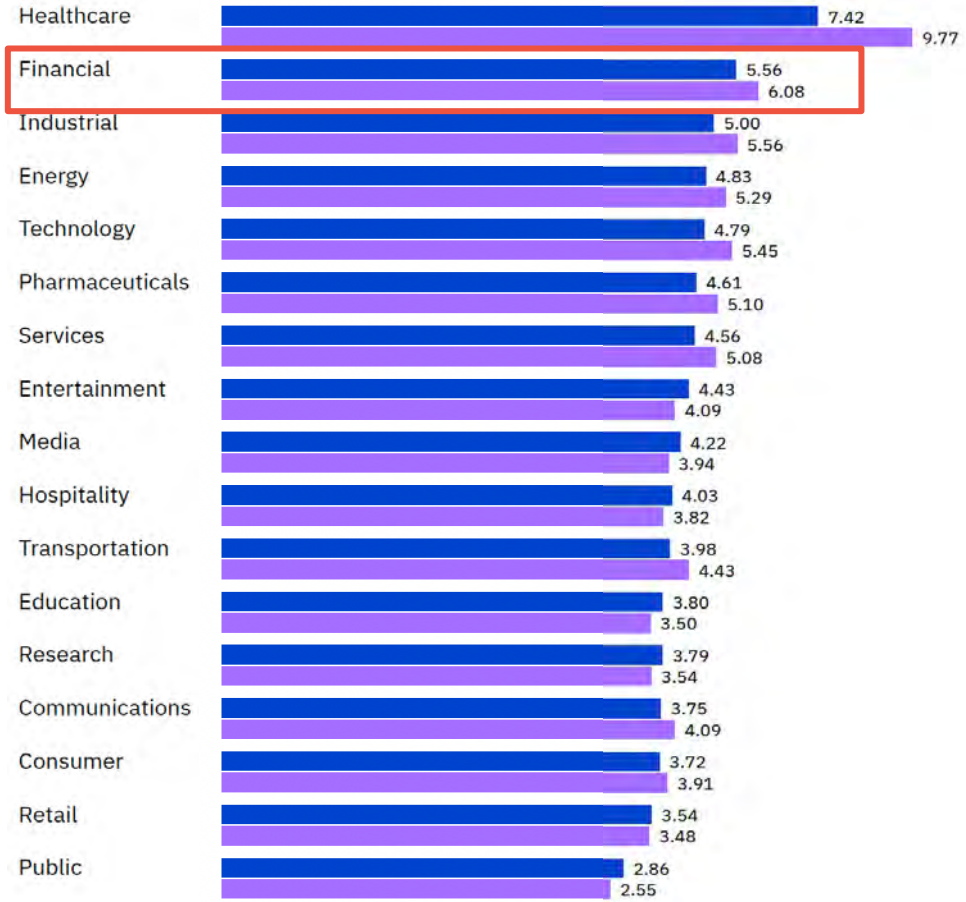
They will hit you with any or all of the following:

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 2025 is
$4.4 M
(up $900K)

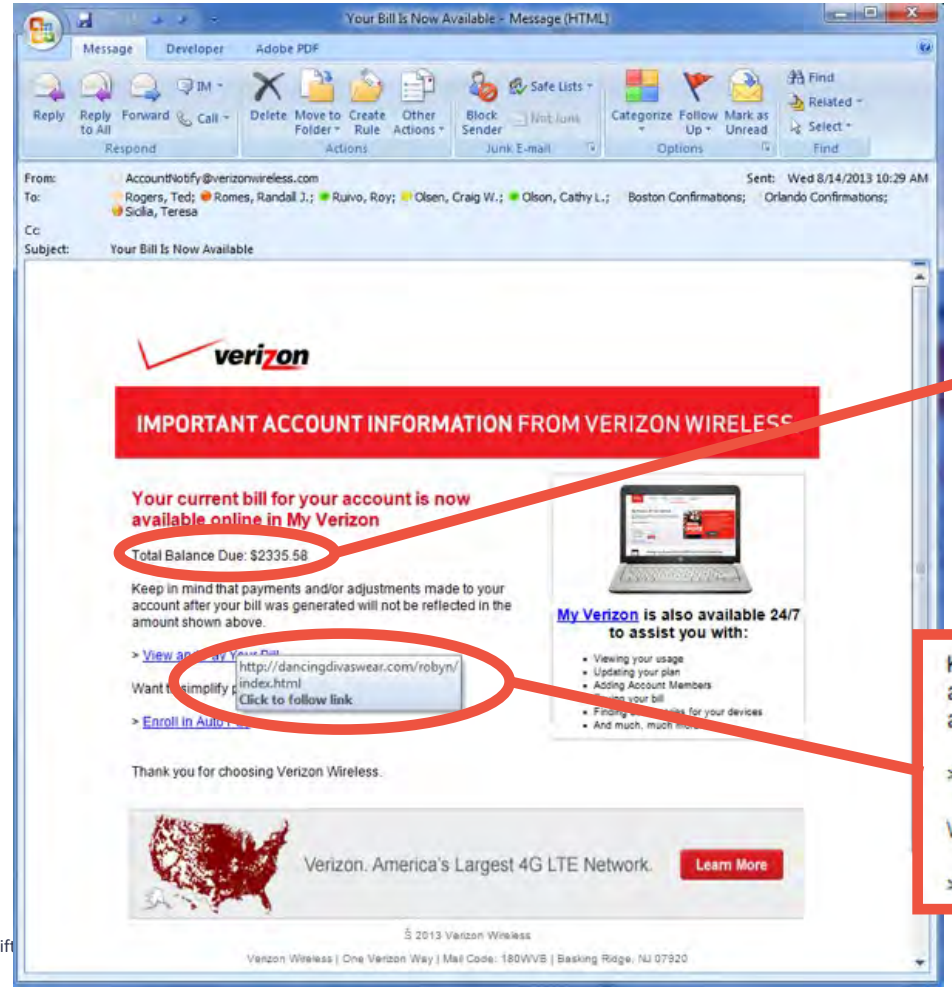


Source: IBM Security Cost of a Data Breach Report 2025

Email (Spear) Phishing

The Root Cause For Most Breaches

Old School Spear Phishing



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

Total Balance Due: $2335.58

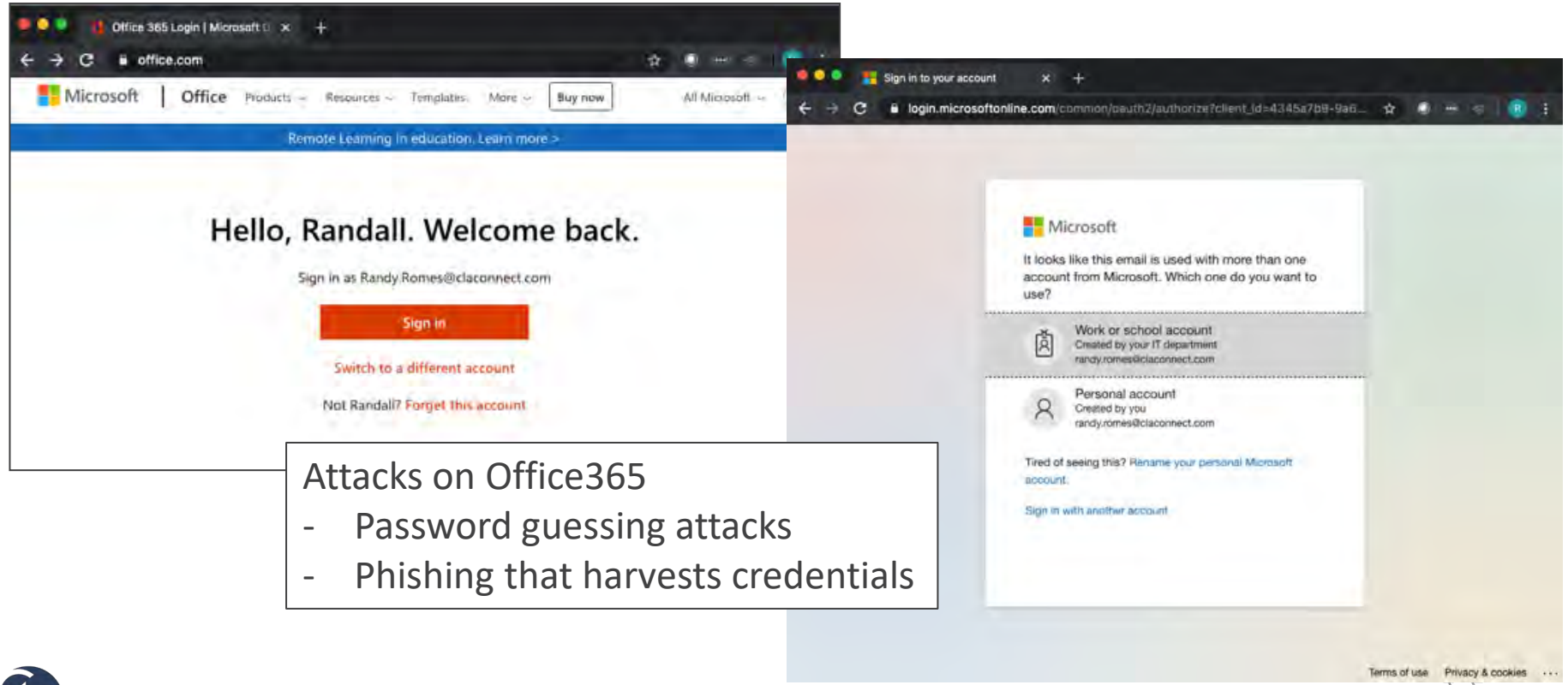
Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> View and Pay Your Bill

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

> Enroll in Auto Pay

Credential Harvesting and Password Guessing:



Attacks on Office365

- Password guessing attacks
- Phishing that harvests credentials

Phishing Service Or Penetration Test?

- “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 are important…

- 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…**

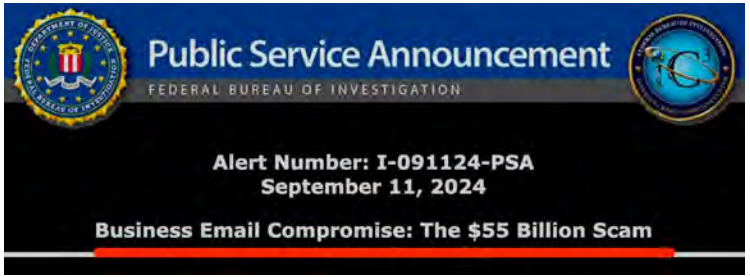
Microsoft Digital Defense Report: Targeting Businesses

Credentialed phishing schemes on the rise – indiscriminately target all inboxes

The volume of phishing attacks is orders of magnitude *greater than all other threats*

Over 700 million phishing emails blocked per week

- 1hr 12 m - The median time is takes for an attacker to access your private data if you fall victim to a phishing email
- 1hr 42 m - median time for an attacker to begin moving laterally within your network once a device is compromised



Case Study

BEC, Payment Diversion, and Data Loss

Overview

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

Analysis – Controllers Email? YES

Email that was sent to from controller to AP was sent using actual controller's actual email account

In addition, the email headers contained the "***X-MS-Exchange-Organization-AuthAs: Internal***" flag showing the message originating from the user's account and was authenticated.

Snippet of SMPT email headers from fraudulent email

X-MS-Exchange-Organization-MessageDirectionality: Originating

X-MS-Exchange-Organization-AuthSource: [redacted] *prod.outlook.com*

X-MS-Exchange-Organization-AuthAs: Internal

X-MS-Exchange-Organization-AuthMechanism: 04

Analysis

Additionally, the “Originating-IP” of 46.219.210.254 indicates the source IP address was from Ukraine:

X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [46.219.210.254]
X-MS-Exchange-Organization-Network-Message-Id:

```
┌──(user㉿server)-[~]
└─$ whois 46.219.210.254
% IANA WHOIS server
% for more information on IANA, visit
http://www.iana.org
% This query returned 1 object
# whois.ripe.net

role:           Freenet Network Coordination Center
address:        Freenet
address:        of 268, 17 Dragomanova st., Kyiv
address:        Ukraine (UA) 02068
admin-c:        FL4510-RIPE
```

Analysis

- Reviewing authentication logs showed the controller's account with several failed logins over a period of time

- Yellow rows indicate Saturday or Sunday

May	101
1-May	12
2-May	3
3-May	2
4-May	5
5-May	2
6-May	2
7-May	1
8-May	1
9-May	1
10-May	5
11-May	3
12-May	1
13-May	3
14-May	4
15-May	6
16-May	10
17-May	12
18-May	5
19-May	12
20-May	11

Analysis

- Authentication logs show the fraudster accessed email with an email client (e.g., Outlook)
- Email clients will synchronize all email, contacts, calendar, etc.
- **Controller account had 8 year's worth of email**

Date (UTC)	User	Username	Application	IP address	Location	Status	Failure reason	Client app
[redacted]	[redacted]	[redacted]	Microsoft Office	199.116.115.139	Chicago, Illinois, US	Success	Other.	Mobile Apps and Desktop clients
[redacted]	[redacted]	[redacted]	Microsoft Office	199.116.115.143	Chicago, Illinois, US	Success	Other.	Mobile Apps and Desktop clients

Analysis

- Analysis of email showed controller had documents with users' social security numbers and credit card 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 log retention settings
- Microsoft 365 Licensing – E5

Attacking the Supply Chain and Exposed Services

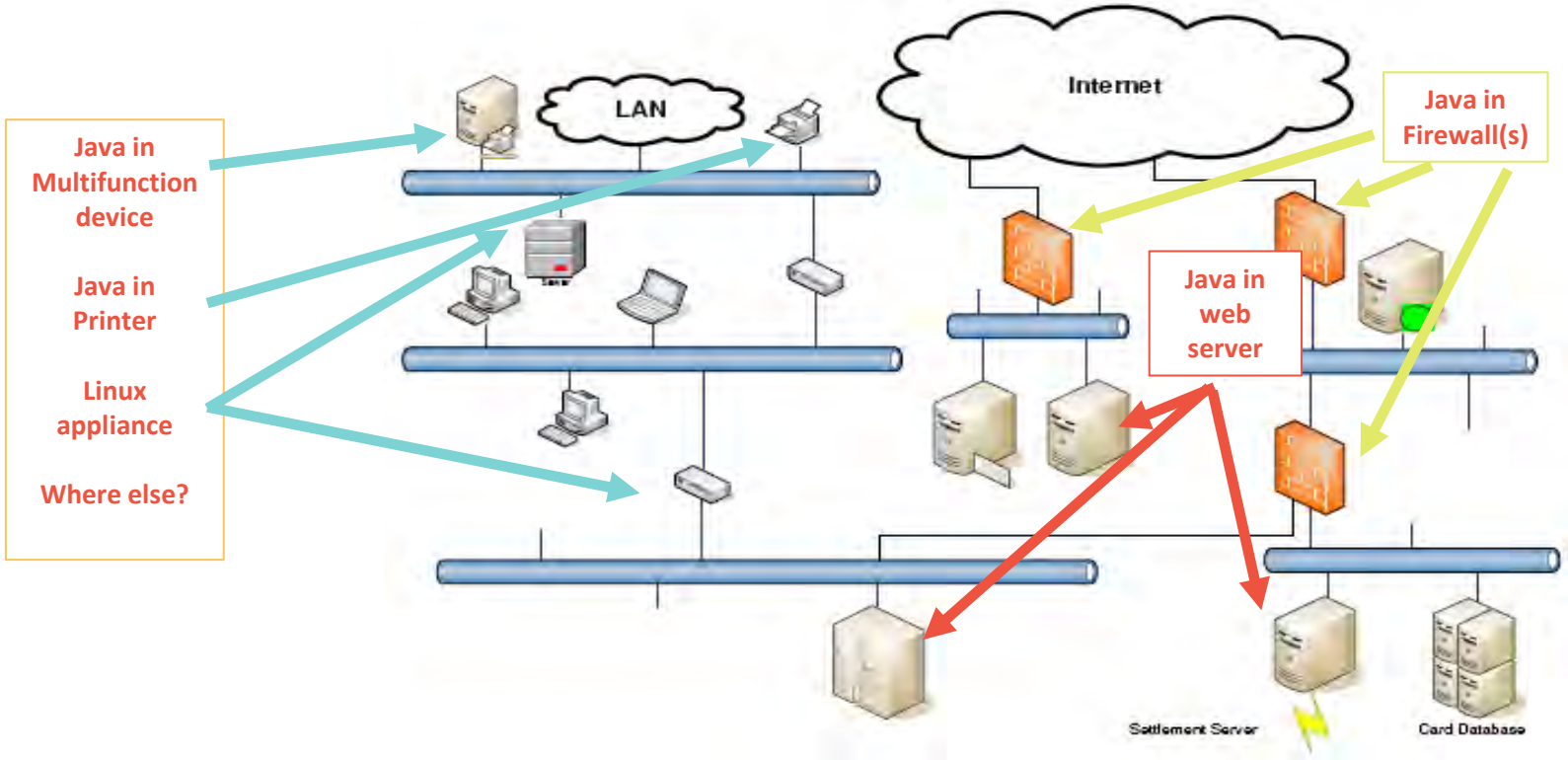
Software Vendor/Supply Chain Risk Management

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. _____

Case Study

Exposed Services, Credential Hygiene, Excessive Admin Rights and Inadequate Logging, Monitoring and Alerting

Case Study – Tale of Two “Hackers”

White Hat

- LDAP service exposed to the internet
  - Previously reported, not exploited
  - Exploited on second cycle – weak passwords, no MFA, excessive rights
  - Service disabled
- Internal escalation and lateral movement
  - Additional weak passwords on privileged accounts
  - Vulnerable SQL servers
- Limited alerting and visibility
  - Client did not know/understand what was occurring until they were told

Black Hat Hat

- LDAP service exposed to the internet
  - Exposed service exploited to gain access
  - Hackers created other persistence…
  - *Reported on second cycle and closed*
- Alerts occurred, but were not well understood or acted on
  - Changes to accounts, passwords reset
  - File permission modified
- 5 TB of data exfiltrated in 72 hours
  - No egress filters or blocking
  - No monitoring / alerting for unusual activity

Preventative Measures / Mitigating Controls

- Minimized attack surface
- MFA (for all services)
- Credential Hygiene
- Privilege Account Management (PAM)
- Server Hardening
- Change Default Logging
- Egress filtering and alerting

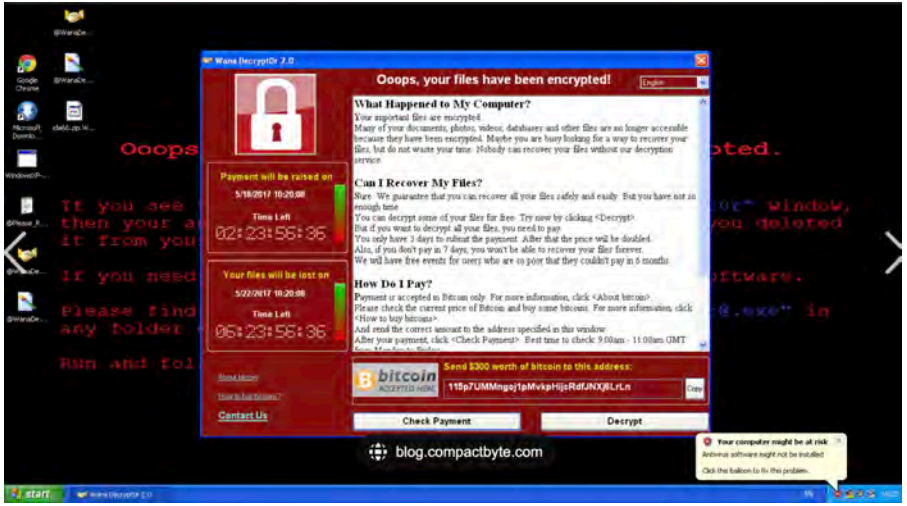
- NOTE: Vulnerability Patching was NOT and issue in this situation.

Operational Stability

Ransomware is not going away…

Ransomware

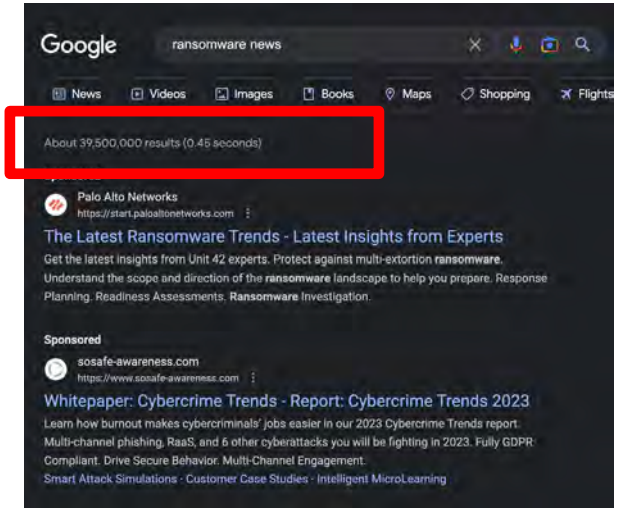
- Ransomware bursts on the scene more than ten years ago
- Hollywood Presbyterian decided to pay after ___
- Why did they wait to pay?



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 (EDR)
- Logging and monitoring (SIEM)

- **Secure (isolated) backups**
- Cybersecurity insurance

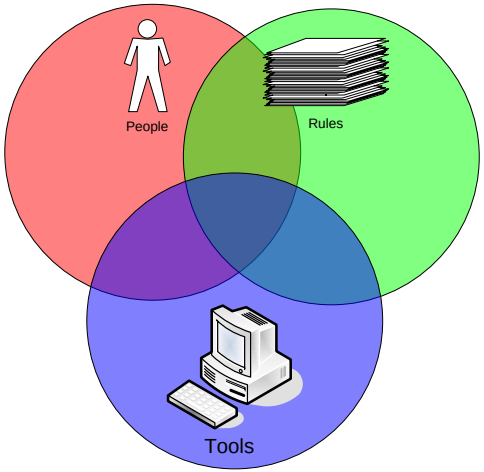
Standards Based Operations

“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, FFIEC, HIPAA, NERC/CIP, FERPA --- Regulatory
  - PCI – DSS, CMMC, HITRUST --- Contractual
  - CIS Critical Controls, NIST CSF --- Operational standards

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

- Includes Maturity Model

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

Payment Card Industry Data Security Standard

Anyone entity that stores, processes or transmits CC data…

- Approximately 140 Controls

- A cadence of three for each control
  - Policies/Standards/Procedures
  - People
  - Evidence

→Over 400 “things to address”

→PCI is all about
“Daily Business as Usual”

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls 2. Apply secure configurations to all system components
Protect Account Data	3. Protect stored account data 4. Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software
Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data 11. Test security of systems and networks regularly
Maintain an Information Security Policy	12. Support information security with organizational policies and programs

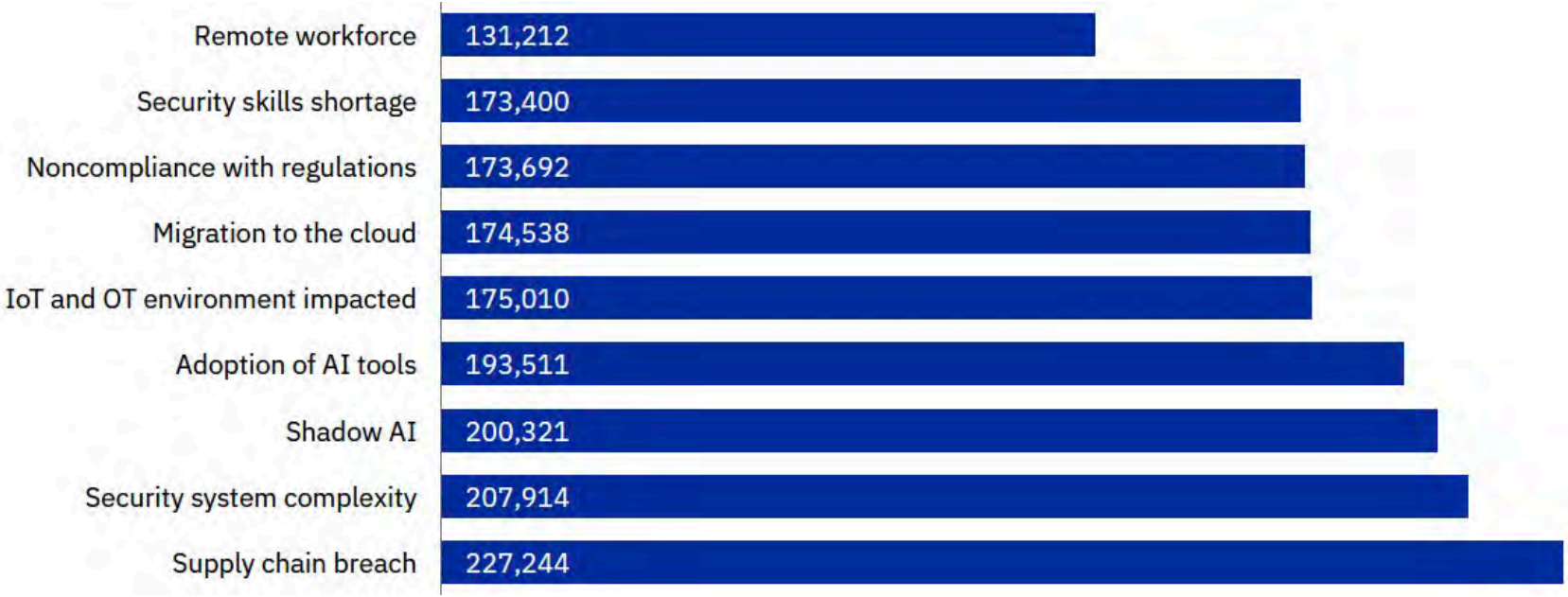
Incident Response, Disaster Recovery & Business Continuity

- 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

Factors That Make Breaches More Costly



Source: IBM Security Cost of a Data Breach Report 2025

Mature Operational Factors that Mitigate Breach Impact and Cost

Source: IBM Security Cost of a Data Breach Report 2025

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
  - Ensure security operations tools support IT and Forensic needs
- **Practice and Test**
  - Audit your operations controls (against a framework)
  - Red Team and Purple Team engagements to test and validate preventative controls aligned to logging, monitoring, and alerting
  - Schedule IR Tabletop and Disaster Recovery exercises

Thank you!

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

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