Cybersecurity Risk and Assessment

September 12, 2022

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.

Learning Objectives

- Understand the latest threat developments
- Recognize critical dependencies and risks in outsourced service provider relationships
- Learn where organizations can focus valuable risk mitigation resources
- Develop and refine a framework of knowledge to plan future security efforts

Who is CLA?

More than

7,500

people

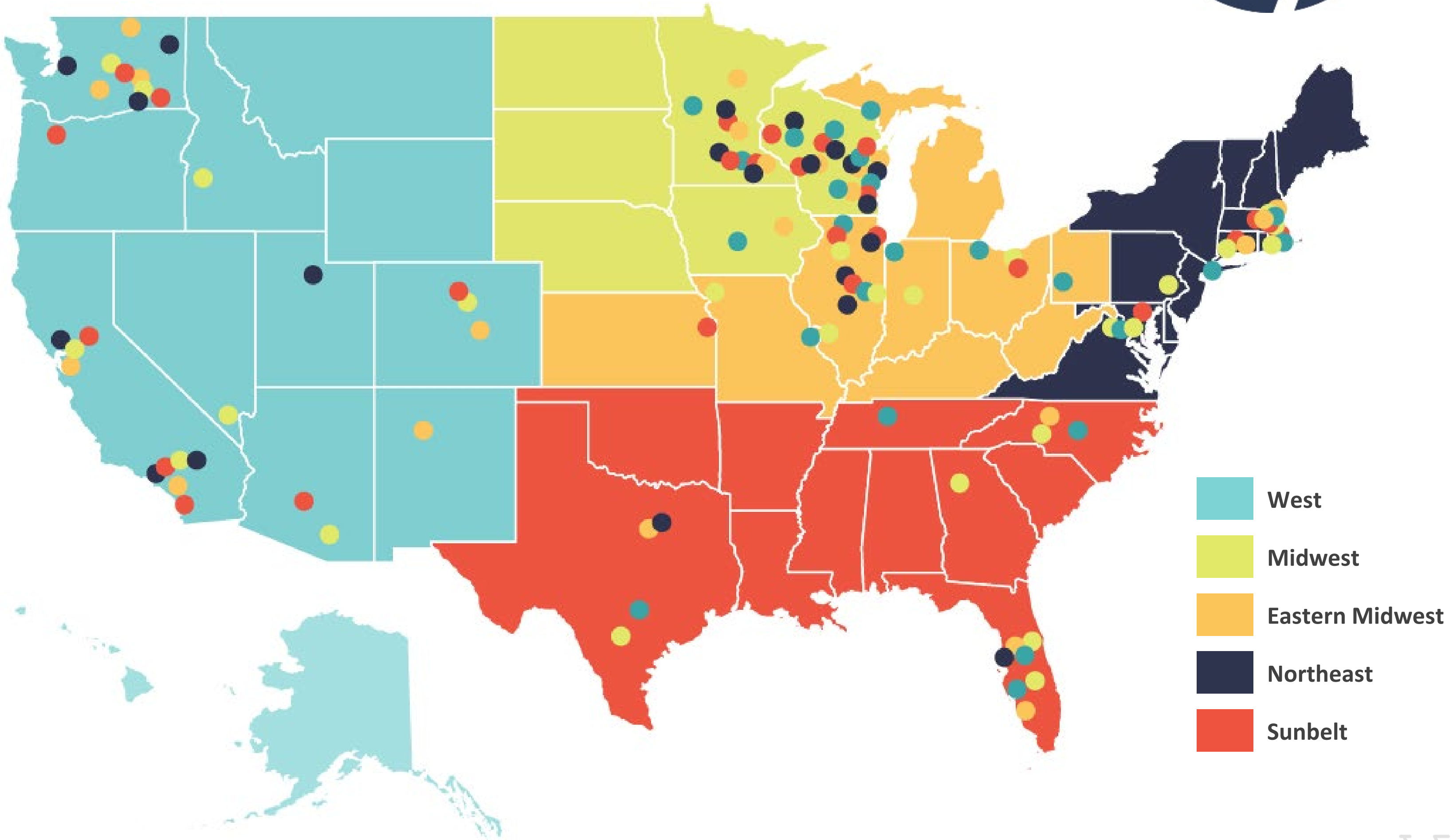
More than

120

U.S. locations

CLA is now

global



~$whoami

- Snake_Eyes
- Family
- BBQ
- Cybersecurity
  - Insider Threat
  - Incident Response
  - Penetration Testing
  - Controls
  - Compliance

The Current Threat Landscape

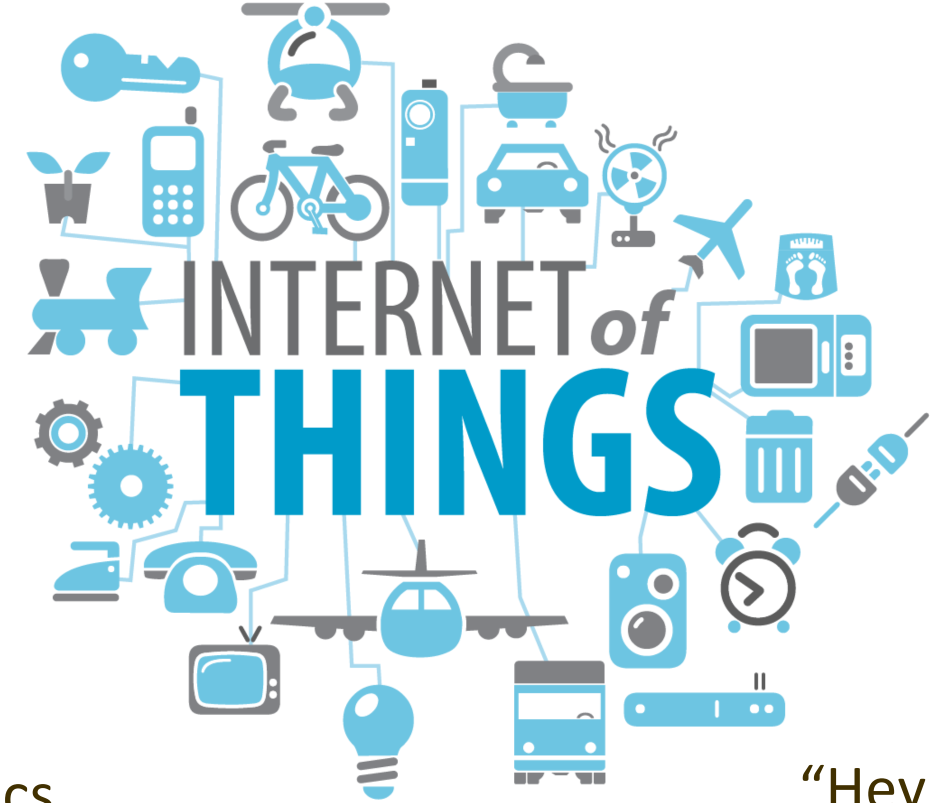
WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

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”

Cybercrime and Black-Market Economies

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

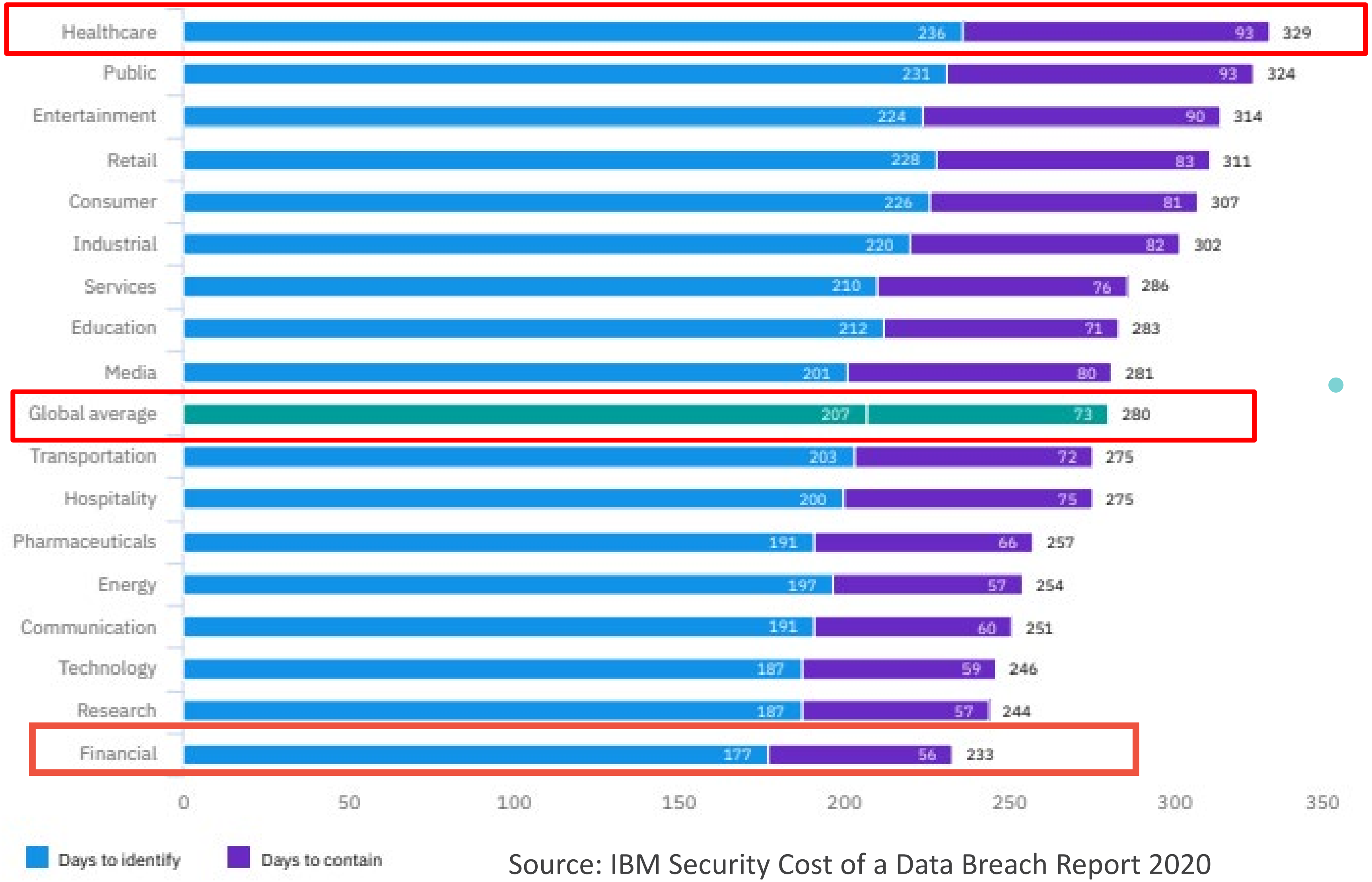
- Most common cyber fraud scenarios we see affecting our clients
  - Theft of information
    - Credit card information
    - ePHI, PII, PFI, account profiles, etc.…
    - Log-in Credentials
  - Ransomware and interference w/ operations

➢ 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



Source: IBM Security Cost of a Data Breach Report 2020

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

Behind the statistics

- Hackers can do a lot in AND to your network in 236 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

Average cost
$8.4M

The Supply Chain Exposing Us

Log4j and Other Imbedded Software Components

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

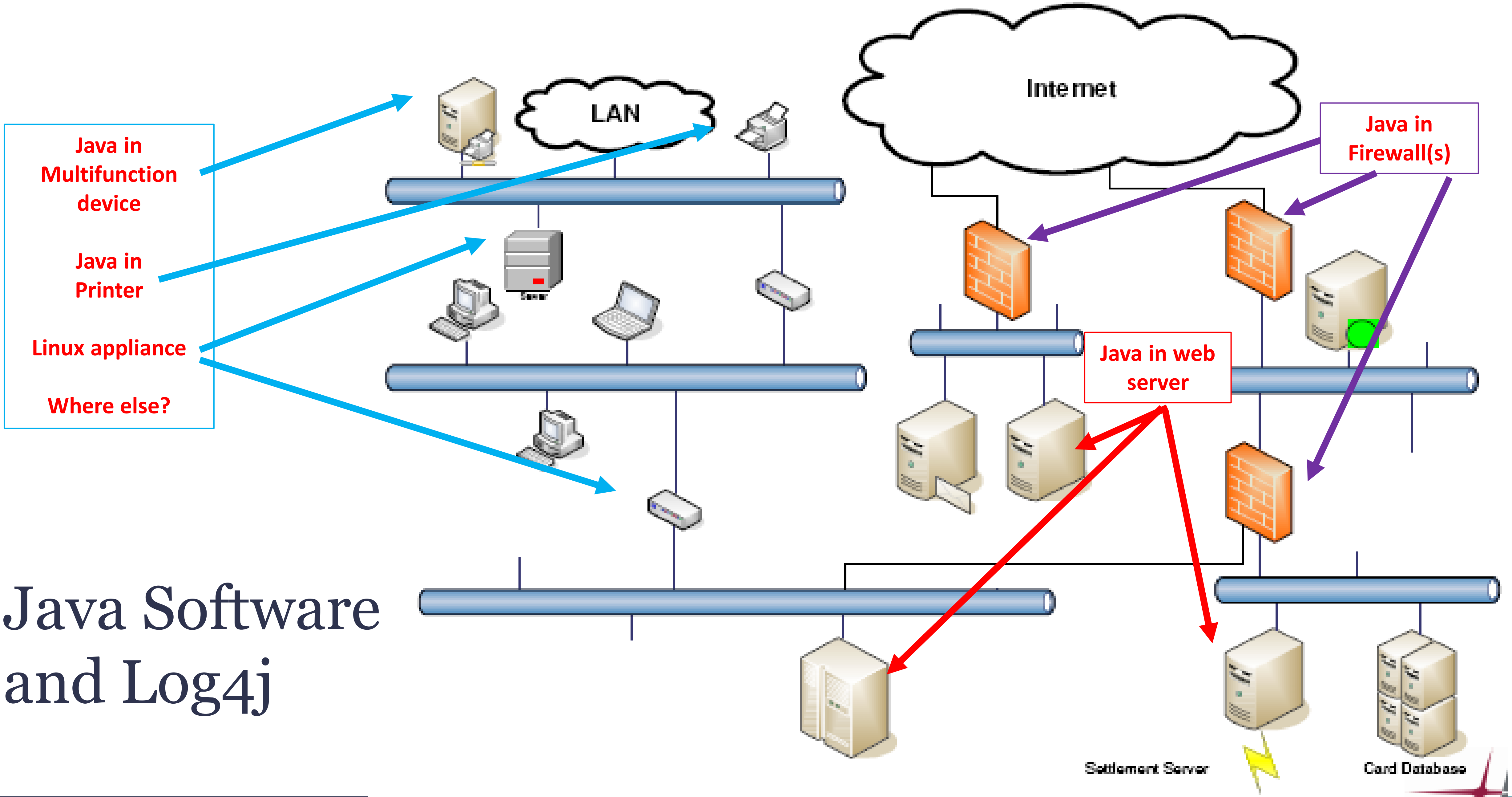
Software Vendor/Supply Chain Risk Management

Recent Significant Issues:

- Common software components with exploitable vulnerabilities.
- Recent examples include
  - “**Log4j**” Java vulnerabilities…
  - **Pkexec** - CVE-2021-4034 (PwnKit)

Google:
Log4j banking vulnerabilities

Linux system service bug gives root on all major distros, exploit released



Java Software and Log4j

Case Studies

Ransomware

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

What is Ransomware?

- Cryptolocker, Locky, WannaCry, etc..
- Encrypts all data, holds in “ransom” for $$
  - Data on local machine and on network
- Can affect non-Windows OS (e.g., Mac)

How Does Ransomware Get Into Business Networks?

Insecure Internet Accessible Log-in Prompts

Outlook Web Access (OWA)

Citrix Gateway

Virtual Private Network (VPN)

Remote Desktop Protocol (RDP)

Email phishing resulting in:

- User opening an infected attachment.
- User downloading malicious payload from a website.

Unpatched systems or mobile devices running outside of organization's firewall.

Ransomware in the News

JBS Foods

- Paid $11 million
- Shutdown operations at beef plants for several days.
- Supply chain disruption.

Colonial Pipeline

- Paid $4.5 million.
- Shutdown operation for several days.
- Caused consumers panic buying gas.

Cyber Preparedness

What can we do to Prepare?

1. Risk assess, classify, and inventory systems
2. Perform IT audit/cybersecurity assessments including internal network penetration testing and external network penetration testing – at least annually AND after significant changes
3. Review and assess risks related to privileged user accounts (i.e. administrator access)
4. Harden network technology and applications against attack
5. Continue to enhance and tune network, system and application monitoring and alerting
6. Train and test employees frequently (Human Factor)
7. Develop a cyber resilience plan and test frequently

Internal Penetration Testing

- Organizations should perform a technical evaluation of key devices (*file servers, mail servers, production servers, routers, switches, etc.*.) that reside their network.
- The goal should be to identify vulnerabilities and potential attack vectors and mitigate those to confirm that your network is reasonably protected threats.
- Should consider patch management, configuration management, authentication, and awareness.

Strong User Controls and Data Backups

- Staff should not have local admin rights to their workstations.
- No email, browsing, or general computer use when using admin credentials.
- Network and domain admins should be required to have two sets of credentials.
- Administrators should NOT log into workstations with domain admin rights.
- Attackers are getting smarter and deleting or encrypting online backups; so, organizations should ensure that they have off-line copies of backup and restore files available.
- Backup and restore files should be saved in well secured location.
- Perform a thorough review of file permissions for network file shares.
- Test the restoration of your data

External Penetration Testing

- Organizations should perform a thorough assessment of their externally facing infrastructure.
  - Login prompts secure (webmail, VPN, etc..)?
  - External systems patched?
  - Email filters up to par?
  - Unnecessary ports closed?
- Should consider patch management, configuration management, authentication, and awareness.

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

User Education and Phishing Awareness

- Malware typically needs a helper to do its job.
- Educate users on phishing scenarios and consider internal phishing “tests” to gauge employee readiness.
- Tests should familiarize employees with common phishing scenarios as well as teach employees how to identify masked links and spoofed sender addresses.

Social Engineering

Strong UNIQUE Passwords (Passphrases Actually)

Password1

Spring2022

IHatePasswords!

NCBBQistheBestintheUSA!

NCBBQ!$@m@z!ng

H!p21Y@wn!ng95$v(

Multifactor Authentication (MFA)

- A Complement to strong passwords.
  - Not a mitigation of risk for weak passwords.
- Pin Code
- Push Notification
- Phone call

- Implement on all remote connections at your organization.
- Educate users about rogue MFA requests.
  - This is a successful technique applied by malicious actors.

Incident Response Preparedness

- Unfortunately, data breach can still occur despite implementing all the best security precautions
- When that occurs, organizations need to ensure they are ready to respond to a data breach.

Have a plan, practice the plan, prove the plan

Have a Plan

- Develop an incident response 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

Practice the Plan

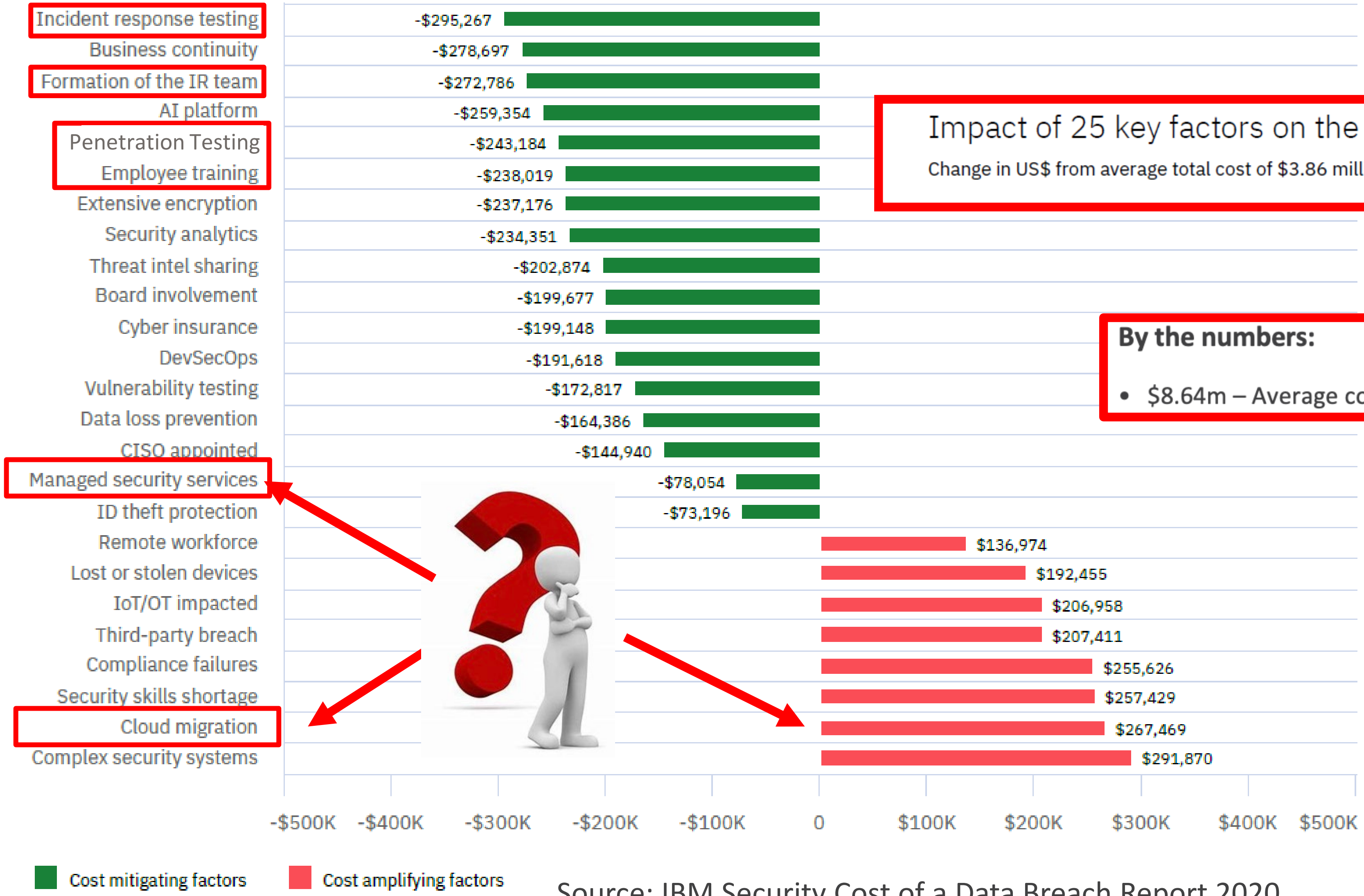
- Like all emergency procedures, they need to be practiced
- Table-top exercises- simulations where participants walk through the incident and response procedures
- Two types of table-top exercises
  - Technical
  - Management
- Both types should be conducted annually

Team Held
K1
TORNADO DRILL
Video by The Crescent-News – Defiance, Ohio – crescent-news.com

Prove the plan

- Many businesses end up over-notifying customers about data breaches, significantly increasing costs and risk of litigation
- Low visibility into IT infrastructure means lack of forensic evidence to determine which system or data hackers accessed
- Conduct trial forensic exercises to ensure you have the proper data and visibility

Incident Response Preparedness- Cost Savings



Impact of 25 key factors on the average total cost of a data breach

Change in US$ from average total cost of $3.86 million

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

Case Studies

Microsoft Exchange

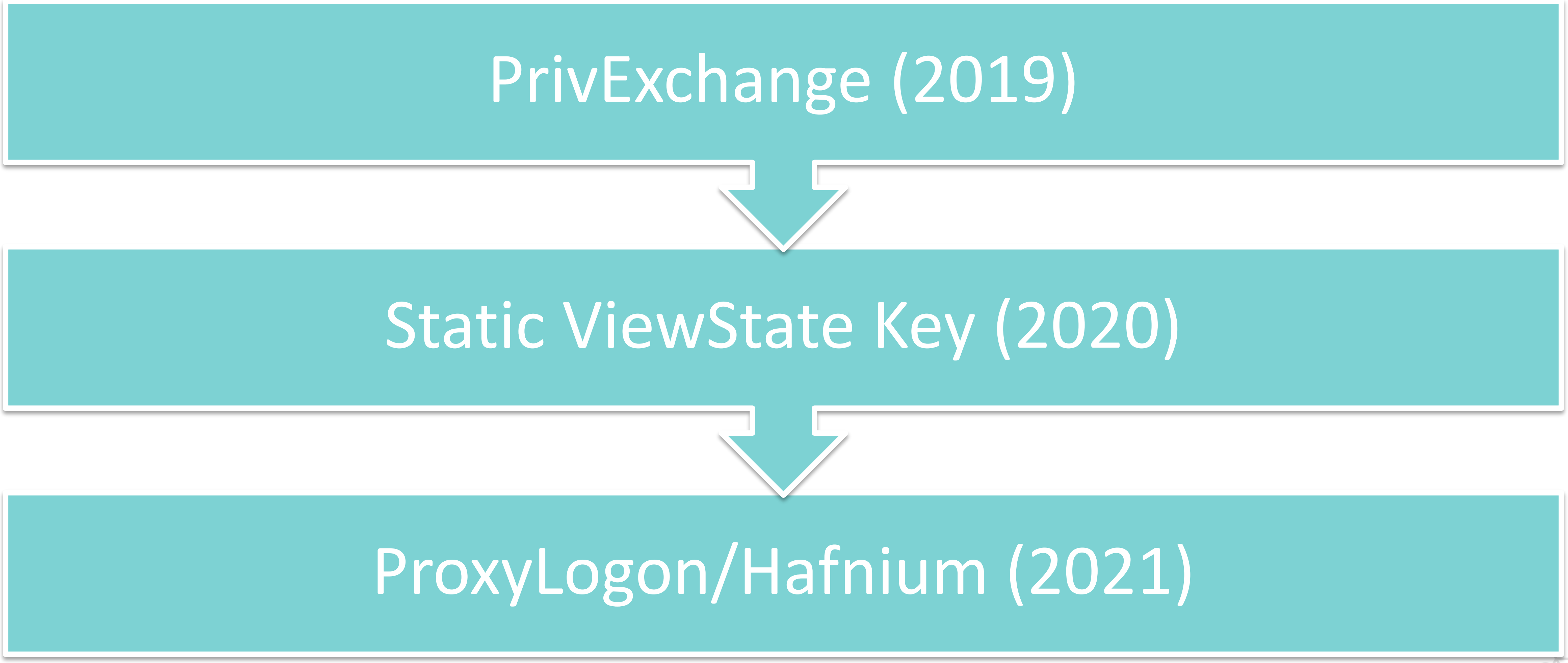
WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Microsoft Exchange

- Exchange
  - Installed on-premise
  - Installed on corporate servers
  - Exchange servers have privileged access in network
- Exchange Online
  - Hosted by Microsoft in Microsoft’s cloud
  - Organizations don’t have to manage server, only application

Exchange Vulnerability History



PrivExchange (2019)

Static ViewState Key (2020)

ProxyLogon/Hafnium (2021)

Why Target Exchange

- Central hub for every organization

Conversations

Files

Authorization

Hafnium (According to Microsoft)

- Hacking group based out of China
- Targets US companies
- Operates using Virtual Private Servers (VPS) in US

https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

Timeline

- Jan 5 – Security firm (DEVCORE) notifies Microsoft of vulnerability
- Jan 6 – Security firm (Volexity) notifies Microsoft that it sees hackers exploiting Exchange, going back to as early as Jan 3
- Jan 8 – Microsoft confirms vulnerability
- Jan 27 – Another security firm (Dubex) notifies Microsoft of organizations being hacked by “unknown” Exchange vulnerability

https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/

Timeline (cont.)

- Feb 18 – Microsoft notifies security firm that patches will be released on March's patch Tuesday (March 9)
- Feb 26 – Mass exploitation of Exchange vulnerability around the world
- Mar 2 – Microsoft releases Exchange patches early

https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/

Impact?

https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/

30,000 U.S. Organizations Impacted

Hospitals

State and Local Governments

First Responders

School Districts

Mitigating Controls

- Logging and monitoring
- Egress filtering
- Install public-facing services in DMZ
- Antivirus/endpoint controls
- Multi-Factor Authentication for Email and remote connections

Create Opportunities

Javier Young, CISSP
Principal – Cybersecurity
704.816.8470
Javier.Young@claconnect.com

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

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor