Cybersecurity Effects and Failures

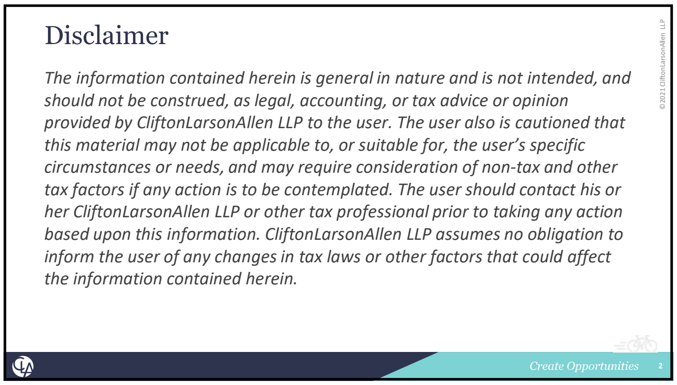
Preparedness, and Managing the Unsuspected Breach

May 10, 2023

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

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

1



Disclaimer

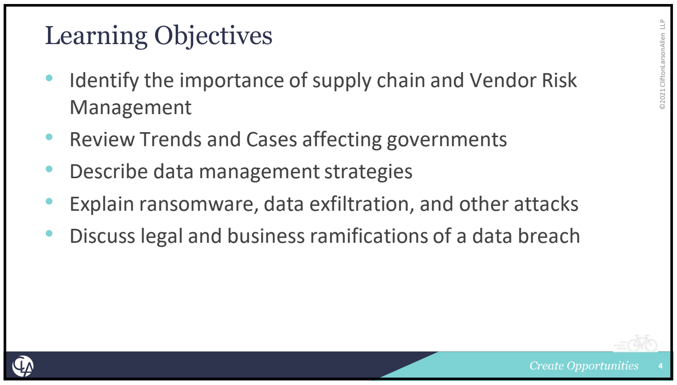
The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific 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.

2

Today's Discussion

- Learning Objectives
- Current Cybersecurity Landscape
- Case Analysis
- Cyber Security Preparedness
- Closing Remarks

3



Learning Objectives

- Identify the importance of supply chain and Vendor Risk Management
- Review Trends and Cases affecting governments
- Describe data management strategies
- Explain ransomware, data exfiltration, and other attacks
- Discuss legal and business ramifications of a data breach

4

Current Cybersecurity Landscape

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

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

5

Cybersecurity Landscape in Recent Years

- As a result of the pandemic, we have seen both traditional, and more commonly, nontraditional forms of hacking targeting all Industry sectors.
- Hackers (both individuals and nation state) recognize many industries including Governments, as the banking targets of the 90's and healthcare targets of the past decade.
- The remote working transition will continue to test the resiliency of company's cyber security strategy and has created risks/exposures that may not have been fully vetted.
- Companies must be proactive in educating their employees on the fundamentals of managing and protecting their data and embed security awareness within their daily policies.

6

Headlines – Front Page

- Colonial Pipeline – ransomware attack affecting a week long pipeline shutdown to infrastructure. $4 million ransom paid, but much recovered with help of FBI.
- US Cellular – social engineering targeted to employees is believed to be the source. 276 reported customers impacted, but allegedly 4.9 million account records potentially exposed.
- IBM reported in 2020 hackers backed by foreign governments targeted companies that maintain the cold chain necessary to ship and store mRNA vaccines by posing as executives of Haier Medical and solicited usernames and passwords.
- Reportedly 800-1500 companies breached this past July… with $70 million ransom request via BitCoin.
- Federal Government Breach
  - https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

7

What about these headlines?

- Oldsmar, FL – Water Treatment facility hit with ransomware… believed to have been through social engineering and/or stolen credentials.
- California DMV – attack affected driver records and data for allegedly from a third party vendor.
- Tyler Munis – breach of network, with disruption to cloud customers, and notifications and details on client actions, including account and access changes.
- California State Controllers Office – phishing attack that reportedly opened limited access to PII in unclaimed property records. Full extent still being investigated.
- How many governments affected by SolarWinds? While we focus on the SolarWinds headline – do we fully understand the scope and number of government (and other) entities impacted and at risk?
- 22 Texas Municipalities – coordinated simultaneous attack – resulting in $2.5 million ransom payments.

8

What Do We Know?

- It is reported in several articles, as well as published studies, that as much as 70% of ALL ransomware attacks in the United States target state and local governments.
- Most studies put government agencies as a top 2 or 3 target of cyberattacks, and one of the largest growing sectors of breaches and attacks.
- Of attacks on governments, 69% or more are reported to be a result of social engineering and phishing (consistent with ic3.org stats). GCN, Verizon, Gartner, and more publish studies consistent with these statistics.
- Cybercrime is increasing at an alarming rate. Many studies report different metrics and rates of growth. Almost all are consistent in showing significant growth. One we researched reported as much as 600% growth during the pandemic. (most within a 20%-80% range)

9

Cybersecurity – What we've learned

- As companies continued to digitize and connect, they created an ecosystem that requires a security architecture adequate to protect beyond its physical buildings.
- Management needs to be aware of its supply chain and vendors (Vendor Risk Management). A proactive Vendor Risk Management strategy is critical to minimizing the disruption of a companies supply chain.
- A robust Data Management Resiliency Strategy is a key imperative – Know your "Crown Jewels", where they reside and review the design and architecture of your cyber security framework.
- Continue to educate and inform your board of directors and senior executives. They will be an important advocate in funding your cybersecurity strategy.
- Awareness of employee home network and device risks must be considered in the strategies.

10

A recent 2021 research on the Cost of a Data Breach conducted by Ponemon Institute and sponsored and published IBM Security noted:

By the numbers:

- $8.64m – Average cost of a data breach in the United States
- 80% - Share of breaches that included records containing Customer Personally Identifiable Information (PII), at an average cost of $150 per record
- $2.64m – Average global total cost of a breach for organizations under 500 employees; $5.52m at enterprises over 25K employees

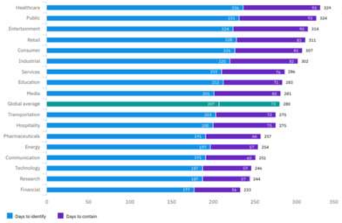
Separately:

- Reported costs to the cities of Atlanta and Baltimore individually are as much as $5-9 million due to recovering and dealing with prior ransomware events.

11

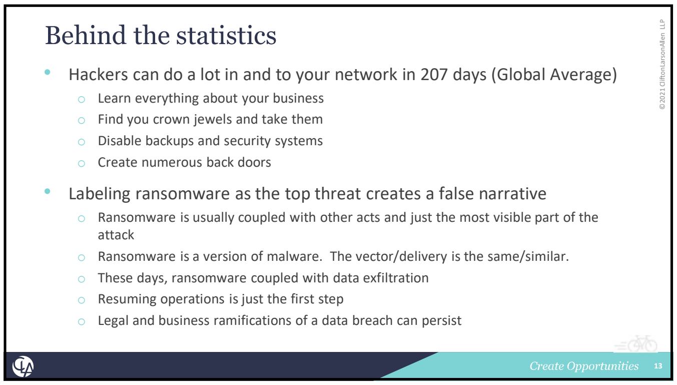
Average Days to Identify and Contain a Data Breach by Industry

- Global average is 280 days
  - 207 days to identify a breach
  - 73 days to contain the attack
- Government (Public)
  - Hard to see – but second highest on table
  - 233 days to identify
  - 324 days to contain



Source: IBM Security Cost of a Data Breach Report 2020

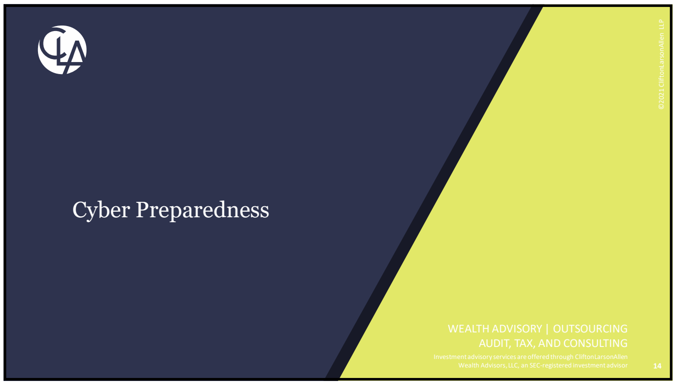
12



Behind the statistics

- Hackers can do a lot in and to your network in 207 days (Global Average)
  - Learn everything about your business
  - Find you crown jewels and take them
  - Disable backups and security systems
  - Create numerous back doors
- Labeling ransomware as the top threat creates a false narrative
  - Ransomware is usually coupled with other acts and just the most visible part of the attack
  - Ransomware is a version of malware. The vector/delivery is the same/similar.
  - These days, ransomware coupled with data exfiltration
  - Resuming operations is just the first step
  - Legal and business ramifications of a data breach can persist

13

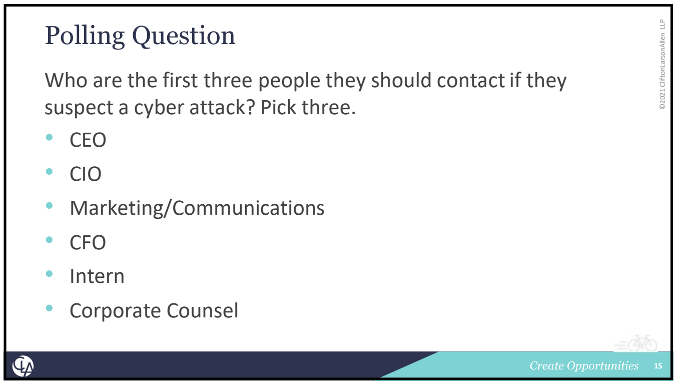


Cyber Preparedness

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

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

14

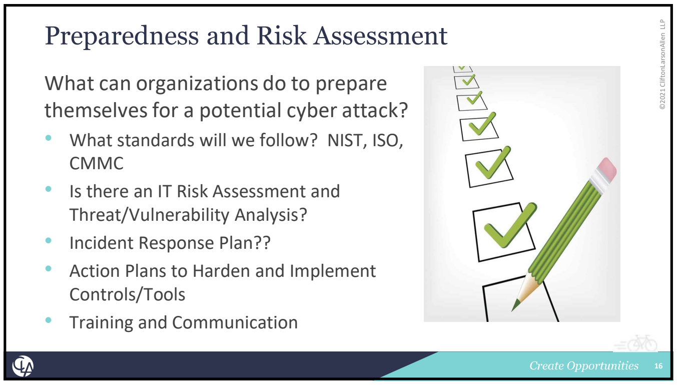


Polling Question

Who are the first three people they should contact if they suspect a cyber attack? Pick three.

- CEO
- CIO
- Marketing/Communications
- CFO
- Intern
- Corporate Counsel

15

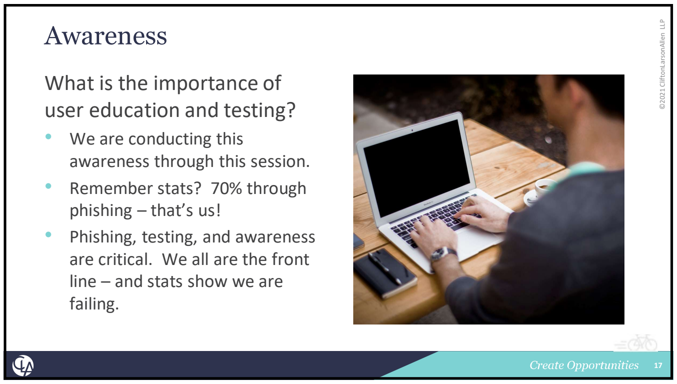


Preparedness and Risk Assessment

What can organizations do to prepare themselves for a potential cyber attack?

- What standards will we follow? NIST, ISO, CMMC
- Is there an IT Risk Assessment and Threat/Vulnerability Analysis?
- Incident Response Plan??
- Action Plans to Harden and Implement Controls/Tools
- Training and Communication

16

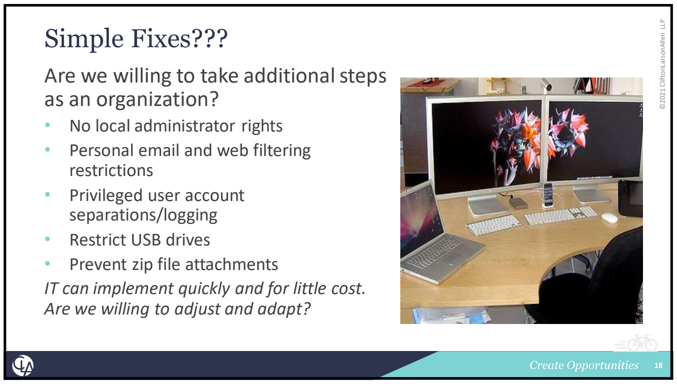


Awareness

What is the importance of user education and testing?

- We are conducting this awareness through this session.
- Remember stats? 70% through phishing – that's us!
- Phishing, testing, and awareness are critical. We all are the front line – and stats show we are failing.

17



Simple Fixes???

Are we willing to take additional steps as an organization?

- No local administrator rights
- Personal email and web filtering restrictions
- Privileged user account separations/logging
- Restrict USB drives
- Prevent zip file attachments

IT can implement quickly and for little cost. Are we willing to adjust and adapt?

18

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

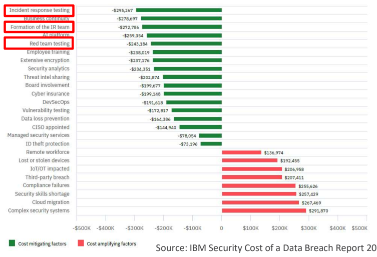
Have a Plan

- 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

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



Source: IBM Security Cost of a Data Breach Report 2020

Questions

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

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

Thank you!

Jim Kreiser CISA, CRMA, CFSA
James.Kreiser@CLAconnect.com

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

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