
©2021 CliftonLarsonAllen LLP
Developing Trends, Cybersecurity Preparedness, and Managing the Unsuspected Breach
June 24, 2021
WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

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.

©2021 CliftonLarsonAllen LLP

Today's Discussion

- Learning Objectives
- About CLA
- Our Panelists
- Current Cybersecurity Landscape
- Case Analysis
- Cyber Security Preparedness
- Closing Remarks

©2021 CliftonLarsonAllen LLP

Learning Objectives

- Importance supply chain and Vendor Risk Management
- Describe data management strategies
- Explain ransomware, data exfiltration, and other attacks
- Discuss legal and business ramifications of a data breach

©2021 CliftonLarsonAllen LLP

About CLA

- CLA creates opportunities for businesses, individuals, and communities through our wealth advisory, outsourcing, audit, tax and consulting services.
- With 7,400 people, more than 120 U.S. locations, and a global affiliation, we promise to know you and help you. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.
- Our IT Cybersecurity practice has over 100 professionals nationally with expertise in IT architecture assessment, compliance testing, remediation as well as incident response and CISO outsourcing.

©2021 CliftonLarsonAllen LLP

Our Panelists

Francis Nemia
Principal, Cybersecurity

Francis.Nemia@CLAconnect.com
617-658-5224

David Sun
Principal, Cybersecurity

David.Sun@CLAconnect.com
703-483-2650

Javier Young
Manager, Cybersecurity

Javier.Young@CLAconnect.com
704-816-8470

Randy Romes
Principal, Cybersecurity

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

©2021 CliftonLarsonAllen LLP


Current Cybersecurity Landscape
©2021 CliftonLarsonAllen LLP
WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor
7

Cybersecurity Landscape in 2021

- 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 Life Sciences (Pharma and Healthcare) as the banks of the 21st century.
- The remote working transition will continue to test the resiliency of company's cyber security strategy.
- 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.

©2021 CliftonLarsonAllen LLP

Cybersecurity – What we learned in 2020

- 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.

©2021 CliftonLarsonAllen LLP

The WHY? Hackers steal Pfizer, BioNtech data in European Medicines Agency (EMA) breach and more (ENDPOINTS NEWS) – One Industry Example

- In December 2020, the EMA was subject to a "cyber attack" and confirmed its data had been "unlawfully accessed". The stolen documents could potentially give useful information to other countries developing a vaccine as well as information on other companies and systems developing and distributing it.
- Throughout 2020 Nation State groups made various attempts to compromise passwords and launched phishing schemes as the hackers posed as World Health Organization officials and solicit people's passwords.
- 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.

©2021 CliftonLarsonAllen LLP

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

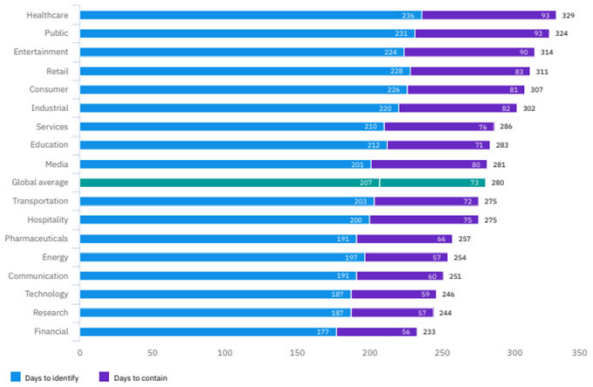
©2021 CliftonLarsonAllen LLP

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
- $7.13m – Healthcare Industry average cost of a data breach – Up 10% from 2019

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
- Financial Services average 233 days
  - 177 days to identify a breach
  - 56 days to contain the attack
- Healthcare average is 329 days
  - 236 days to identify a breach
  - 93 days to contain the attack



Source: IBM Security Cost of a Data Breach Report 2020

©2021 CliftonLarsonAllen LLP

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
  - These days, ransomware coupled with data exfiltration
  - Resuming operations is just the first step
  - Legal and business ramifications of a data breach can persist

©2021 CliftonLarsonAllen LLP

What have we seen?

- Biotechnology company up and running within days from a ransomware attack
  - Having an adequate BC/DR plan and procedures in place
  - They got lucky
- Recently assisted a client who was a victim of a ransomware attack to become operational within days
  - Client backups were destroyed
  - Entire network infrastructure was compromised
- Worked with a company where hundreds of sensitive client documents were compromised
  - Month's long notification process

©2021 CliftonLarsonAllen LLP


Case Analysis
©2021 CliftonLarsonAllen LLP
WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor
15

Case Study

- Company experiences ransomware outage
  - Most systems encrypted
  - Operations has been shut down
  - Client had an IR plan and attempted to implement. Primary contact of CIO changed but identified to correct lead IT person
  - System backups exist, IT has been trying to restore for last 3 days
  - Company did not have cyber insurance coverage
  - CEO is responding to vendor and client inquires on why the company was not responding to emails and rumors of an incident
  - Board was notified of breach and instructed CEO to bring in outside assistance

©2021 CliftonLarsonAllen LLP

Case Study

- CLA's cyber response team is brought in to assist
  - Examined all key systems
    - Identified which systems were encrypted and when
    - Collected logs from all available devices
  - Forensics examination was performed
    - Determined that the ransomware variant was Sodinokibi- which is known to exfiltrate data
    - Logs showed CFO's account logged in to remote access server from Vietnam, Germany and Philippines
    - Logs only go back 2 months and evidence the threat actor was in the network appears as far back as then
    - Company did not maintain systems to monitor for data going out of the network

©2021 CliftonLarsonAllen LLP

Case Study

- Restoring operations
  - After working with company's IT, we were able to isolate all infected systems
  - Built new servers and systems
  - Restored data from backup to the newly built systems
- Fallout
  - One of the compromised systems contained protected data covered under state reporting regulations
  - Because the ransomware group is known to exfiltrate data and company did not have anything monitoring outbound data, all clients with protected information in the system needed to be notified of the potential compromise
  - Risk of litigation from clients

©2021 CliftonLarsonAllen LLP

Polling Question

Did the organization have adequate visibility into their systems to protect against a data breach?

- Yes
- No

©2021 CliftonLarsonAllen LLP

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

©2021 CliftonLarsonAllen LLP

Polling Question

Were they prepared to mitigate a cyber attack?

- Yes
- No

©2021 CliftonLarsonAllen LLP


Cyber Preparedness
©2021 CliftonLarsonAllen LLP
WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor
22

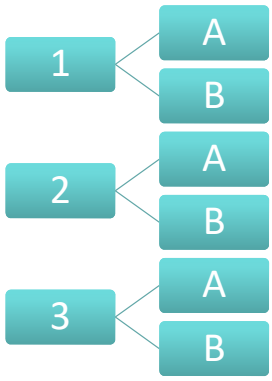
What can organizations do to prepare themselves for a potential cyber attack?

©2021 CliftonLarsonAllen LLP

1.Risk assess, classify, and inventory systems
- Determine Cyber standards you wish to align to your Security Architecture framework (NIST, CMMC, CIS Critical Controls)
- Conduct a Cyber Security Risk Assessment taking into consideration the Domains identified in the respective Framework e.g. Identify, Protect, Detect, Respond And Recover – Assess for both Design and Compliance
- Develop an immediate, short and long-term strategy for remediating findings identified as part of the review.
- Consider testing for compliance as part of your verification strategy

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

You mentioned penetration testing. Can you explain the internal and external testing approach by CLA?



©2021 CliftonLarsonAllen LLP

Can you talk about the importance of user education and testing?

©2021 CliftonLarsonAllen LLP

- 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.

Are there any controls on workstations
that organizations should consider?

©2021 CliftonLarsonAllen LLP

- Staff should not have local administrator rights to their PCs, workstations, and laptops.
- No email, browsing, or general computer use when using administrator level credentials.
- Network and domain administrators should be required to have two sets of credentials (general use and elevated privileges).
- Implement a policy and practice that stipulates administrators do NOT log into workstations with domain administrator rights.

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

©2021 CliftonLarsonAllen LLP

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

©2021 CliftonLarsonAllen LLP

Practice the Plan

- Like all emergency procedures, they need to be practiced
- 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
- Red Team penetration testing

©2021 CliftonLarsonAllen LLP

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

©2021 CliftonLarsonAllen LLP


Questions
©2021 CliftonLarsonAllen LLP
WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor
31

We're Here For You

Find additional resources and learn about upcoming events at CLAconnect.com.

Improving your financial health starts with an honest check-in.

Our guidance can help organizations and individuals stay on the right track.

Learn More

©2021 CliftonLarsonAllen LLP

Thank you!

Francis Nemia CISA, CRISC, CDPSE
Francis.Nemia@CLAconnect.com

Javier Young
Javier.Young@CLAconnect.com

David Sun CISSP, CCE, EnCE
David.Sun@CLAconnect.com

Randy Romes CISSP, CRISC, CISA, MCP, PCI-QSA
Randy.Romes@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

©2021 CliftonLarsonAllen LLP