Cybersecurity Risk Landscape

January 26, 2022

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

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.

Today's Discussion

- Current cybersecurity landscape
- Why cybersecurity is an issue for business owners and executives
- Common cyber attacks
- Managing cyber risks
- Q&A

Cybersecurity at CLA

Risk Assessment
- Regulatory compliance
- Framework readiness assessments
- Controls review
- Office365 review

Security/Vulnerability Assessment
- Penetration testing
- Vulnerability scanning
- Application testing
- Social Engineering (Phishing)
- Wireless penetration testing

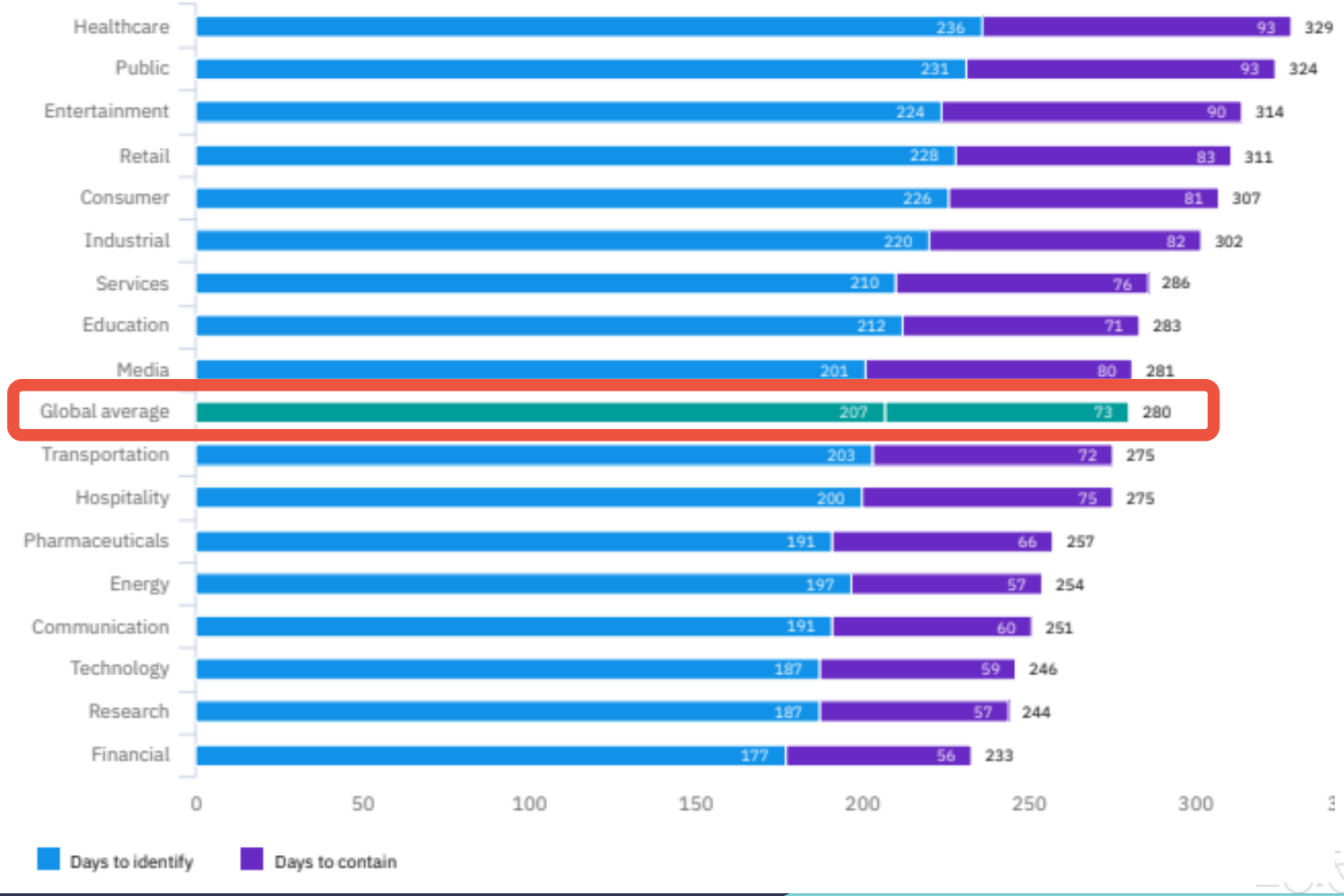
Security Integration
- Secure network infrastructure deployment
- Disaster recovery planning
- Business continuity planning
- Outsourced Information Security Advisor (OISA)

Incident Response & Readiness
- Data breach response
- Ransom negotiation
- System remediation
- Incident response testing
- Expert witness testimony

Cyber Facts & Stats

- Every 39 seconds there is a hacker attack
- Since COVID-19, the FBI reported a 300% increase in reported cybercrimes
- 95% of cyber security breaches are facilitated by human error
- 56% of Organizations don't require multi-factor authentication (MFA) to log into online accounts
- Ransomware attacks are estimated to cost $6 trillion annually by 2021
- Only 25% of Organization's have a Cyber Security Incident Response Plan

How Long Does it Take to Identify and Contain?



Source: IBM Security Cost of a Data Breach Report 2020

2021 global average increased by 7 days

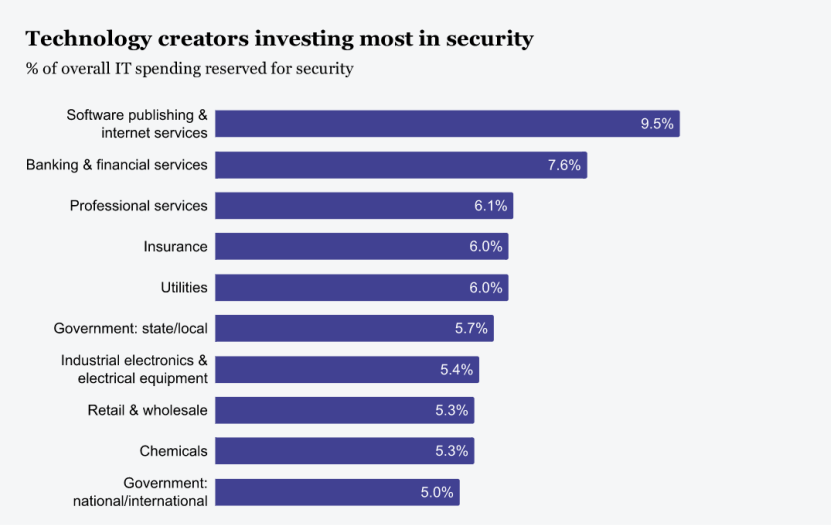
Question 1

- Before this presentation, did you think the average time to identify and contain a security incident was:
  - Less than 280 days
  - More than 280 days
  - Exactly 280 days

Why Cybersecurity is an Issue for Business Owners and Executives

Poor Leadership Examples on Cybersecurity

- Implementing appropriate cybersecurity measures is costly and inconvenient.
- Businesses want to avoid reputational damage from a data breach leading them to keep things quiet.
- Individuals are kept in the dark that their data has been compromised.



Samantha Ann Schwartz/Cybersecurity Dive, data from Gartner

Pre/Post-Breach Cyber Regulation Examples

- Depending on an organization's industry, there are various compliance "standards" to implement
- All 50 states and DC have legislation requiring notification
- Applicable law is based on location of impacted individual- not company
- Two general objectives:
  - Pre-Breach: Force businesses to spend money to implement protocols to reduce the likelihood of a breach
  - Post-Breach: Require business to notify impacted individuals of potential damages as a result of a breach

Post-Breach Penalties

- Equifax: (At least) $575 Million
- Home Depot: ~$200 million
- Uber: $148 million- (Executive Under Federal Indictment)
- Yahoo: $85 million
- Capital One: $80 million
- Morgan Stanley: $60 million
- Marriott: $23.7 million

Maryland Post-Breach Cyber Regulation

- “Breach of the security of a system” means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business.
- The notification shall be given as soon as reasonably practicable, but not later than 45 days
  - after the business discovers or is notified of the breach of the security of a system.
  - after the business concludes any investigations legally required.
- Prior to giving the notification a business shall provide notice of a breach of the security of a system to the Office of the Attorney General.
- No requirement on the minimum number of impacted individuals.

Question 2

- Do you know the physical address of every individual your organization has sensitive data on?
  - Yes
  - No
  - Not sure or N/A

Common cyber attacks

Top Causes of Data Breaches

- So much easier to steal passwords than hack into a system
- 91% attacks start with phishing!

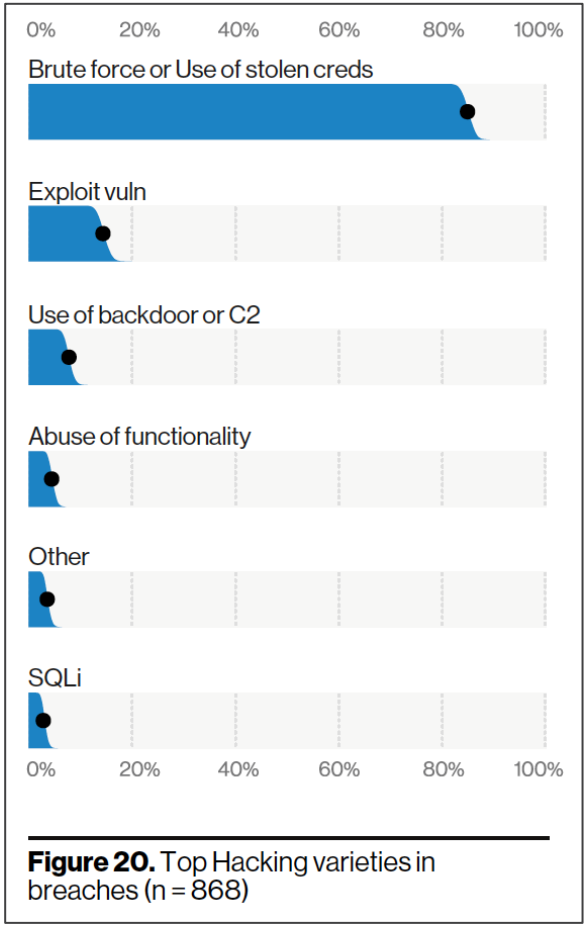


Figure 20. Top Hacking varieties in breaches (n = 868)

Source: 2020 Verizon DBIR

Question 3

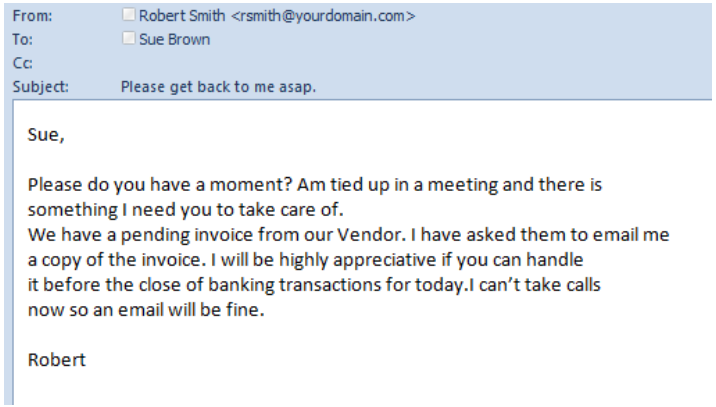
- Have you performed an email phishing test at your company in the past 6 months?
  - Yes
  - No
  - Not sure or N/A

Business Email Compromise

- Using the compromised (or guessed) credentials, they connect to your email server and download the contents.
  - What do you have in your email?
  - This by itself is a data breach
- Leverage the information learned from the emails
  - Email connections (CC vs. BCC)
  - Specific names of friends/family
  - Travel schedule
- Send out very convincing emails for other fraud schemes

CEO Fraud / Wire Fraud

- Victim legitimately wires funds from account
  - Very prevalent
  - Rarely recoverable
  - No wrongdoing from sender's bank
  - Friday afternoon before long weekend



From: Robert Smith <rsmith@yourdomain.com>
To: Sue Brown
Cc:
Subject: Please get back to me asap.

Sue,

Please do you have a moment? Am tied up in a meeting and there is something I need you to take care of.
We have a pending invoice from our Vendor. I have asked them to email me a copy of the invoice. I will be highly appreciative if you can handle it before the close of banking transactions for today.I can't take calls now so an email will be fine.

Robert

```
From: "Robert Smith" <rsmith@yourdomain.com>
To: "Sue Brown" <sbrown@yourdomain.com>
Subject: Please get back to me asap.
Reply-To: rsmith@attackerdomain.com
User-Agent: Roundcube Webmail/1.0.6
```

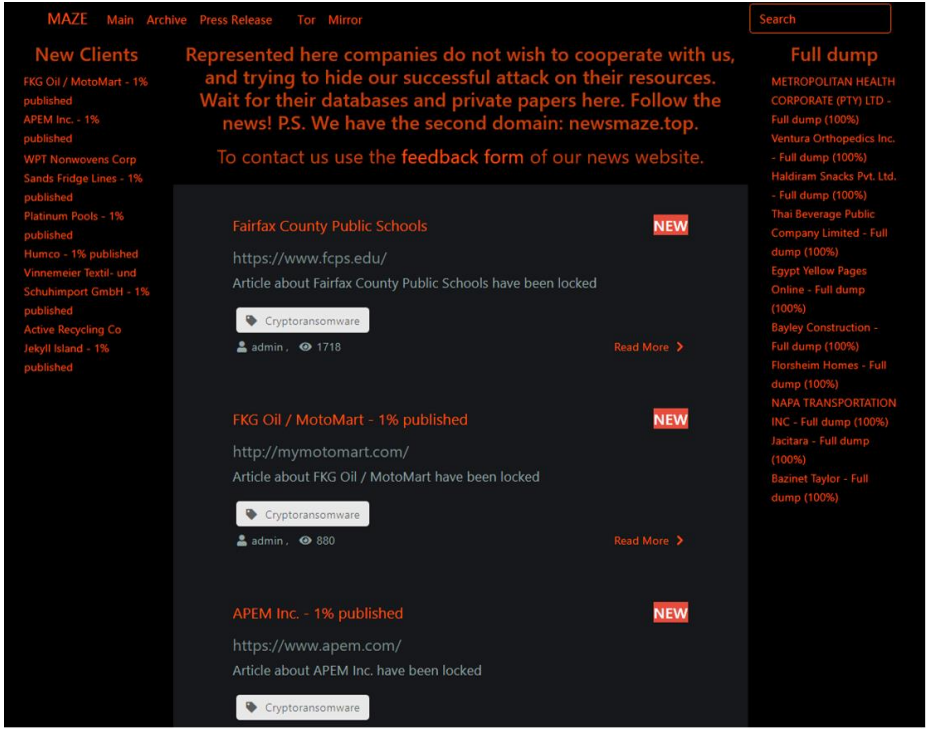
Ransomware (old fashioned)

- Caused by a computer “malware” introduced into the environment
- Encrypts all files accessible by computer
  - Computer internal hard drive
  - Network drives
- Ransomware options
  - Pay ransom for decryption key
  - Restore files from backup to state prior to encryption

It’s ransomware time, do you know where your backups are?

Ransomware Evolved

- As companies do a better job with backups, ransomware evolved
- Double extortion
  - Encrypting files is not the only activity
  - Data exfiltration
  - Demand payment not to release data
- Triple extortion (newer)
  - Calling clients to increase pressure
- Ransom amounts are increasing

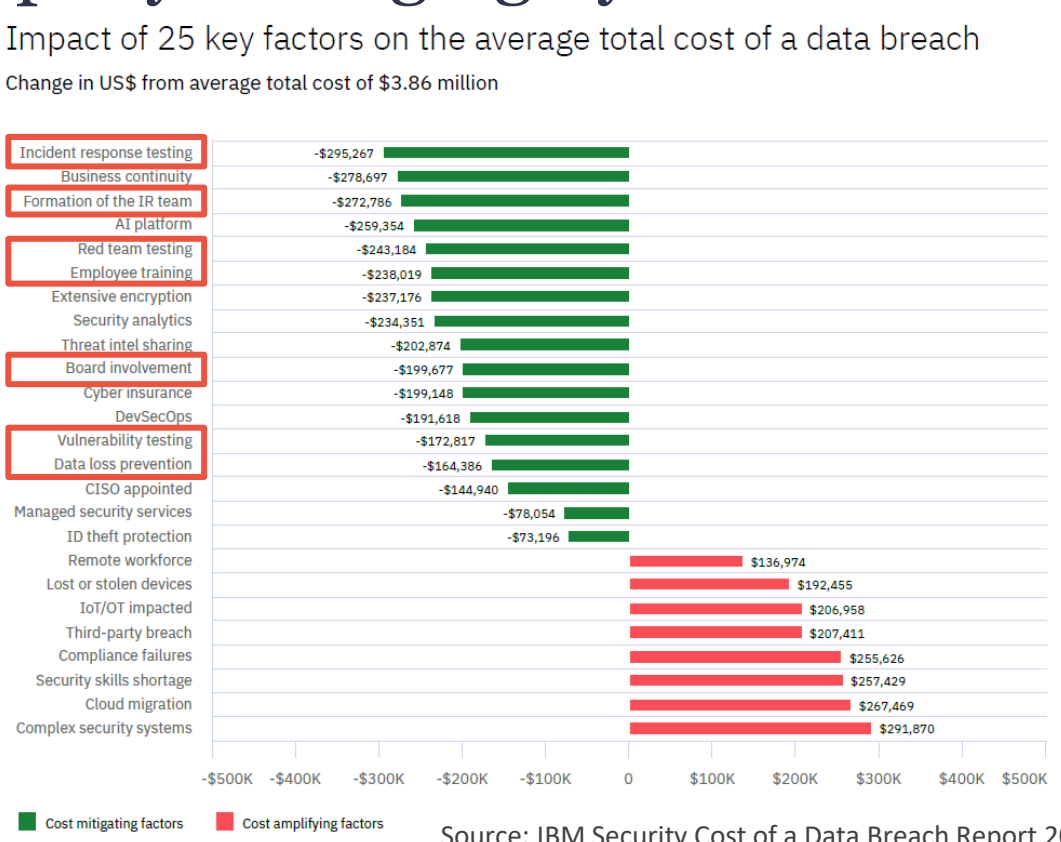


Question 4

- Do you have an incident response plan in place?
  - Yes
  - No
  - Not sure or N/A

Managing Cyber Security can make a Difference

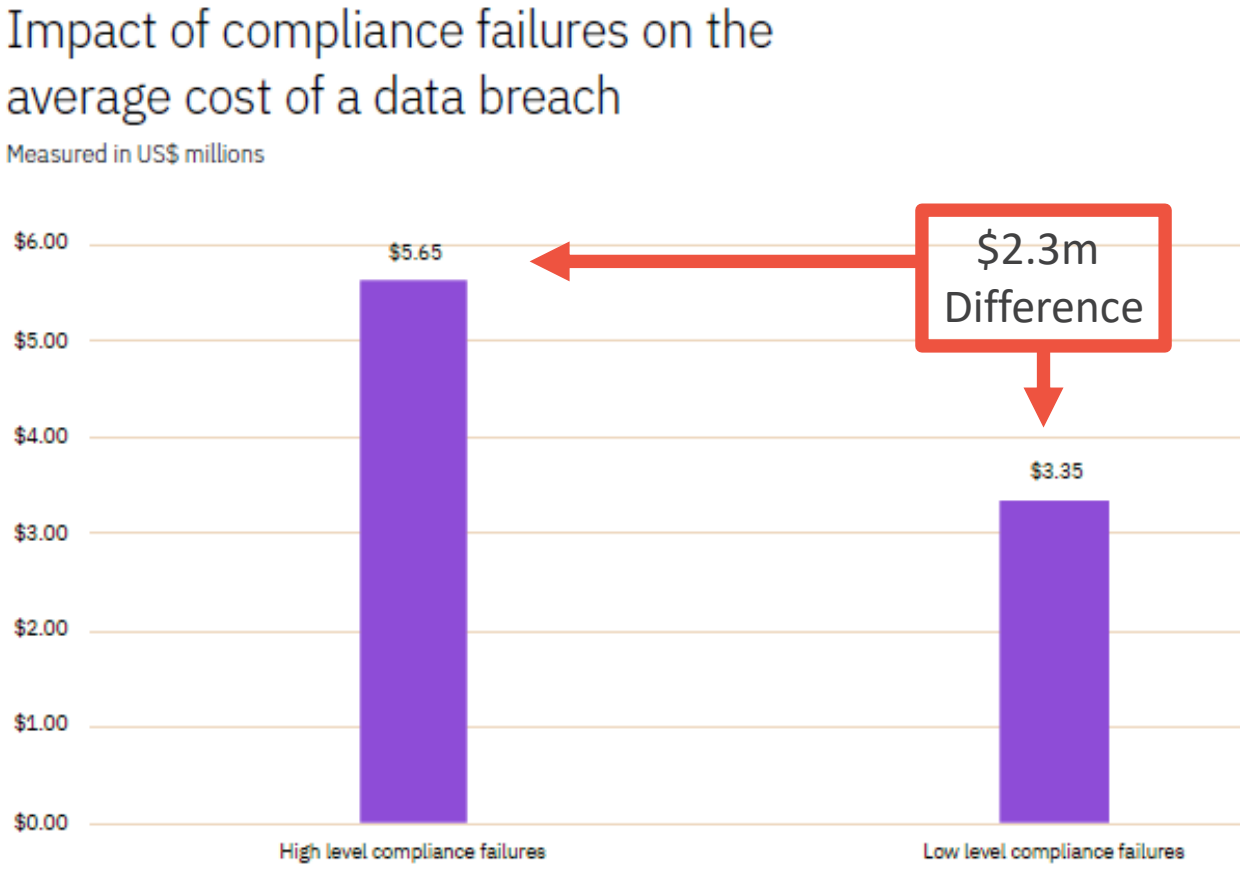
Properly Managing Cyber Risks makes a Difference



Source: IBM Security Cost of a Data Breach Report 2020

- 2021 average total cost was $4.24 million, up over 10% from 2020
- $2.98 million with less than 500 employees

Properly Managing Cyber Risks makes a Difference



Source: IBM Security Cost of a Data Breach Report 2021

Phillip Del Bello

phillip.delbello@claconnect.com

410-308-8181

David Sun

david.sun@claconnect.com

703-483-2650

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING