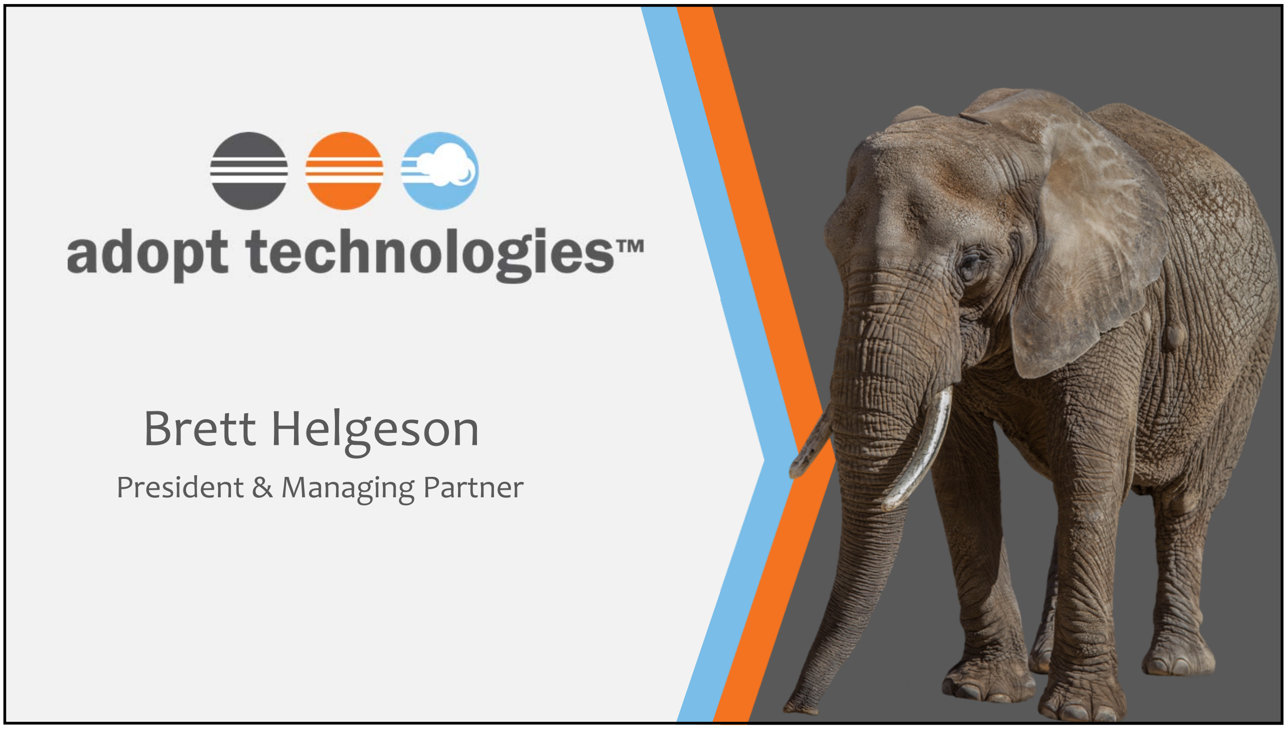


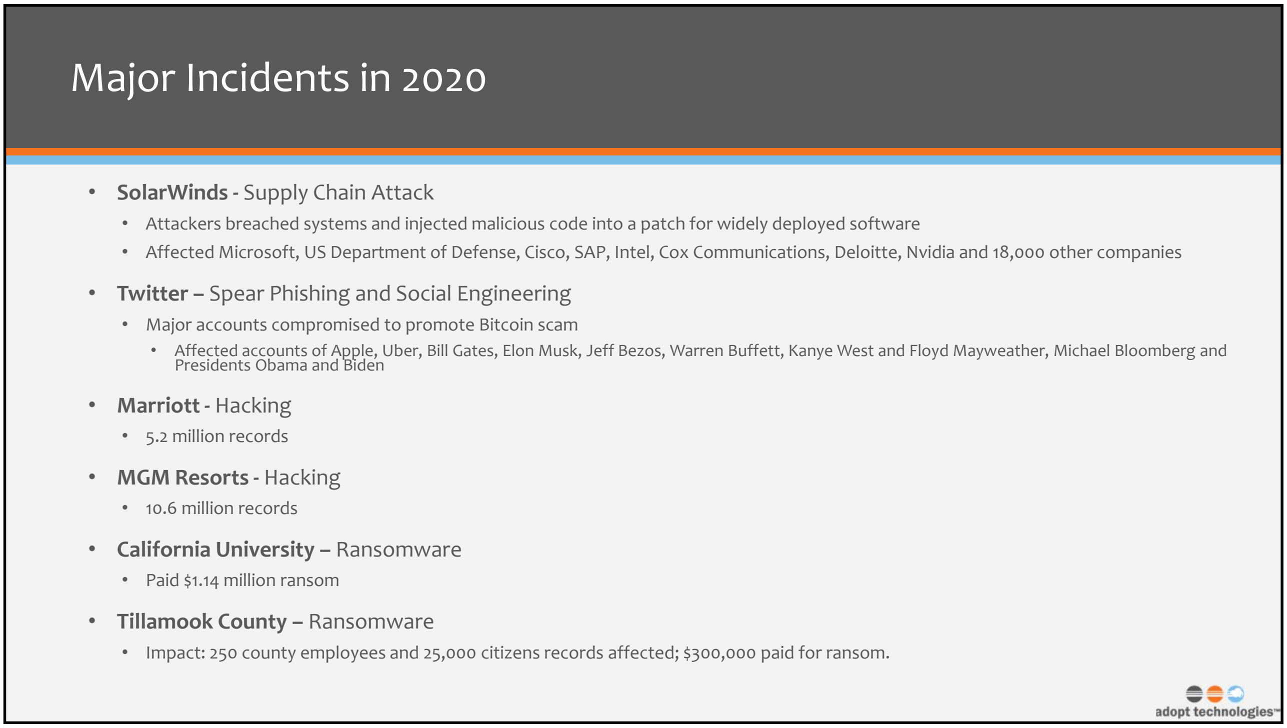
adopt technologies™

Brett Helgeson

President & Managing Partner

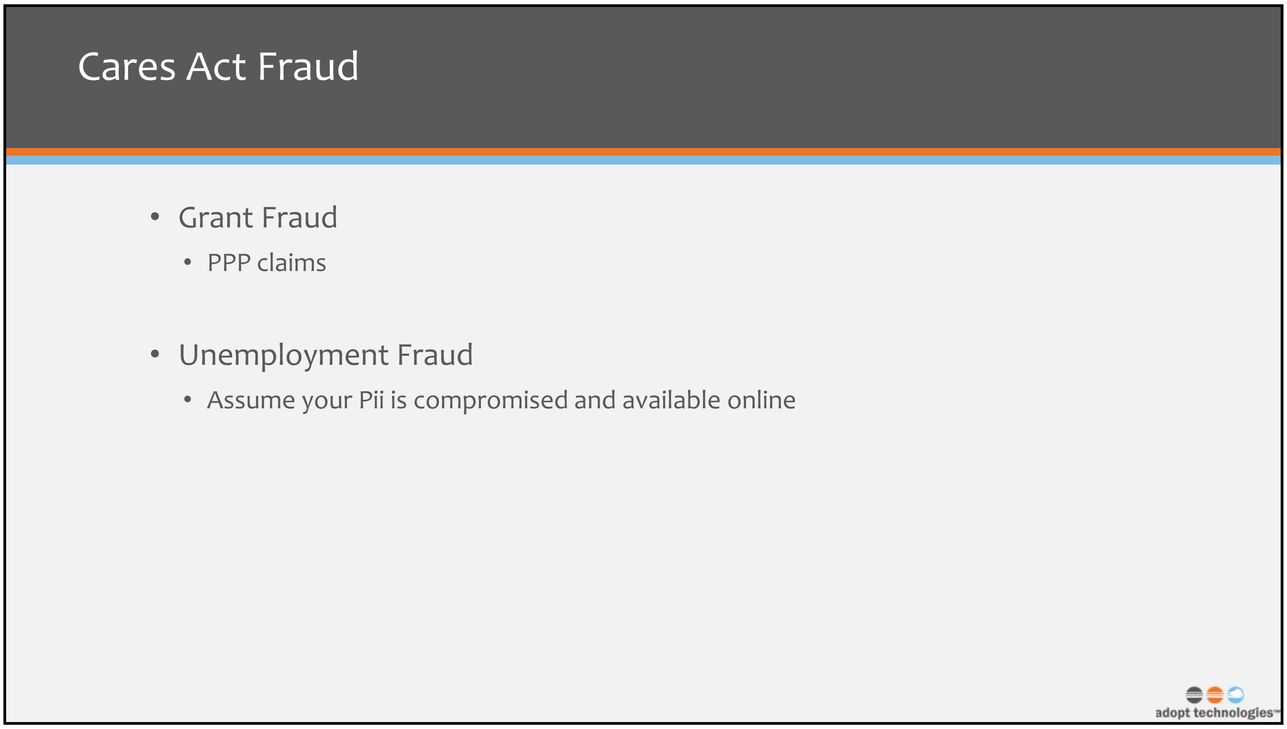
IT Security in the New Normal

- Recap of major events
- State of security update
- Improving your security posture
- The new normal
- Q & A
- Adopt Technologies Overview



Major Incidents in 2020

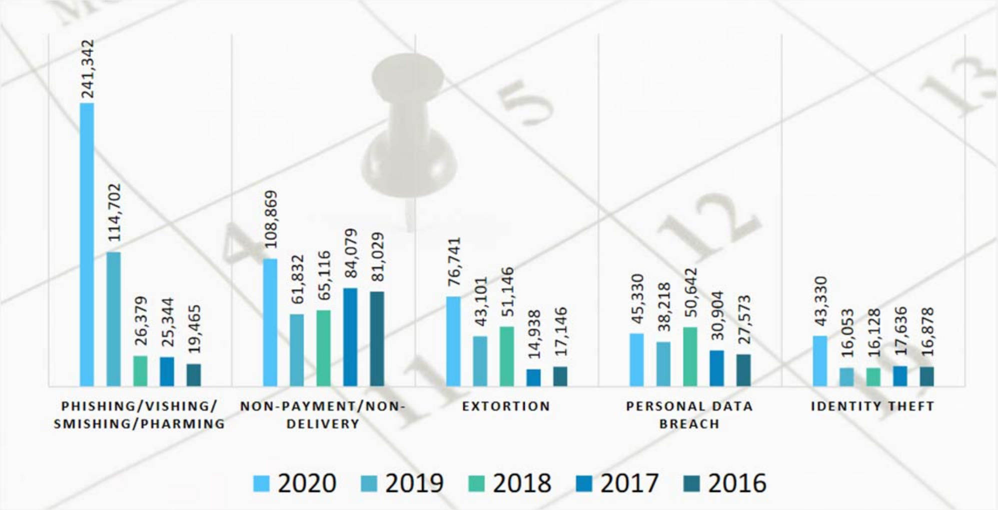
- **SolarWinds -** Supply Chain Attack
  - Attackers breached systems and injected malicious code into a patch for widely deployed software
  - Affected Microsoft, US Department of Defense, Cisco, SAP, Intel, Cox Communications, Deloitte, Nvidia and 18,000 other companies
- **Twitter –** Spear Phishing and Social Engineering
  - Major accounts compromised to promote Bitcoin scam
    - Affected accounts of Apple, Uber, Bill Gates, Elon Musk, Jeff Bezos, Warren Buffett, Kanye West and Floyd Mayweather, Michael Bloomberg and Presidents Obama and Biden
- **Marriott -** Hacking
  - 5.2 million records
- **MGM Resorts -** Hacking
  - 10.6 million records
- **California University –** Ransomware
  - Paid $1.14 million ransom
- **Tillamook County –** Ransomware
  - Impact: 250 county employees and 25,000 citizens records affected; $300,000 paid for ransom.



Cares Act Fraud

- Grant Fraud
  - PPP claims
- Unemployment Fraud
  - Assume your Pii is compromised and available online

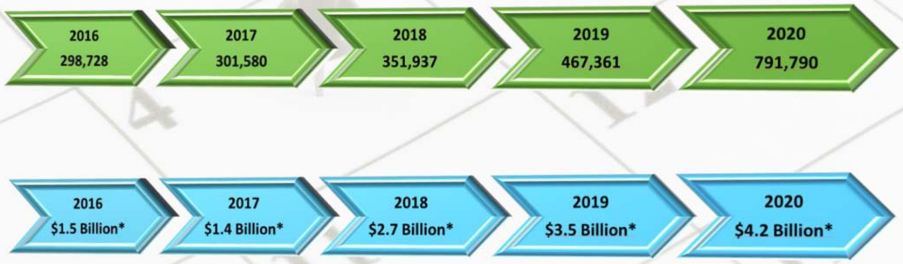
Top 5 Crime Type Comparison – Incidents Last Five Years



adopt technologies™

IC3 Complaint Stats – Last Five Years - FBI iC3 (Internet Crime Complaint Center)

2,211,396 TOTAL COMPLAINTS



2016 298,728

2017 301,580

2018 351,937

2019 467,361

2020 791,790

2016 $1.5 Billion*

2017 $1.4 Billion*

2018 $2.7 Billion*

2019 $3.5 Billion*

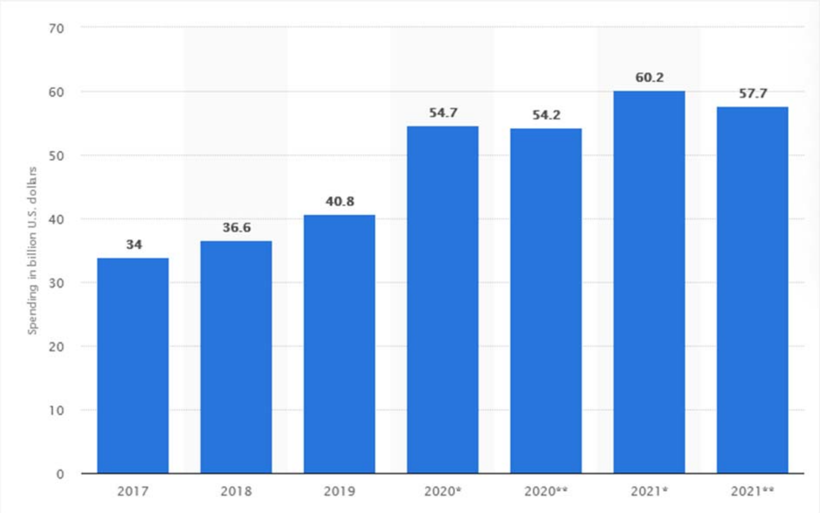
2020 $4.2 Billion*

$13.3 Billion TOTAL LOSSES*

(Rounded to the nearest million)

adopt technologies™

Cybersecurity Spending from 2017 to 2021



adopt technologies

Business Email Compromise (BEC)

- $1.8 billion in losses in 2020
  - More than doubled over previous years
- Social engineering
- Appears to be coming form legitimate source
  - Requesting W-2's
  - Redirecting of payment for bills or large transactions
- Can only be addressed by training at the end user level
- Requests or changes to transactions must be confirmed directly – not over email/text

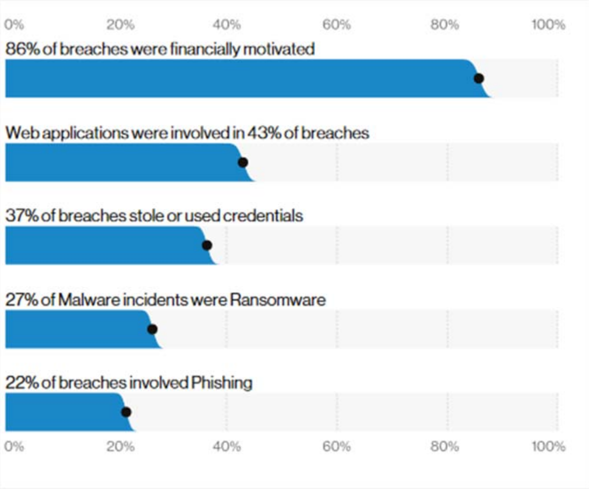
adopt technologies

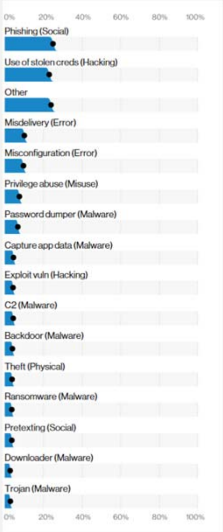
Cost of a data breach in 2020 (IBM)

- Average US company data breach cost $8.64 million
- Average time to identify and contain a breach – 280 days
- According to the National Cybersecurity Alliance, 10% of small businesses that had a data breach shut down.
- According to Cybersecurity Ventures, the costs of cybercrime is estimated to hit $10.5 Trillion USD annually by 2025

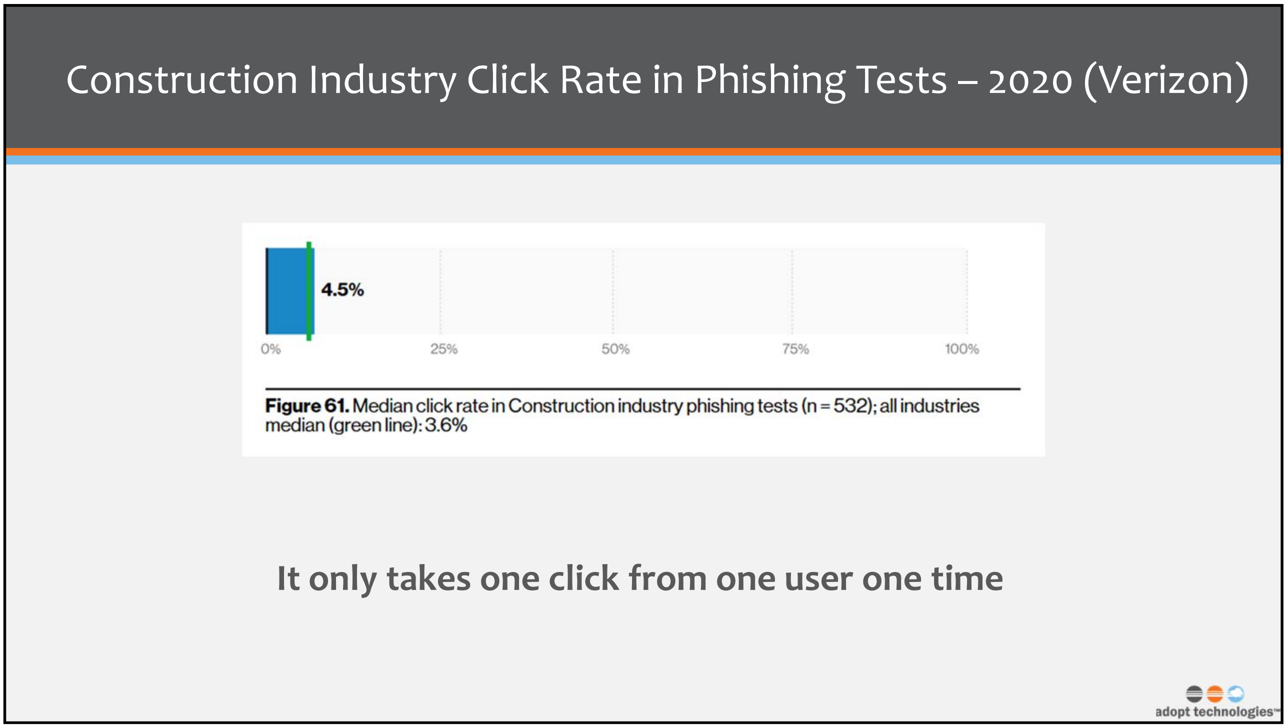
adopt technologies™

Incident and Breach Breakdown and Attack Vector (Verizon)





adopt technologies™

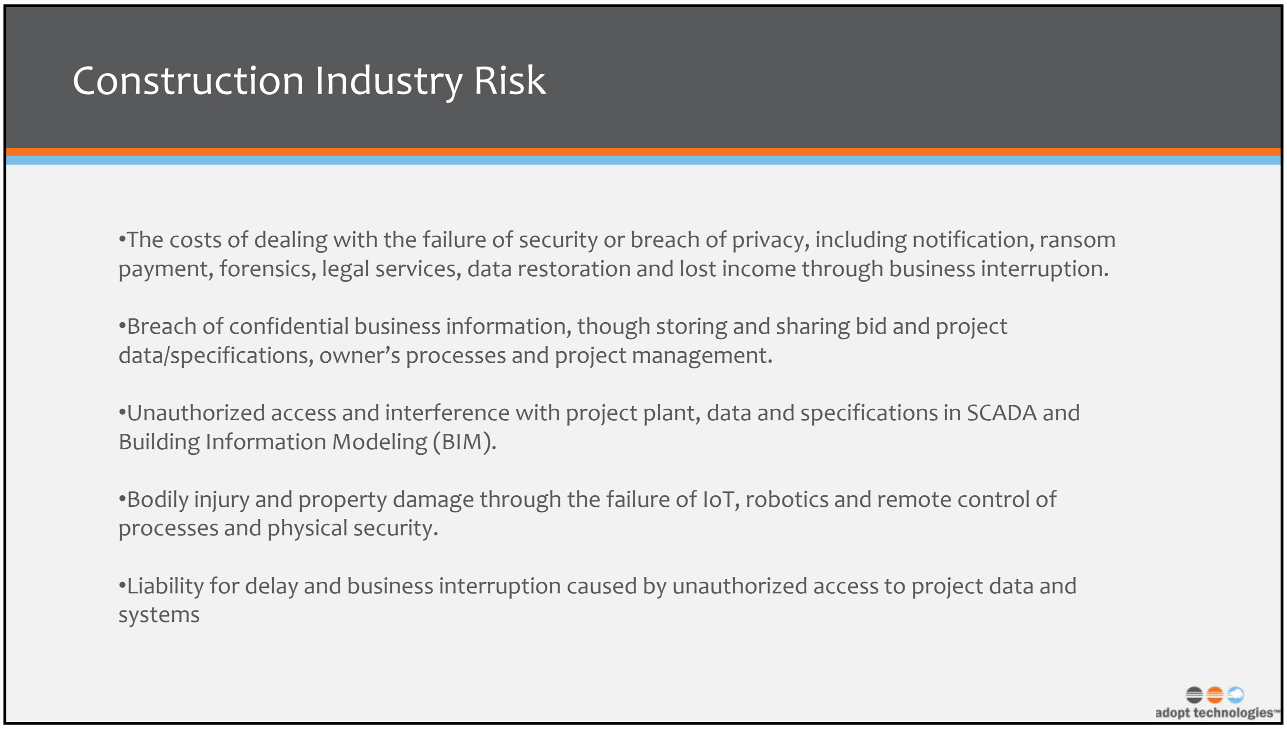


Construction Industry Click Rate in Phishing Tests – 2020 (Verizon)

Figure 61. Median click rate in Construction industry phishing tests (n = 532); all industries median (green line): 3.6%

It only takes one click from one user one time

adopt technologies



Construction Industry Risk

•The costs of dealing with the failure of security or breach of privacy, including notification, ransom payment, forensics, legal services, data restoration and lost income through business interruption.

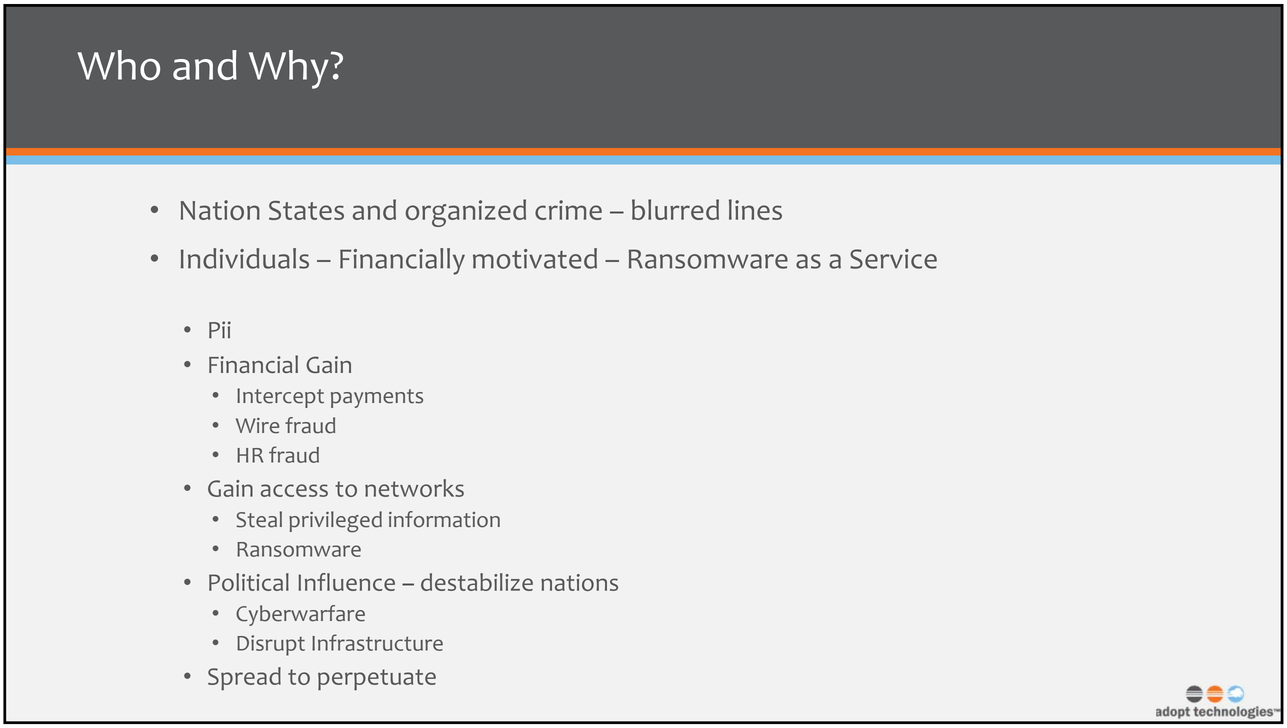
•Breach of confidential business information, though storing and sharing bid and project data/specifications, owner's processes and project management.

•Unauthorized access and interference with project plant, data and specifications in SCADA and Building Information Modeling (BIM).

•Bodily injury and property damage through the failure of IoT, robotics and remote control of processes and physical security.

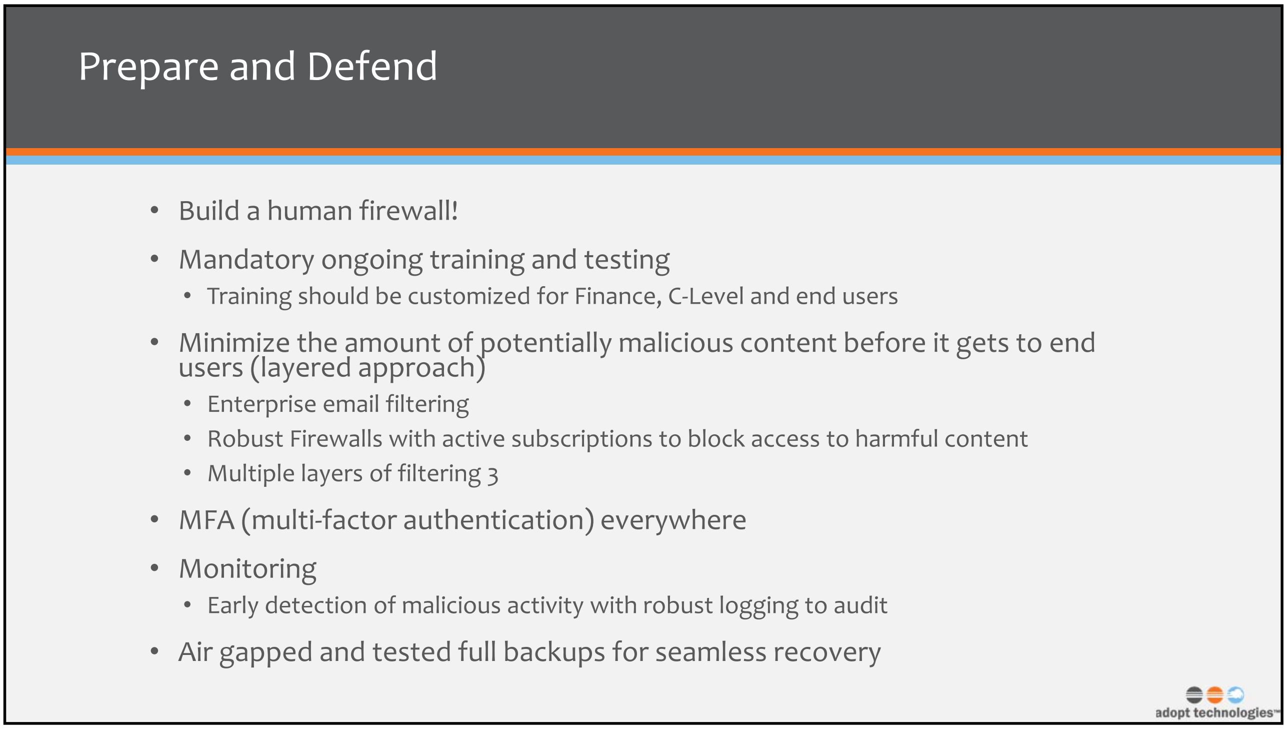
•Liability for delay and business interruption caused by unauthorized access to project data and systems

adopt technologies



Who and Why?

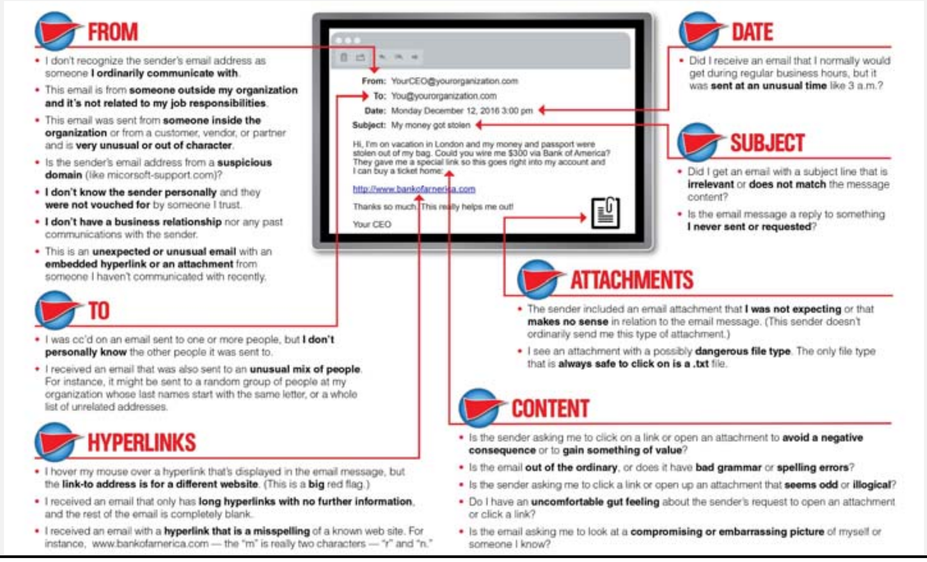
- Nation States and organized crime – blurred lines
- Individuals – Financially motivated – Ransomware as a Service
  - Pii
  - Financial Gain
    - Intercept payments
    - Wire fraud
    - HR fraud
  - Gain access to networks
    - Steal privileged information
    - Ransomware
  - Political Influence – destabilize nations
    - Cyberwarfare
    - Disrupt Infrastructure
  - Spread to perpetuate



Prepare and Defend

- Build a human firewall!
- Mandatory ongoing training and testing
  - Training should be customized for Finance, C-Level and end users
- Minimize the amount of potentially malicious content before it gets to end users (layered approach)
  - Enterprise email filtering
  - Robust Firewalls with active subscriptions to block access to harmful content
  - Multiple layers of filtering 3
- MFA (multi-factor authentication) everywhere
- Monitoring
  - Early detection of malicious activity with robust logging to audit
- Air gapped and tested full backups for seamless recovery

Social Engineering Red Flags



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

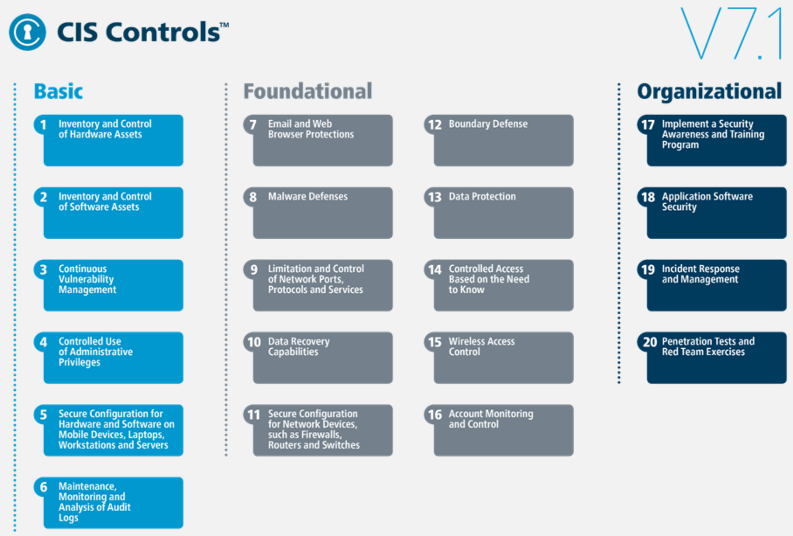
CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

The New Normal

- Hybrid remote work
  - Not new for construction industry
- Vulnerable portable devices
  - Harder to secure physically and virtually
  - VPN is clunky
    - Requires user interaction
    - Slow
    - Incomplete
- Modern Options
  - Remote access to hosted systems (Cloud)
  - Complete solutions including MDM and built-in remote access to files and applications

CIS (Center for Internet Security) Top 20 Controls



CIS Controls™

V7.1

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

adopt technologies™

Resources

https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency

https://www.znetlive.com/blog/top-10-cybersecurity-incidents-in-2020/

https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf

https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

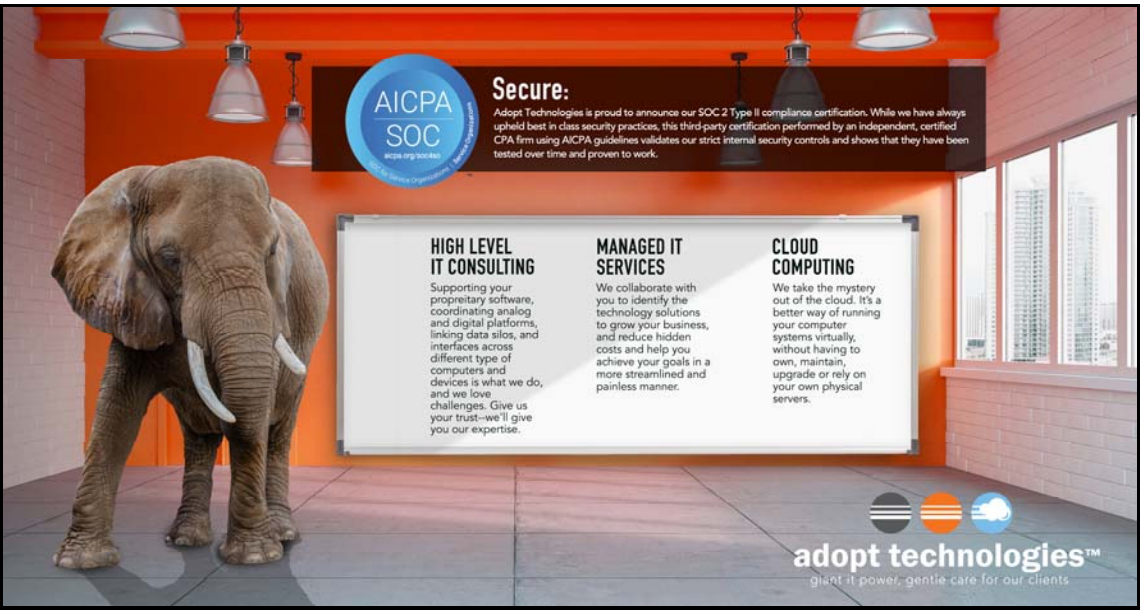
https://www.ibm.com/security/data-breach

https://www.ajg.com/us/news-and-insights/2020/jun/cyber-risk-within-construction-industry/

https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/

adopt technologies™

Questions?


AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
adopt technologies™
giant it power, gentle care for our clients

Secure:

Adopt Technologies is proud to announce our SOC 2 Type II compliance certification. While we have always upheld best in class security practices, this third-party certification performed by an independent, certified CPA firm using AICPA guidelines validates our strict internal security controls and shows that they have been tested over time and proven to work.

HIGH LEVEL IT CONSULTING

Supporting your propreitary software, coordinating analog and digital platforms, linking data silos, and interfaces across different type of computers and devices is what we do, and we love challenges. Give us your trust--we'll give you our expertise.

MANAGED IT SERVICES

We collaborate with you to identify the technology solutions to grow your business, and reduce hidden costs and help you achieve your goals in a more streamlined and painless manner.

CLOUD COMPUTING

We take the mystery out of the cloud. It's a better way of running your computer systems virtually, without having to own, maintain, upgrade or rely on your own physical servers.

Brett Helgeson
President & Managing Partner

480.422.6400
bretth@adopttechnologies.com