FORVIS

Cybersecurity Risks in a Post COVID-19 World

February 22, 2023

TO RECEIVE CPE CREDIT

- You must respond to at least 3 of the 4 polling questions per CPE hour
- You must be logged in for a minimum of 50 minutes per every CPE hour in order to receive CPE credit

FORVIS

Presenter

Cy Sturdivant, CISA®
Director | Advisory
Nashville, Tennessee
cy.sturdivant@forvis.com
615.988.3596

FORVIS

My world in a nutshell!

Cybersecurity Industry Trends & Statistics

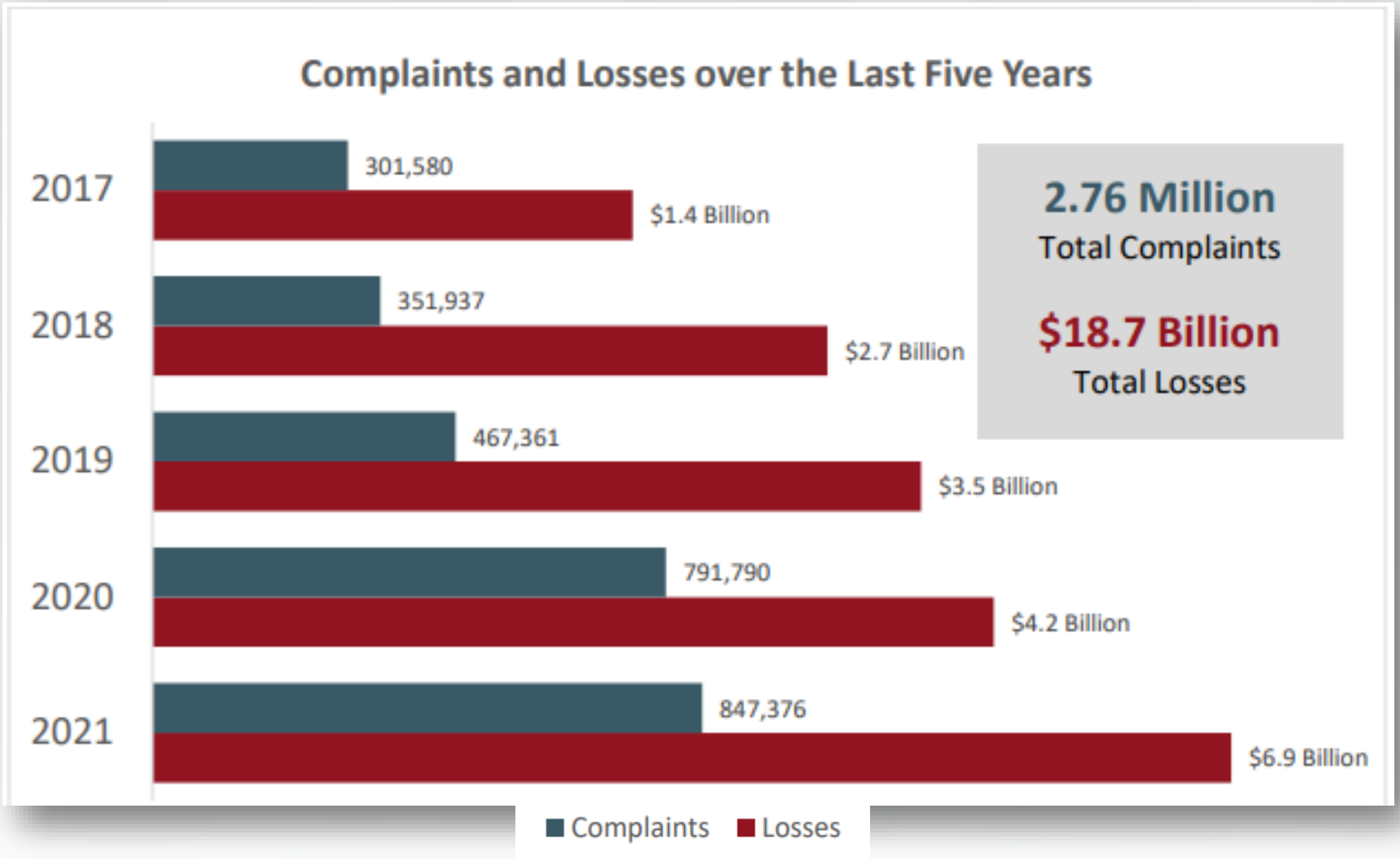
FORVIS

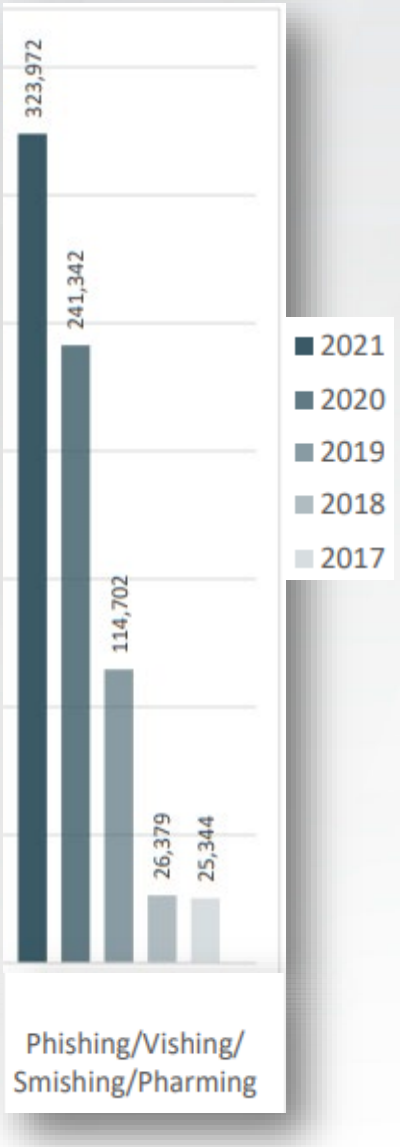
2022 Verizon Data Breach Investigation (DBI) Report

- **Ransomware-related breaches increased by 13%,** *(more than the past five years combined)*
- Nearly 50% of all system intrusion *incidents* involved ransomware last year
  - Ransomware was present in almost 70% of malware breaches in the past year
- **Supply chain was involved in 62% of incidents** this year. *Compromising the right partner is a force multiplier for threat actors*
- **82% of the breaches** reported involved the use of stolen credentials, phishing, misuse or human errors. People still play a large role!

https://www.verizon.com/business/resources/reports/dbir/

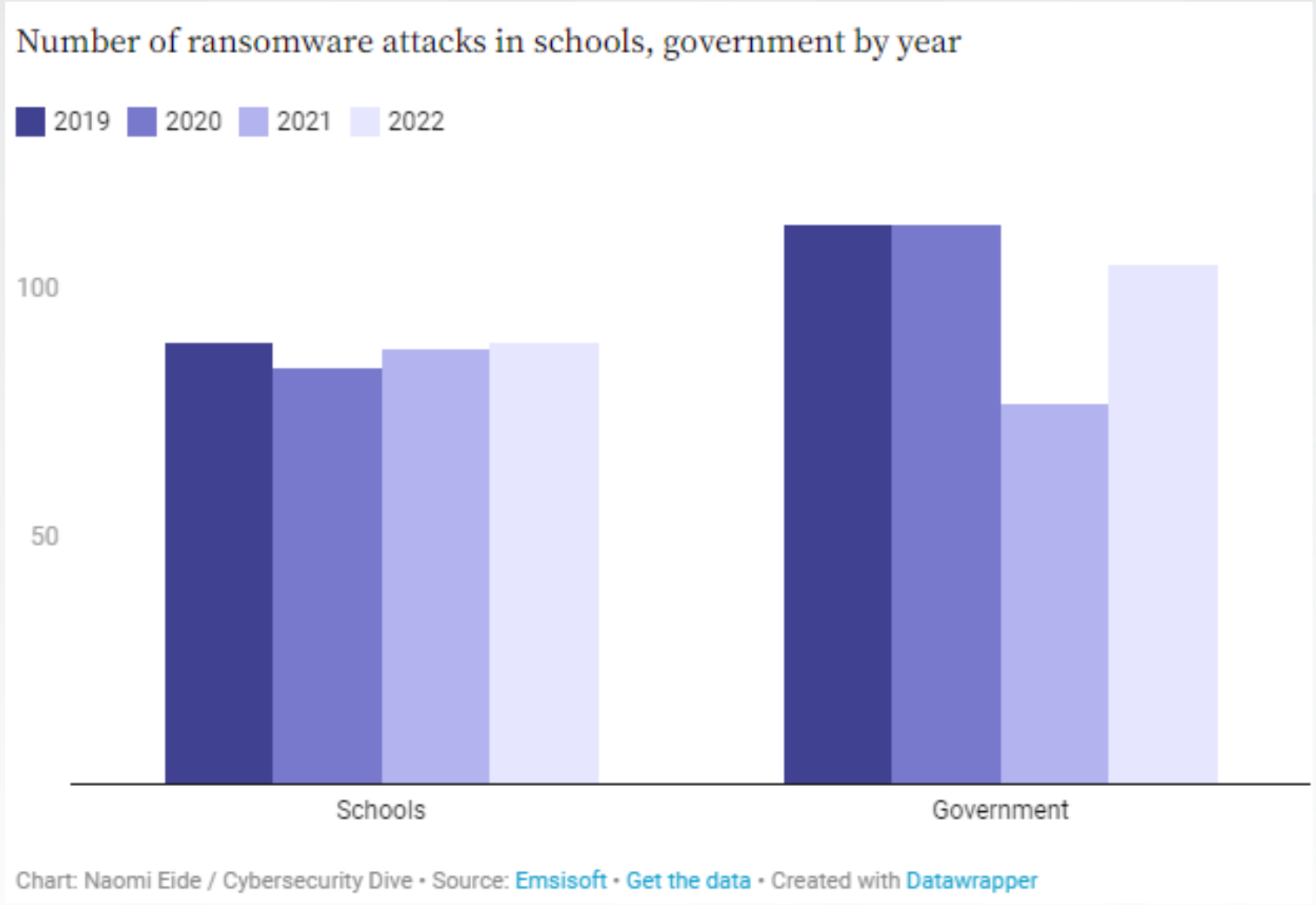
FBI's Internet Crime Complaint Center (IC3) Five-Year Statistics





FORV/S

Schools/Government Four Year Statistics



School districts hit by ransomware in 2022 represent 1,981 schools, almost double the amount of K-12 schools potentially compromised in 2021

Ransomware groups successfully exfiltrated data from U.S. schools at a rate of nearly two-thirds in 2022, up from half of all organizations hit in 2021

FORVIS

Breach Detection & Expense

You can't afford to ignore cybersecurity – Especially now!

Public sector average total cost of a data breach is **$2.07 million ($1.93)**

In the U.S., average total cost of a data breach is **$9.44 million ($9.05)**

Average cost per lost or stolen record is **$161 ($146)**

Mean time to identify a breach **207 days**

Mean time to contain **70 days**

Companies with an incident response team & extensive testing of their response plans saved over $2 million compared to those who did not

Source: Ponemon Institute 2022 Cost of Data Breach Study

FORVIS

Cybersecurity Events/News – Past 16 Months

- LastPass – 33 million customers impacted
- Los Angeles Unified School District – 250,000 files compromised
  - California Transit – Data exposure (unknown)
- T-Mobile – 37 million customer's data breached
- *Log4J Vulnerability – Global software vulnerability

Public Sector: Atlanta, Georgia; Baltimore ($10M), Maryland; St. Lucie, Florida; New Orleans, Louisiana; and Greenville, North Carolina

FORVIS

Cybersecurity Threats & Impacts

FORVIS

Most Common Cybersecurity Threats

- Social engineering attacks – phishing
- Business email compromise
- Supply chain attacks
- Malware/destructive malware
  - Ransomware (Lockbit)
  - Remote access
  - Keyloggers
- Cloud applications/web applications

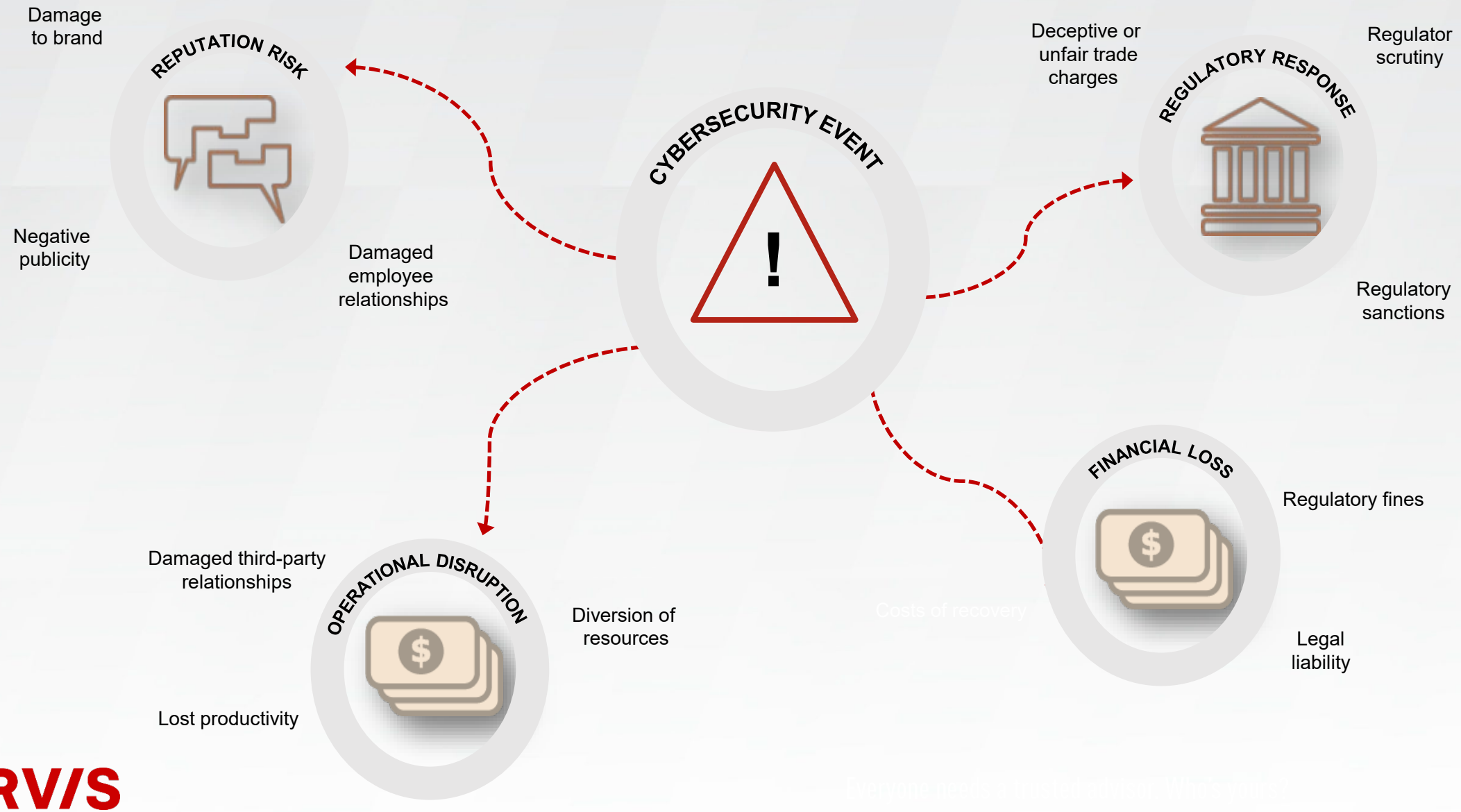
Top Five Most Affected Websites for Phishing

- Tiktok.com (delete now!)
- Instagram.com
- Facebook.com
- Linkedin.com
- Discord.com

Root causes of cyberattacks: Inadequate training, ineffective patch management, weak privileged access controls, & unmonitored detection systems

FORVIS

Breach Impacts



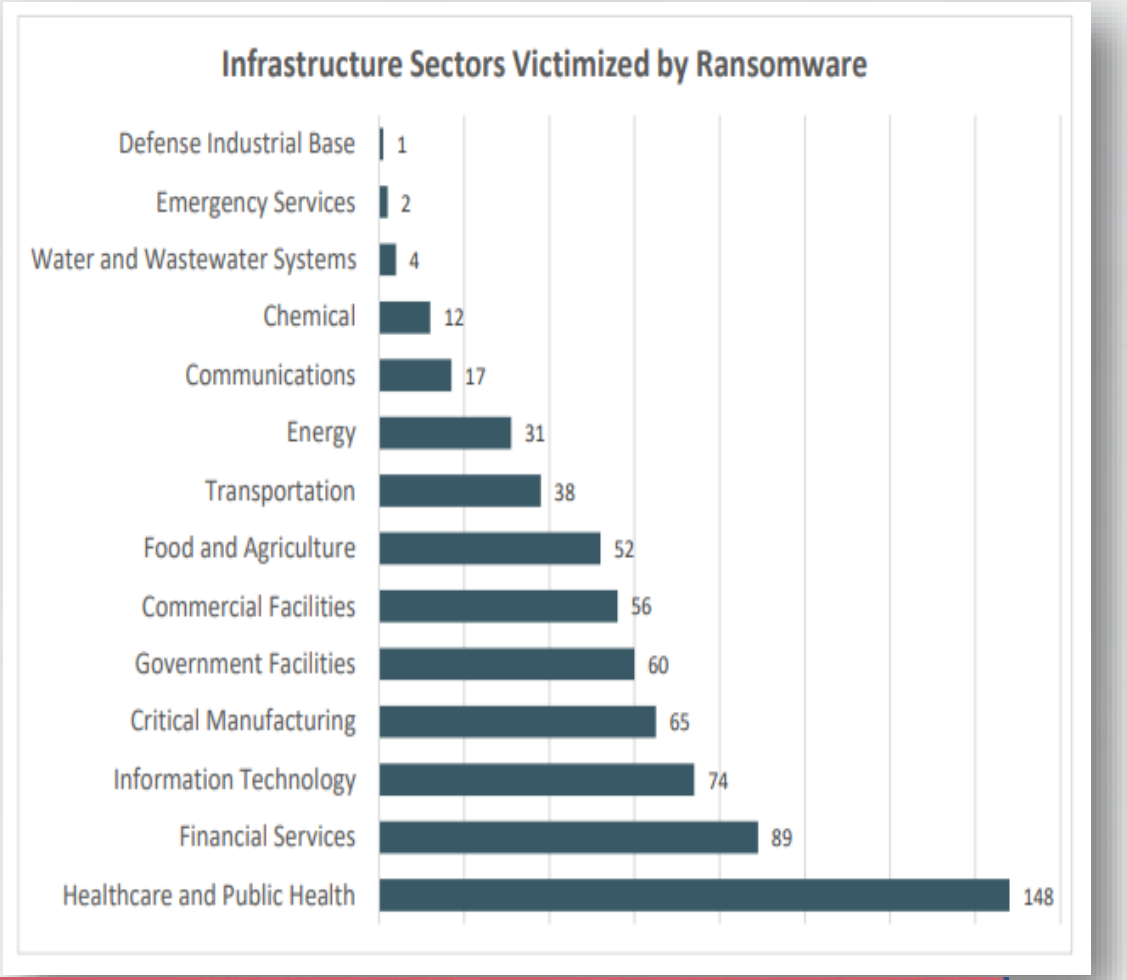
FORVIS

IC3 – Ransomware Fast Facts

The average downtime for a ransomware incident is 16 to 21 days*

For 2021, the FBI's IC3 received 3,729 complaints identified as ransomware with adjusted losses of more than **$49.2 million**

There were 2,474 complaints files in 2020 representing a **66% increase** from 2020 to 2021."2021_IC3Report.pdf"



FORVIS

IC3 – Business Email Compromise (BEC)

In 2021, the IC3 received **19,954 complaints** of Business Email Compromise (BEC)/Email Account Compromise (EAC) complaints with adjusted losses at nearly **$2.4 billion**.

*Note: BEC fraud has cost businesses around the world **$43 billion** during the period between June 2016 & December 2021*

IC3 Recovery Asset Team (RAT) Guidance

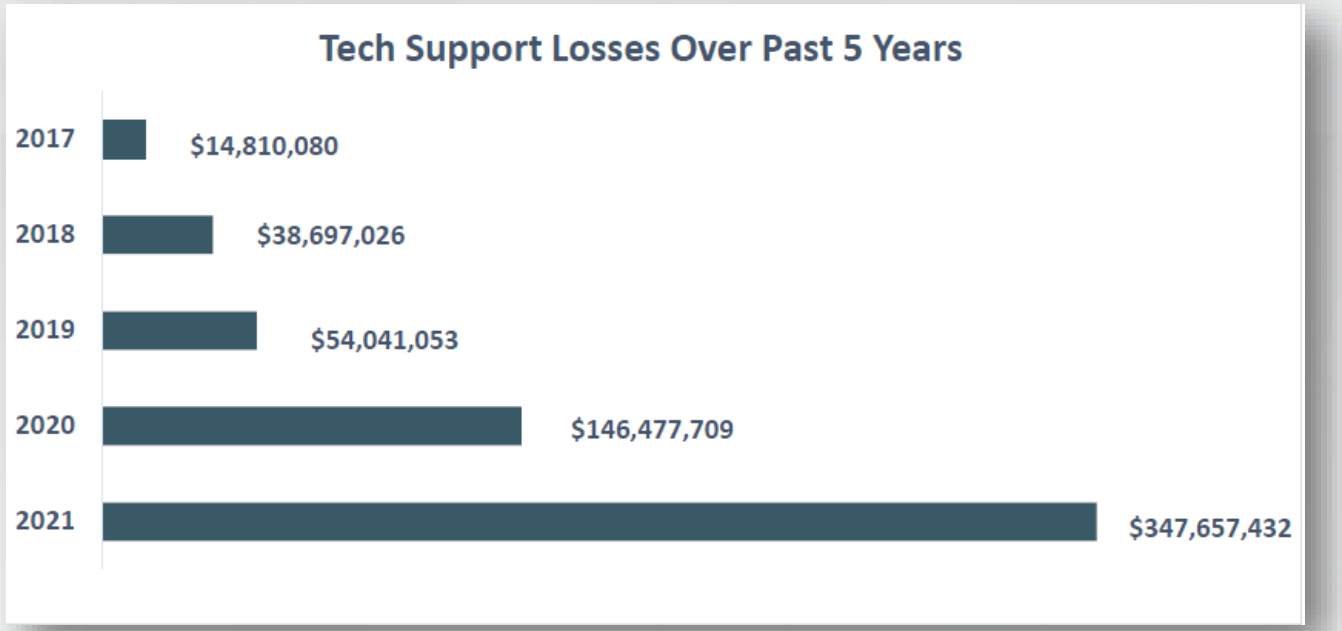
- Contact the originating financial institution as soon as fraud is recognized to request a recall or reversal & a Hold Harmless Letter or Letter of Indemnity
- File a detailed complaint with www.ic3.gov. It is vital the complaint contains all required data in provided fields, including banking information
- Visit www.ic3.gov for updated PSAs regarding BEC trends as well as other fraud schemes targeting specific populations, like trends targeting real estate, pre-paid cards, & W-2s, for example
- Never make any payment changes without verifying the change with the intended recipient; verify email addresses are accurate when checking email on a cell phone or other mobile device

FORVIS

Tech Support Fraud

In 2021, the IC3 received **23,903 complaints** related to tech support fraud from victims in 70 countries. The losses amounted to more than $**347 million**, up ***137% since 2020***

In 2021, the IC3 observed an increase in complaints reporting the impersonation of customer support in the form of financial institutions, utility companies, or virtual currency exchanges



Note: Criminals will often impersonate well-known tech companies, offering to fix non-existent technology issues or renew fraudulent software or security subscriptions

FORVIS

Why Are Your Sectors a Target?

- Aging infrastructure, limited revenue sources, regulatory changes, etc.
- Significant budgetary constraints
- Public Sector = Significant amount of sensitive data
- Threat actors can remain undetected for long periods of time
- You need more cyber-skilled employees

FORVIS

“You” Are the Target

Importance of Awareness Training

C-level executives are 12 times more likely to be the target of social engineering attacks

Are you trained more than employees?

If not, why?

FORVIS

Industry Best Practices

FORVIS

IT vs. IS – Both Have Their Roles

Information Technology	Information Security
Top priority: Ensuring hardware, software, network, etc. remains functional	**Top priority:** Protecting data & assets at all costs
Responsible for new technology implementations & maintenance	Responsible for systems, processes, & risks posed by end users
Puts controls in place	Monitors controls to ensure they work as designed
Stays up to date on new hardware, software, & solutions	Stays up to date on new threats & developments that emerge daily
Often measured in uptime & response times	Recommends & prioritizes action steps & solutions
“Fix-it” mentality	“Secure-it” mentality

FORVIS

Key Considerations: Focus on Governance Controls

- Maintain a strong **information security program**
- Maintain a strong **incident response program**
- Ensure **business continuity/DR** & **vendor management** policies & procedures address cybersecurity
- Consider how **cybersecurity insurance** should fit into your risk management program
- Ensure **cybersecurity awareness training** is performed regularly (educate & motivate)
- Join **an information sharing & analysis center (ISAC)** or other information sharing forums – filter reports based on each employees' role
- Perform **frequent cyber risk assessments**, penetration tests, vulnerability assessments, ransomware assessments, etc.

FORVIS

Key Considerations: Focus on Technical Controls

- Use **multifactor** or **two-factor** for O365, VPN, remote sessions, & privileged access
- Track, report, independently test, & update security **patches** based on a risk priority schedule (Microsoft & non-Microsoft patches)
- Maintain accurate **asset inventories** for hardware & software, including **data classification**
- Enforce **application whitelisting** controls & **remove** unauthorized applications
- **Remove local administrator** rights to reduce malicious software installs
- **Constantly adjust existing security tools** – web content, email filtering, end point, etc.
- Deploy **cloud-based security** software & end-point protection (SentinelOne, Crowdstrike, Windows Defender, etc.)

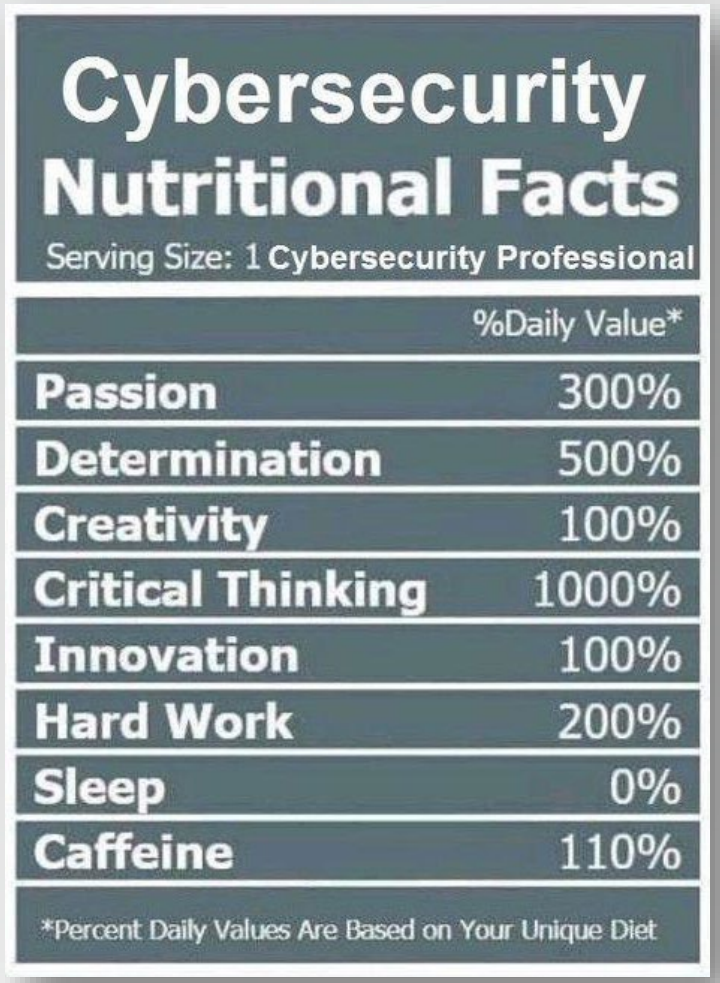
FORVIS

Key Considerations: Technical Controls

- Implement strong cloud-based **data loss prevention** controls
- Use **security information & event management (SIEM)** tools with **“defense in depth”** approach
- **Strengthen** your passwords! Do not use single words.
- Ensure **data encryption** is enforced to protect confidential data
- **Segment** internal networks to isolate critical systems
- Be aware of **insider threat** – layoffs, disgruntled, etc. Think zero trust!
- **Air gap** your backups to keep them out of reach of an attack
- Make your air-gapped backups **immutable**!

FORVIS

Cybersecurity Health



A strong cybersecurity culture & overall program is a must going forward!

Are you taking care of your “cybersecurity health”?

This is the best way you can be ***prepared*** for an attack

FORVIS

Final Thoughts & Conclusion

FORVIS

A Dangerous Perception

Perception of Your Security Controls

vs.

Your Actual Security Controls

FORVIS

A Quote to Motivate

Hearing *is not the same as* ***listening****!*

- Every Mom

FORVIS

Other Resources

- Infosec Institute – https://resources.infosecinstitute.com/
- Info Risk Today – https://www.inforisktoday.com/
- Security Week – https://www.securityweek.com/
- Dark Reading – https://www.darkreading.com/
- The Top Cyber Threat Intelligence Feeds – https://thecyberthreat.com/cyber-threat-intelligence-feeds/

FORVIS

Questions?

Email: cy.sturdivant@forvis.com

Phone: 615.988.3596

FORVIS

CONTINUING PROFESSIONAL EDUCATION (CPE) CREDIT

FORVIS, LLP is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

FORVIS

CPE CREDIT

- CPE credit may be awarded upon verification of participant attendance
- For questions, concerns, or comments regarding CPE credit, please email FORVIS at cpecompliance@forvis.com

FORVIS

Thank you!

forvis.com

FORVIS

Assurance / Tax / Advisory