FORVIS

2022 - Don't Be a Headline: Know Your Cyber Risks

Presenter

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

FORVIS

BKD

My world in a nutshell!

Cybersecurity Trends, Threats and Impacts

FORVIS

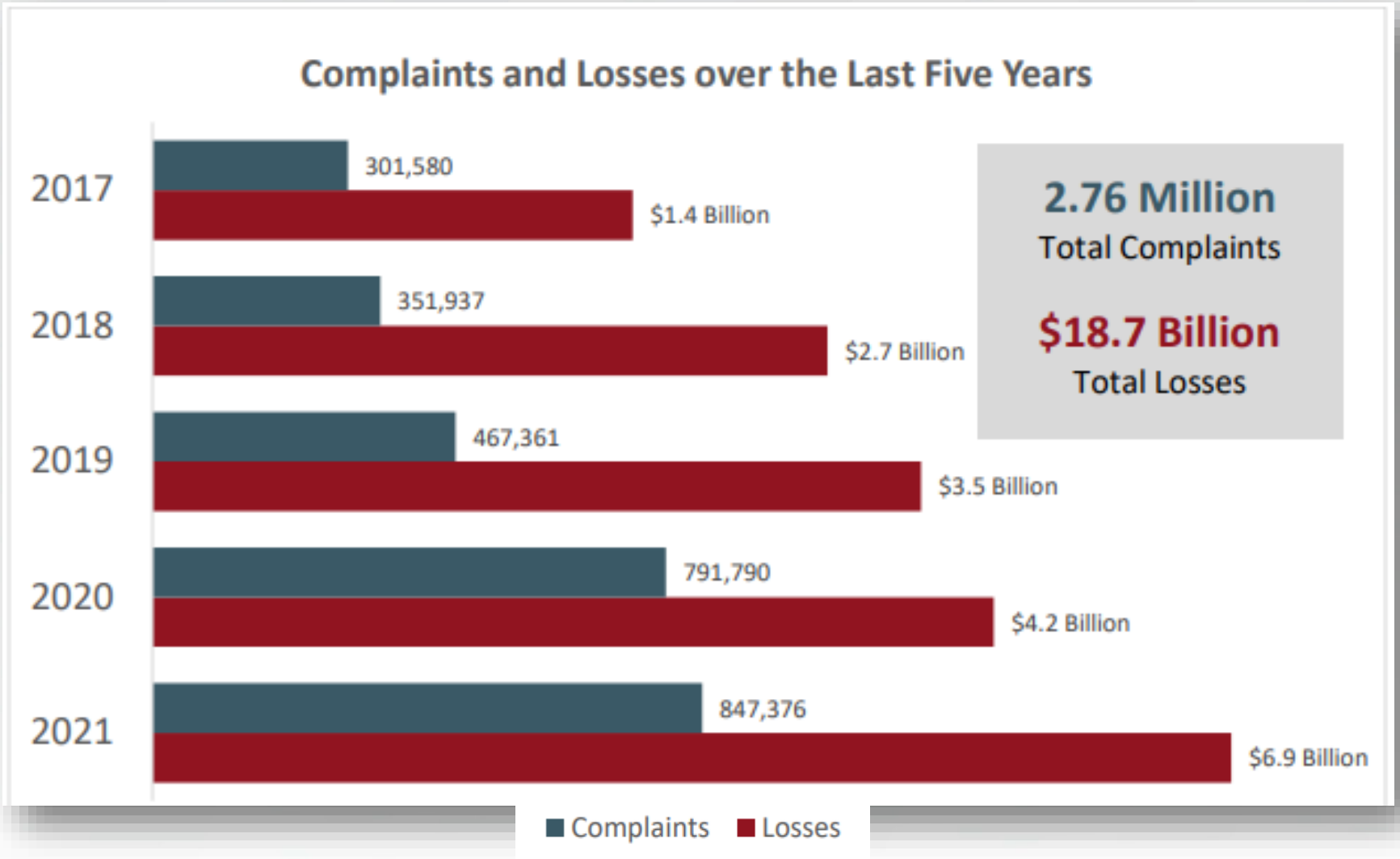
2022 Verizon DBI Report

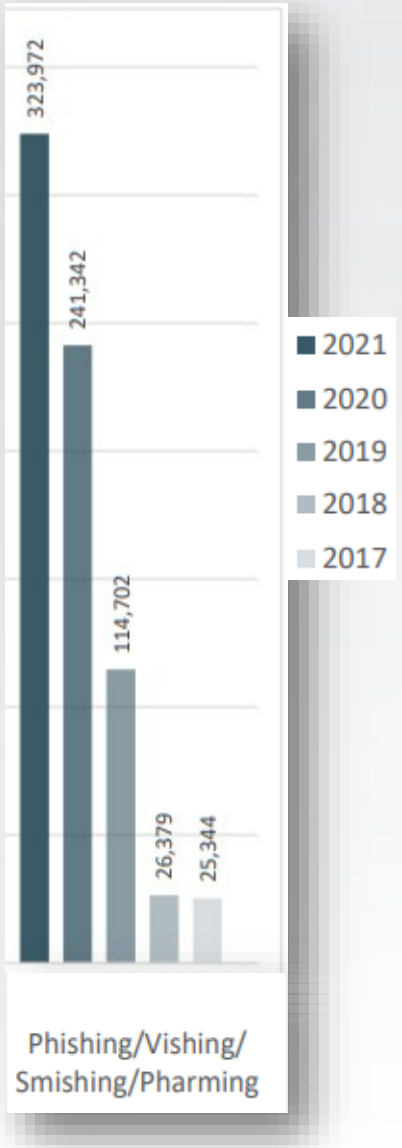
- **Ransomware-related breaches increased by 13%,** *(more than the past five years combined)*
- Nearly 50% of all system intrusion *incidents* involved ransomware last year
  - Ransomware was present in almost 70% of malware breaches in the past year
- **Supply chain was involved in 62% of incidents** 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/

FORVIS

FBI's IC3 Five Year Statistics





FORV/S

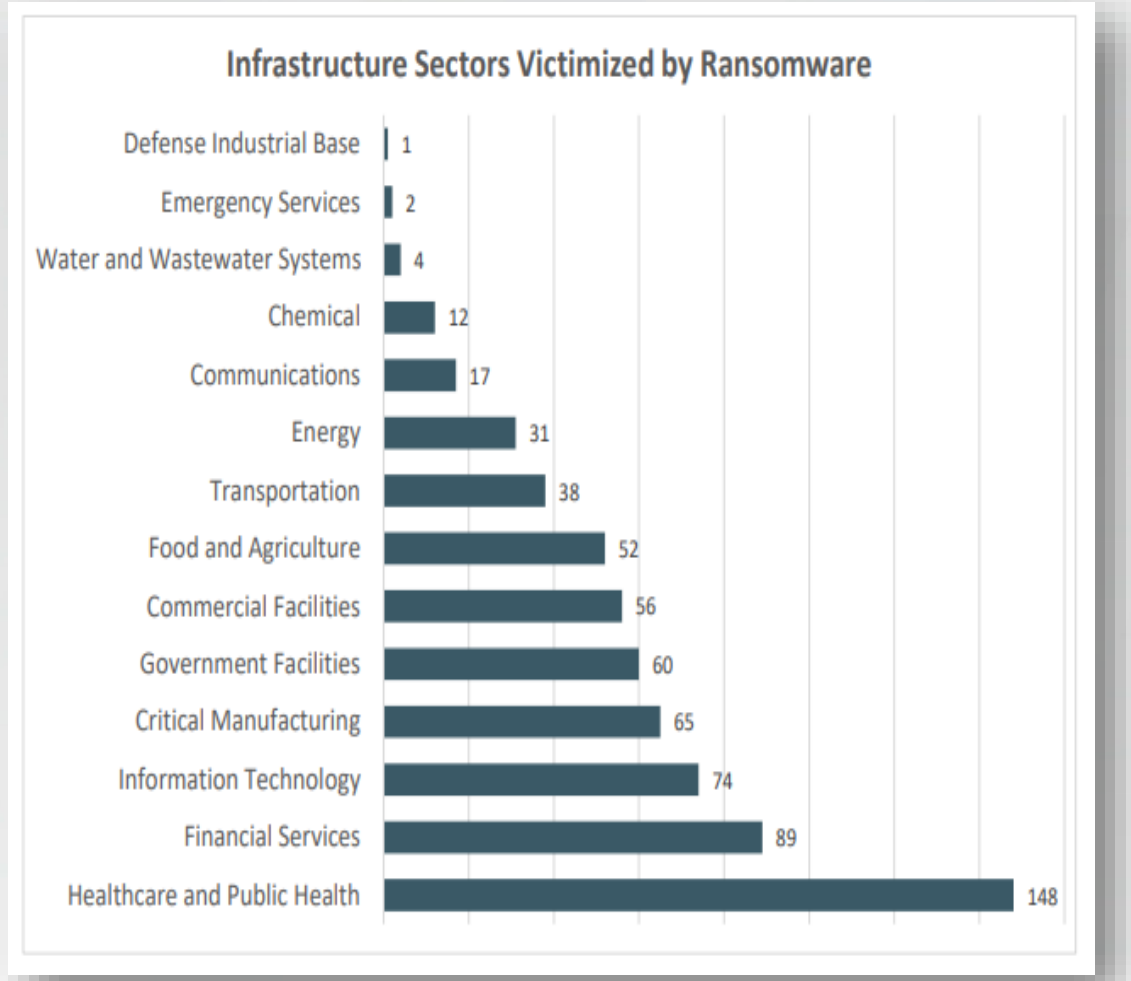
IC3 – Ransomware and BEC Fast Facts

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

For 2021, the FBI's Internet Crime Complaint Center (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"

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 have cost businesses around the world $43 billion during the period between June 2016 and December 2021.



*https://www.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf

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**

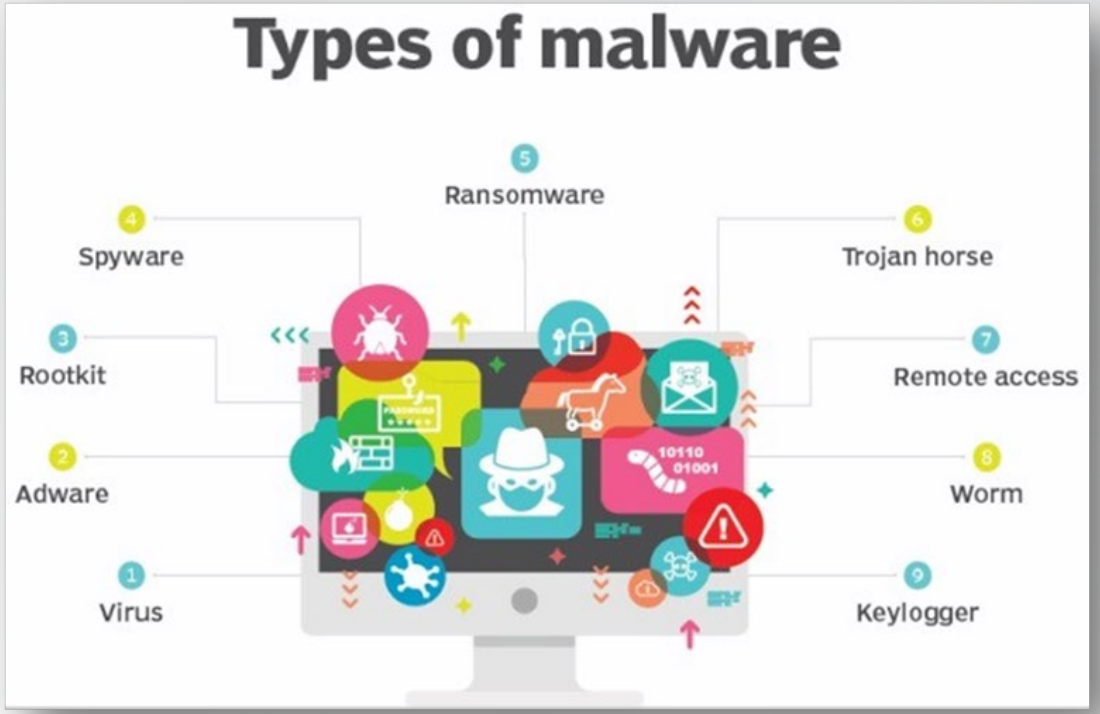
Companies with an incident response team & extensive testing of their response plans saved over $2 million compared to those who did not.

Source: Ponemon Institute 2022 Cost of Data Breach Study

FORVIS

Most Common Cybersecurity Threats

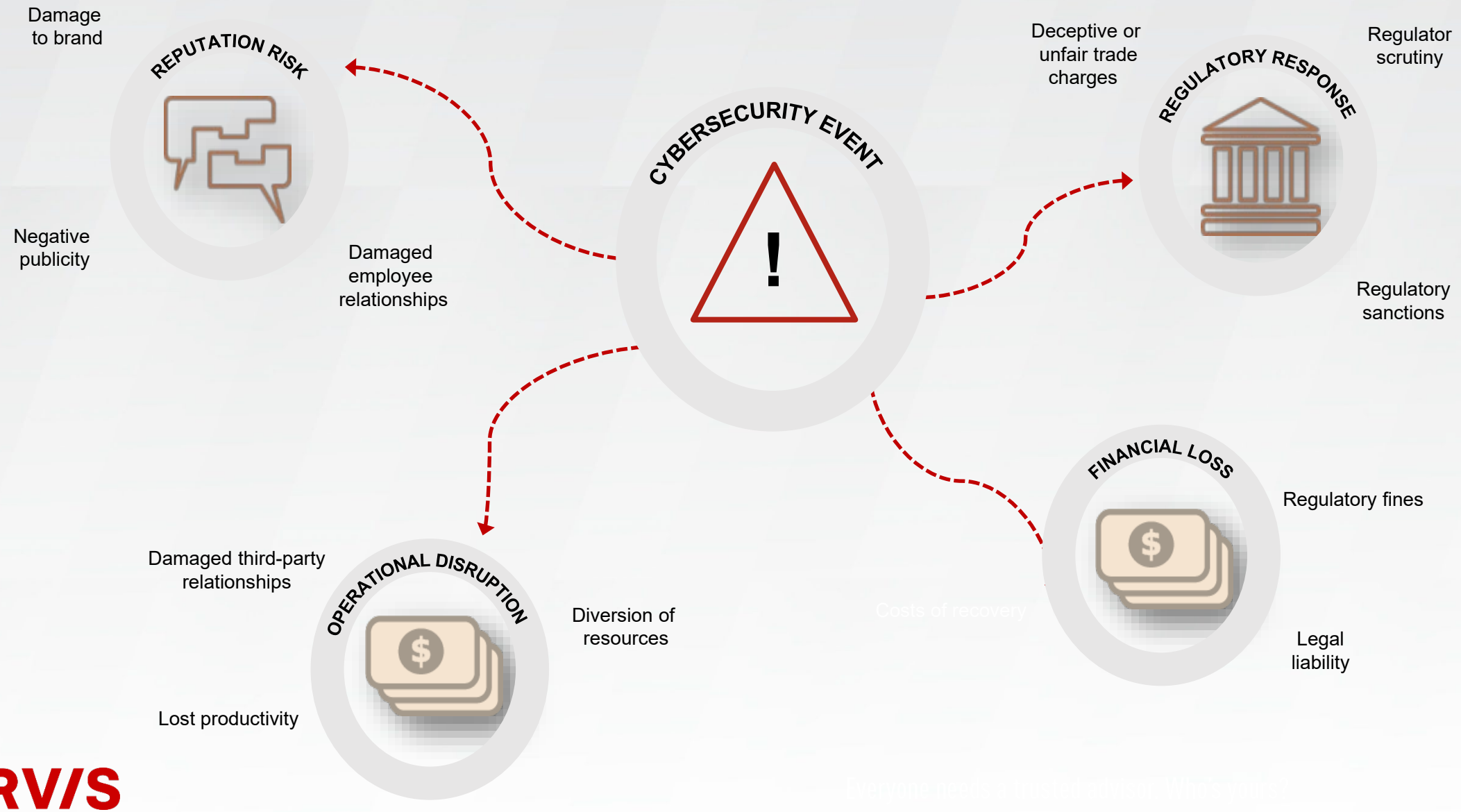
- Social engineering attacks – phishing
- Malware/destructive malware
  - *Ransomware*
  - Remote access
  - Keyloggers
- Business email compromise
- Corporate account takeovers
- Supply chain!



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

FORV/S

Breach Impacts



FORVIS

Why is Your Sector a Target?

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

A Few Prime Examples: Atlanta, GA; Baltimore, Maryland; St. Lucie, Florida; New Orleans, Louisiana; and Greenville, North Carolina

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

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, & IT control audits

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
- **Tune existing security tools** – web content, email filtering, end point, etc.
- Deploy **cloud-based security** software & end-point protection (SentinelOne, Crowdstrike, Windows Defender, etc.)

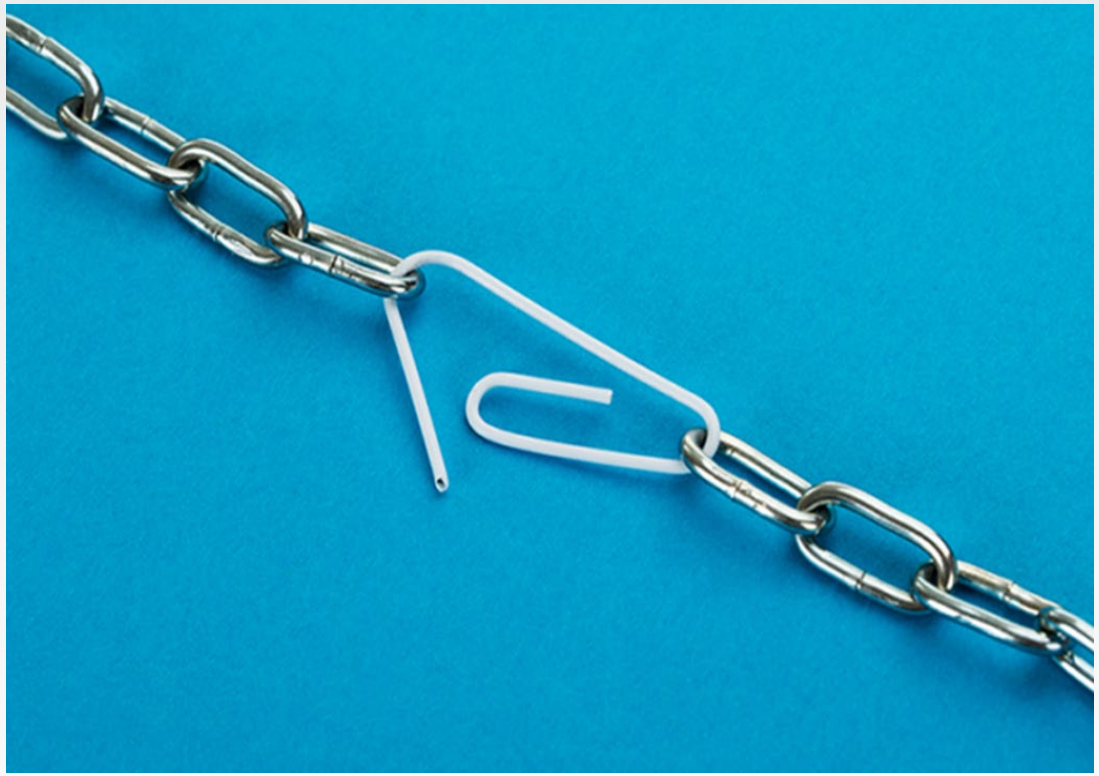
FORVIS

Key Considerations: Technical Controls

- Implement strong cloud-based **data loss prevention** controls
- Use **security information & event management (SIEM)** tools with **“defense in depth”** approach
- **Change** your passwords more frequently during this time
- 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**!

FORV/S

What Cybercriminals See, if You Fail!



FORVIS

Final Thoughts & Conclusion

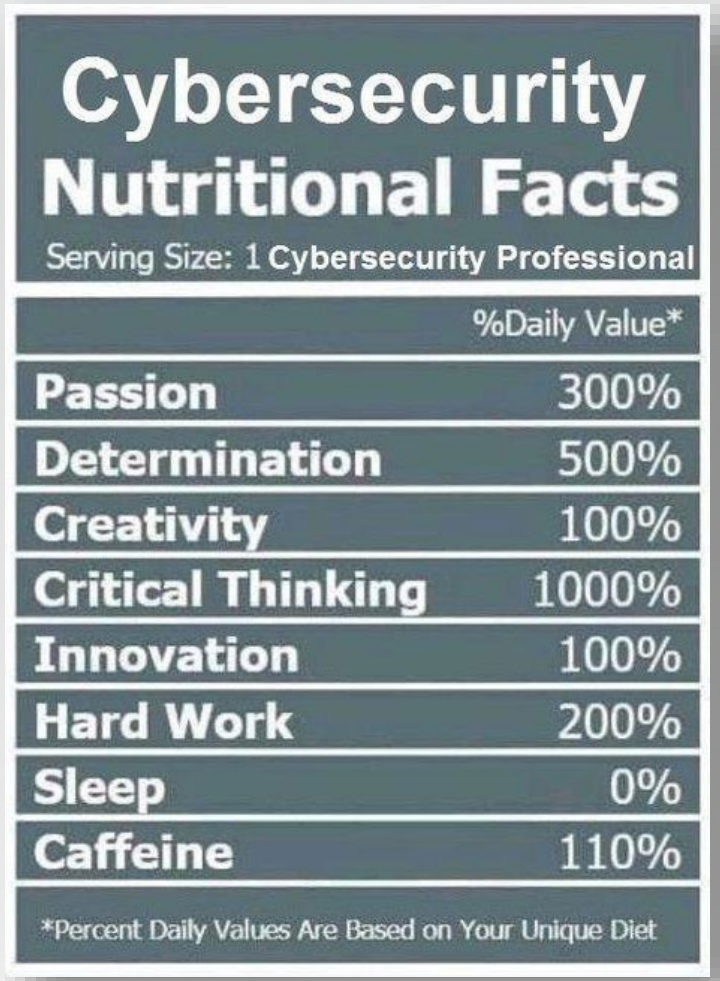
FORVIS

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

Cybersecurity Nutrition



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

Are you taking care of your “cybersecurity health”?

FORVIS

The Wrong Mentality

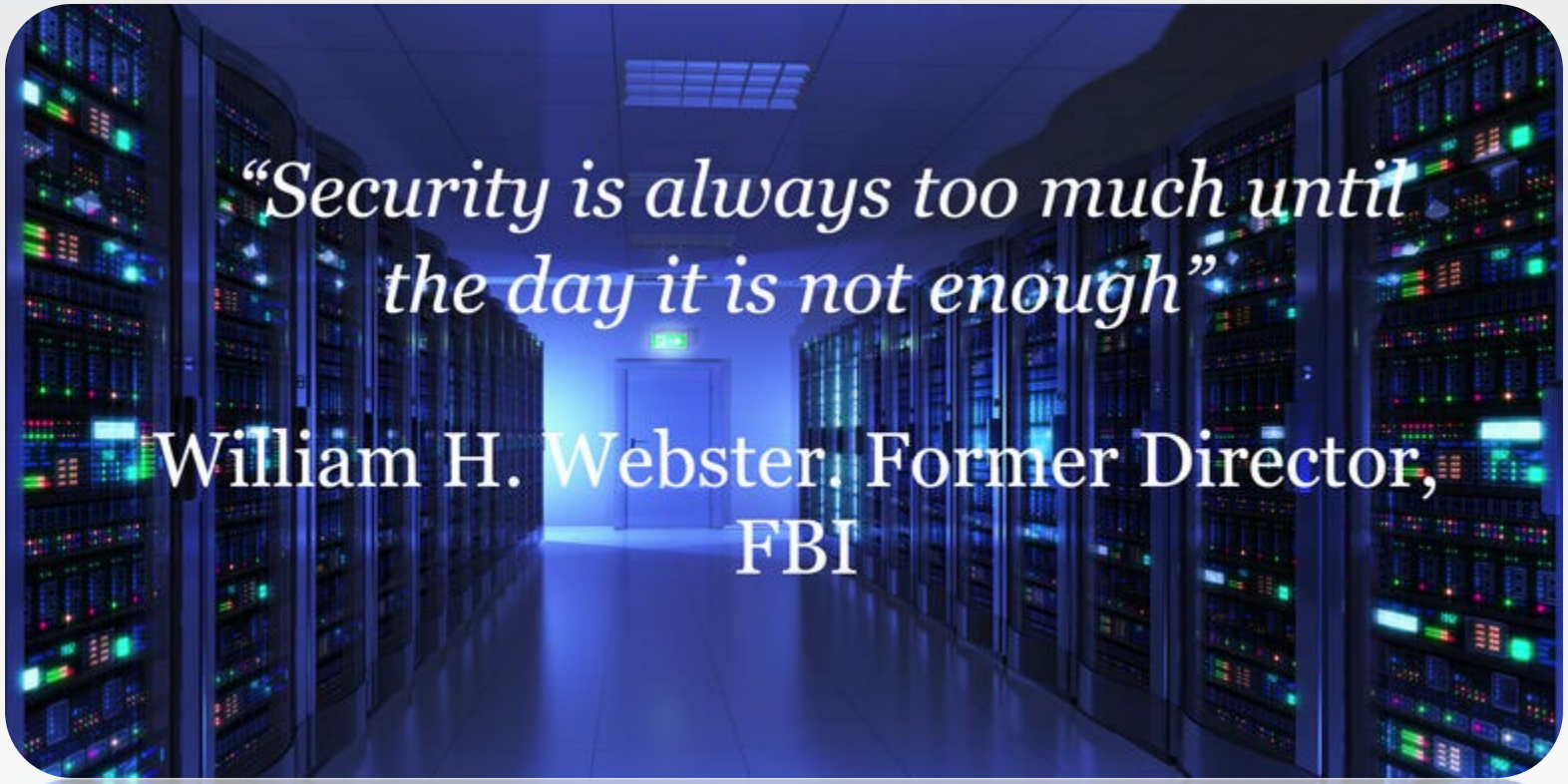
Quote by Colonial CEO, **“Paying the ransom was the right thing to do for the country.”**

Quote by JBS CEO, **“It was very painful to pay the criminals, but we did the right thing for our customers.”**

Wait, WHAT??

FORV/S

A Quote to Remember!



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

Thank you!

forvis.com

FORVIS

Assurance / Tax / Advisory