

**SEE YOURSELF
IN CYBER**



**CYBERSECURITY
AWARENESS
MONTH 2022**

Jason Burt
Cybersecurity Advisor, Region 4
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency



**CYBERSECURITY
AWARENESS
MONTH 2022**

Divisions of CISA

**KNOW YOUR
CYBER BASICS**

**CYBERSECURITY
DIVISION**



**INTEGRATED
OPERATIONS
DIVISION**



**INFRASTRUCTURE
SECURITY
DIVISION**



**NATIONAL RISK
MANAGEMENT
CENTER**



**EMERGENCY
COMMUNICATIONS
DIVISION**



**STAKEHOLDER
ENGAGEMENT
DIVISION**



CISA Mission and Vision

MISSION:

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

VISION:

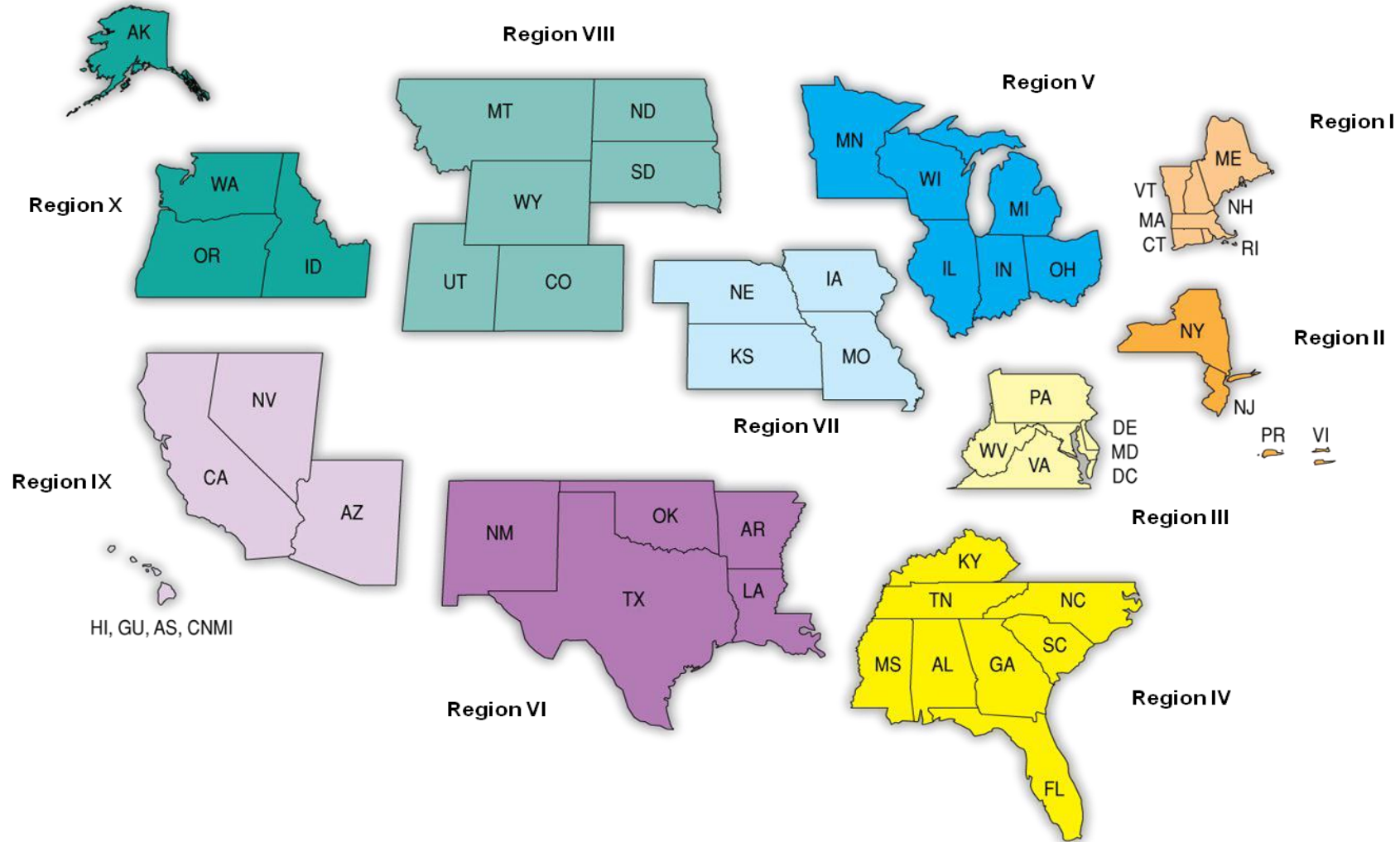
Secure and resilient infrastructure for the American people.



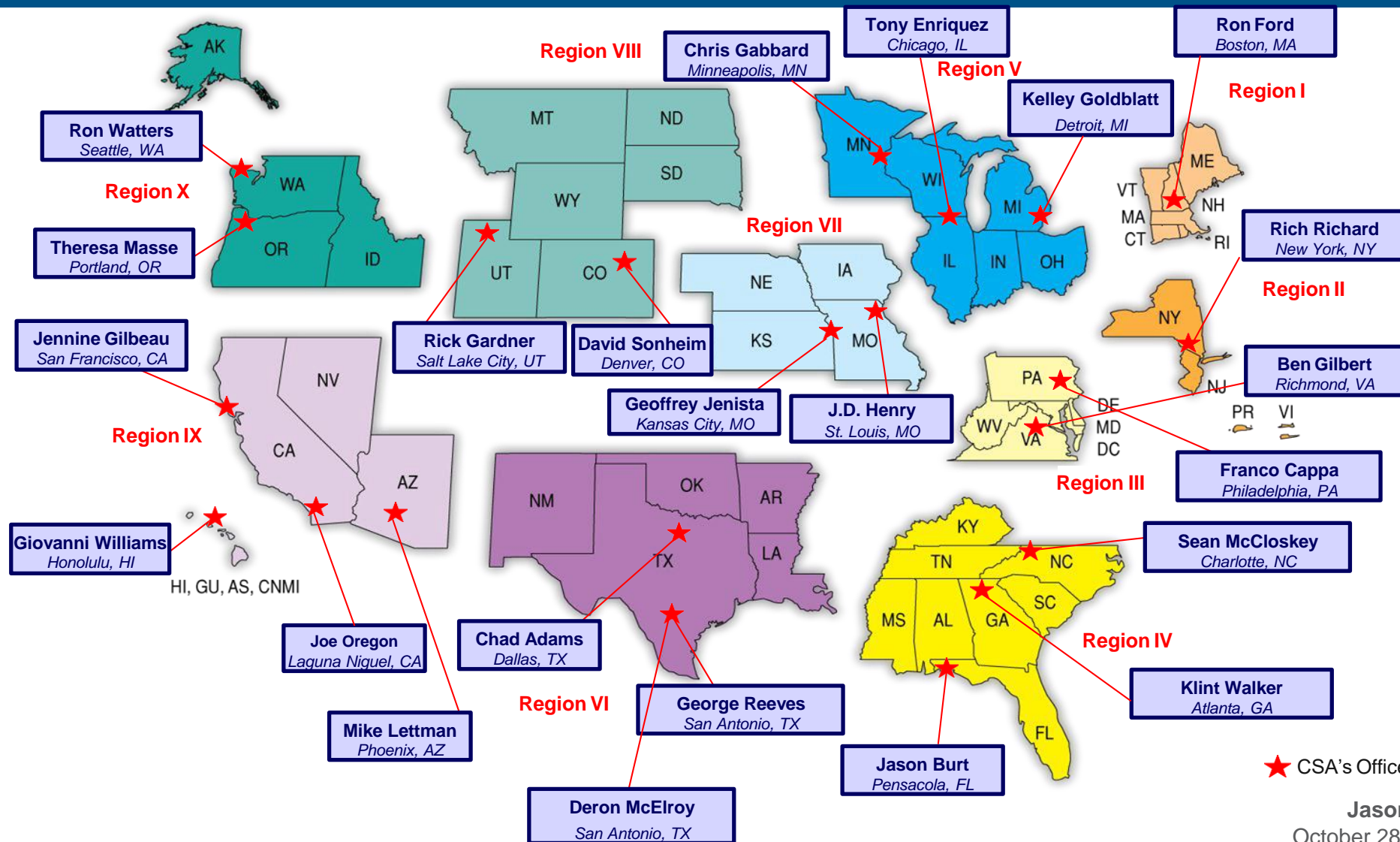
CYBERSECURITY ADVISOR PROGRAM



CSA Regionally Deployed Personnel

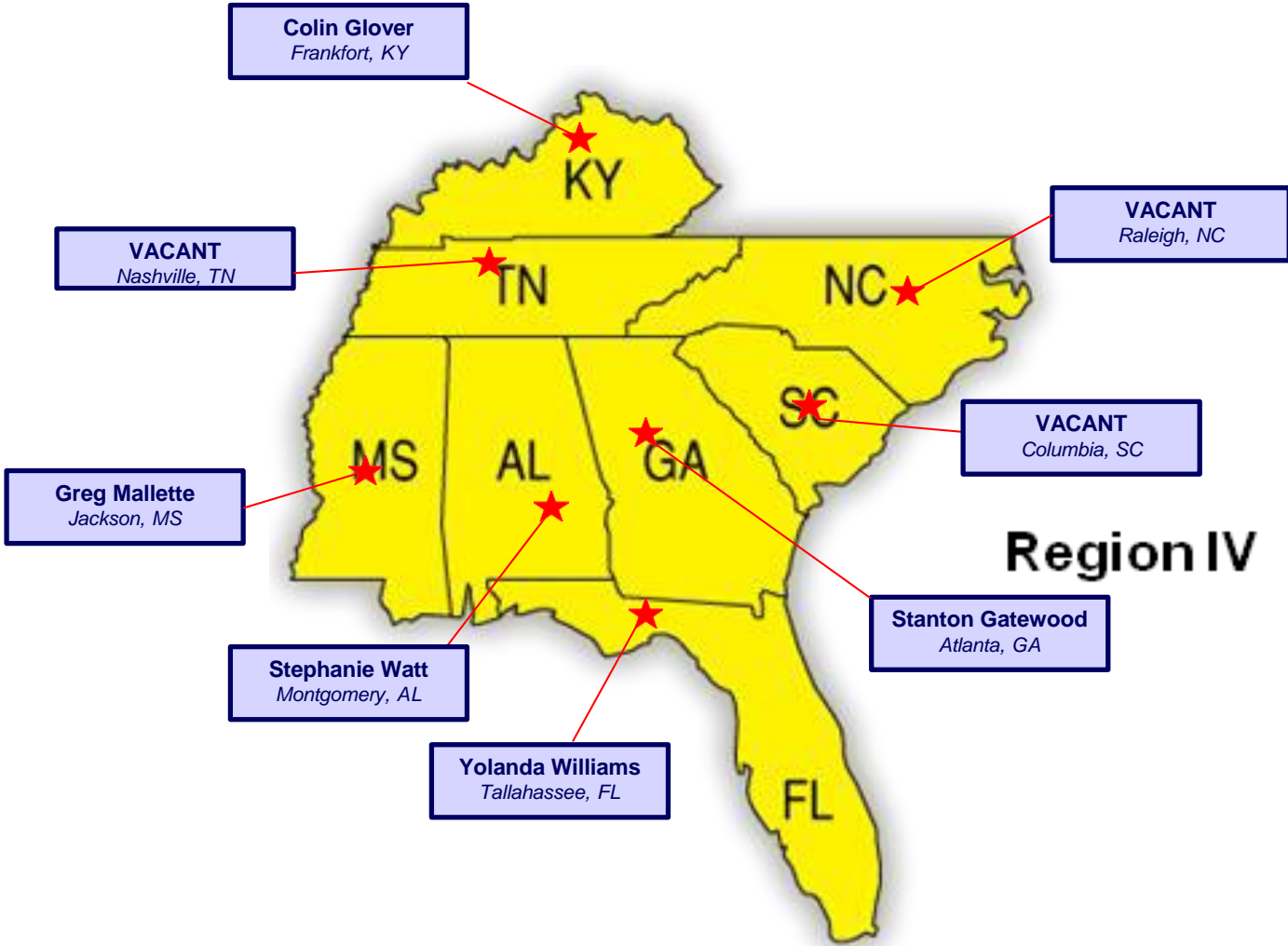


CSA Regionally Deployed Personnel

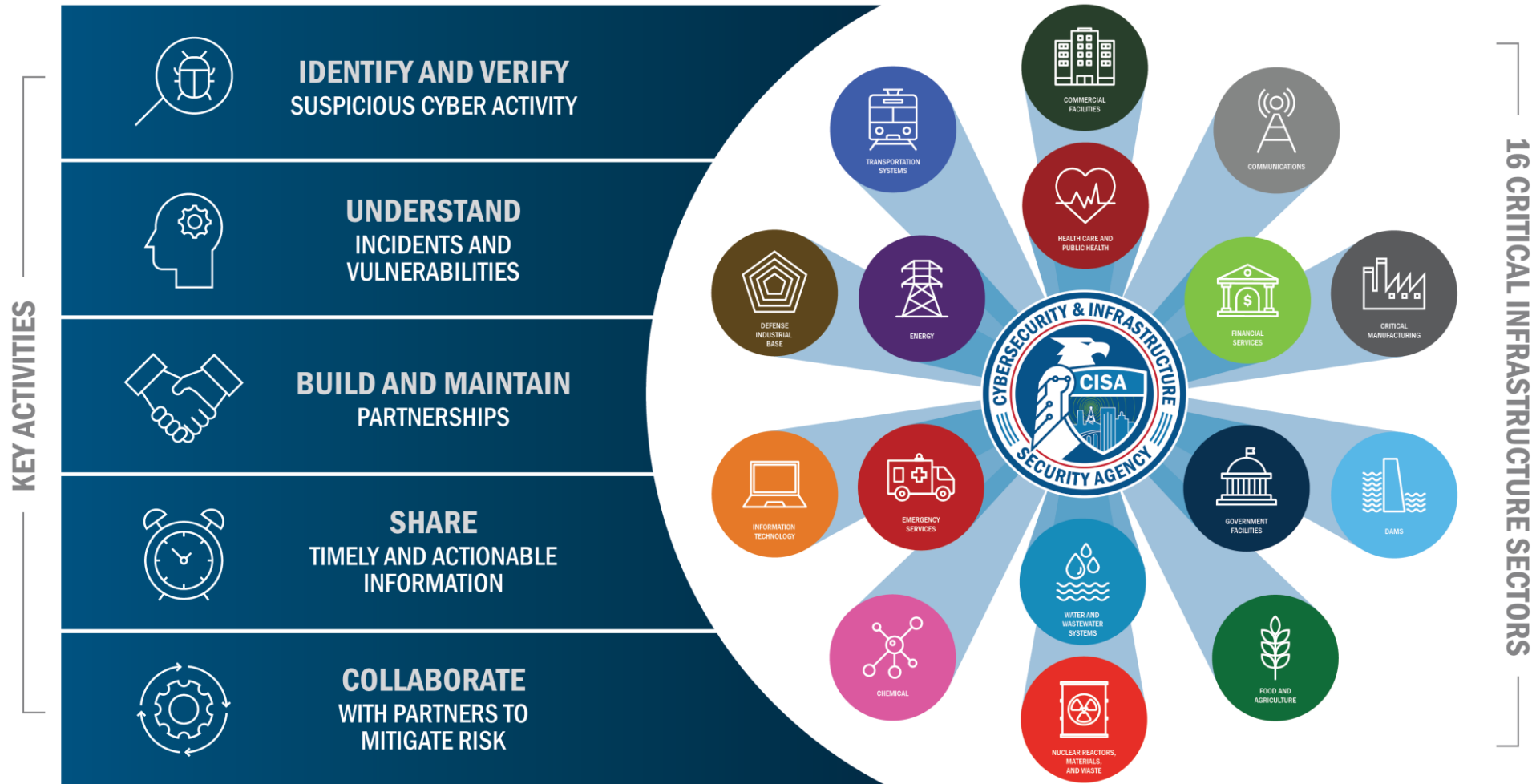


Jason Burt
October 28, 2022

Region 4 Cybersecurity State Coordinators



Serving Critical Infrastructure



Today's Risk Landscape

America remains at risk from a variety of threats:



ACTS OF TERRORISM



CYBER ATTACKS



EXTREME WEATHER



PANDEMICS



ACCIDENTS
OR TECHNICAL
FAILURES

Cyber Threats of Today

Ransomware

- WannaCry
- REvil/Sodinokibi (targeting MSPs)
- Ryuk (targeting medical, education, SLTT)
- Conti, Robinhood, Maze, Fobos, CovidLock, CryptoLocker, Pysa, VoidCrypt...

Malware

- Remote Access Trojans or RATs: **Trickbot**, Emotet, LokiBot, IcedID, BazarLoader
- Wiperware NotPetya
- ICS/OT specific: Triton/hatman malware targets Safety Instrumented Systems (SIS)

Advanced Persistent Threats (APTs)

- Energetic Bear/Berserk Bear (targets U.S. state, local, territorial, and tribal (SLTT) government networks, as well as aviation networks)

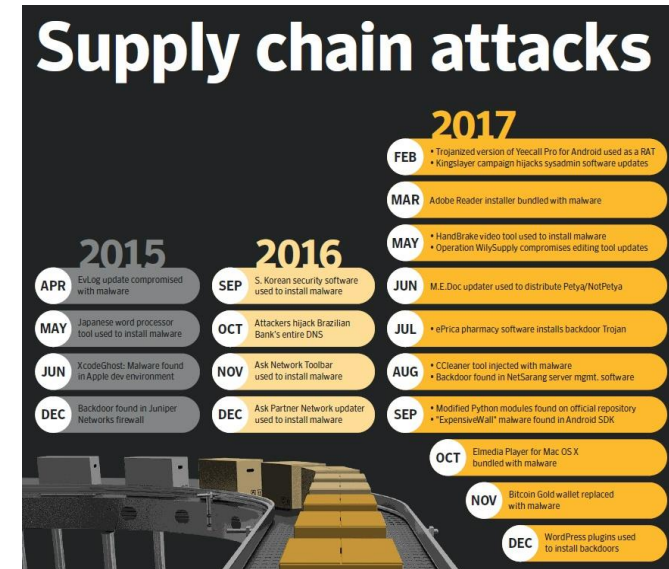
Threats to External Dependencies

- 3rd party vendors, service providers, infrastructure providers
- Supply chain Compromise



SUPPLY CHAIN ATTACKS

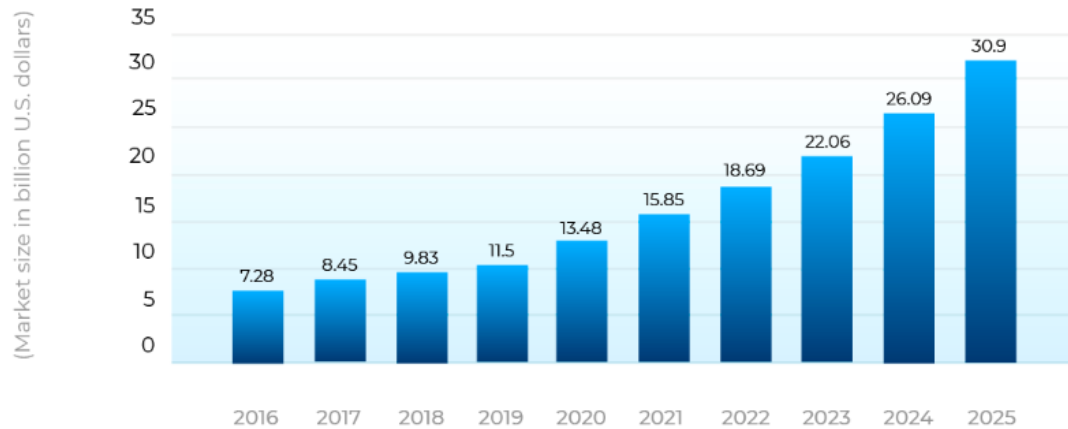
- **Cyber Supply Chain Compromise:** Manipulation of devices or software, or their delivery mechanisms before receipt by the end customer with the goal of data or system compromise of target environment. (T08620)
- **Target becomes the Target:** 2013 Point of Sale system compromised via Fazio HVAC supplier to place malware on POS devices.
Result: 40 Million Card details & \$18.5 million
- **MeDoc Ukrainian Tax Software Compromise:** The Source or 2016 *Petya* and later *NotPetya*
Result: More than \$10 Billion (Merck, Maersk)
- **CCCleaner:** Popular registry clean-up Software 2017 Avast is compromised, poisoned updates
Result: 2.3 million infected downloads
- **Dragonfly Compromise:** 3 ICS equipment providers targeted, and malware was inserted into software bundles – Energy Sector Target
Result: Espionage / Reconnaissance
Result 2: Dragonfly 2.0 – More Disruptive Phase



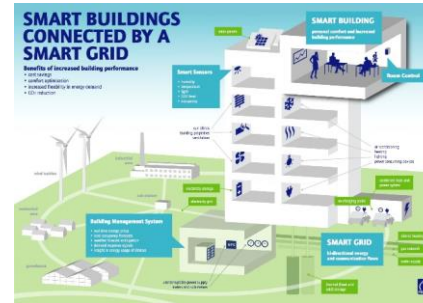
Securing the Internet of Things

- 40B Connected IoT Devices by 2025
- Data: 17.3 ZB in 2019 / 73.1 ZB in 2025
- Healthcare: 82% of attacks focused on IoT

(in billion U.S. dollars)

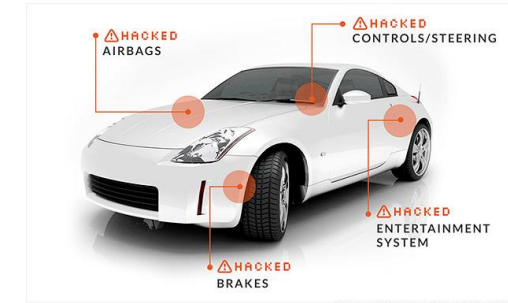


Our buildings



Our Production

Our transport



Our health

Beyond the Headlines: What is Ransomware?

Ransomware 101

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.

Malicious actors then demand ransom in exchange for decryption.



BUSINESS
CNA website back up two weeks after insurance giant hit with 'sophisticated ransomware attack'
By ROBERT CHANNICK
CHICAGO TRIBUNE | APR 05, 2021 AT 11:18 AM



Ransomware suspected in cyberattack that crippled major US newspapers
Source inside Tribune Publishing says printing outage caused by Ryuk ransomware infection.

Jason Burt
October 28, 2022

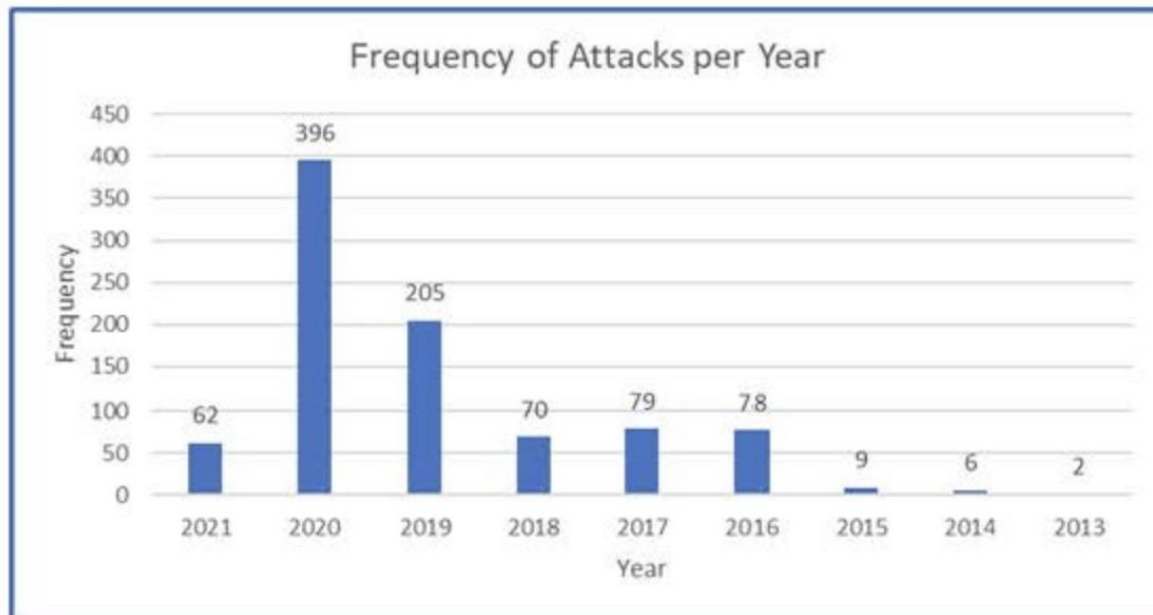
Infects...Encrypts...Extorts

- Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.
- Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.
- The monetary value of ransom demands has also increased, with demands for millions of dollars becoming commonplace.
- Ransomware incidents have become more destructive and impactful in nature and scope.



Ransomware Attacks on CI on the Rise

Attacks on Critical Infrastructure have Risen Dramatically in the Last Two Years



Top 5 Most Targeted Critical Infrastructure Sectors*

Critical Infrastructure Sector	Frequency
Government Facilities	241
Healthcare and Public Health	157
Education Facilities Subsector	135
Information Technology	74
Critical Manufacturing	68

*November 2013 – March 2021

According to Data from Temple University
“Critical Infrastructure Ransomware Incident Dataset”

Why Target CI?

Follow the Money

*“Cybercriminals are becoming more savvy. **They know who has money.** The folks who operate inside those critical infrastructure sectors are no longer immune.”*

– Brandon Wales, CISA Acting Director

According to recent Palo Alto Networks study:



The average ransom paid for organizations increased from \$115,123 in 2019 to **\$312,493** in 2020 → a 171% year-over-year increase.



The highest ransom paid by an organization **quadrupled** from 2020 to 2021, from \$10 million to \$40 million, when CNA Insurance was the victim of a ransomware attack in March 2021.



From 2015 to 2019, the highest ransomware demand was \$15 million. In 2020, the highest ransomware demand was **\$30 million**.

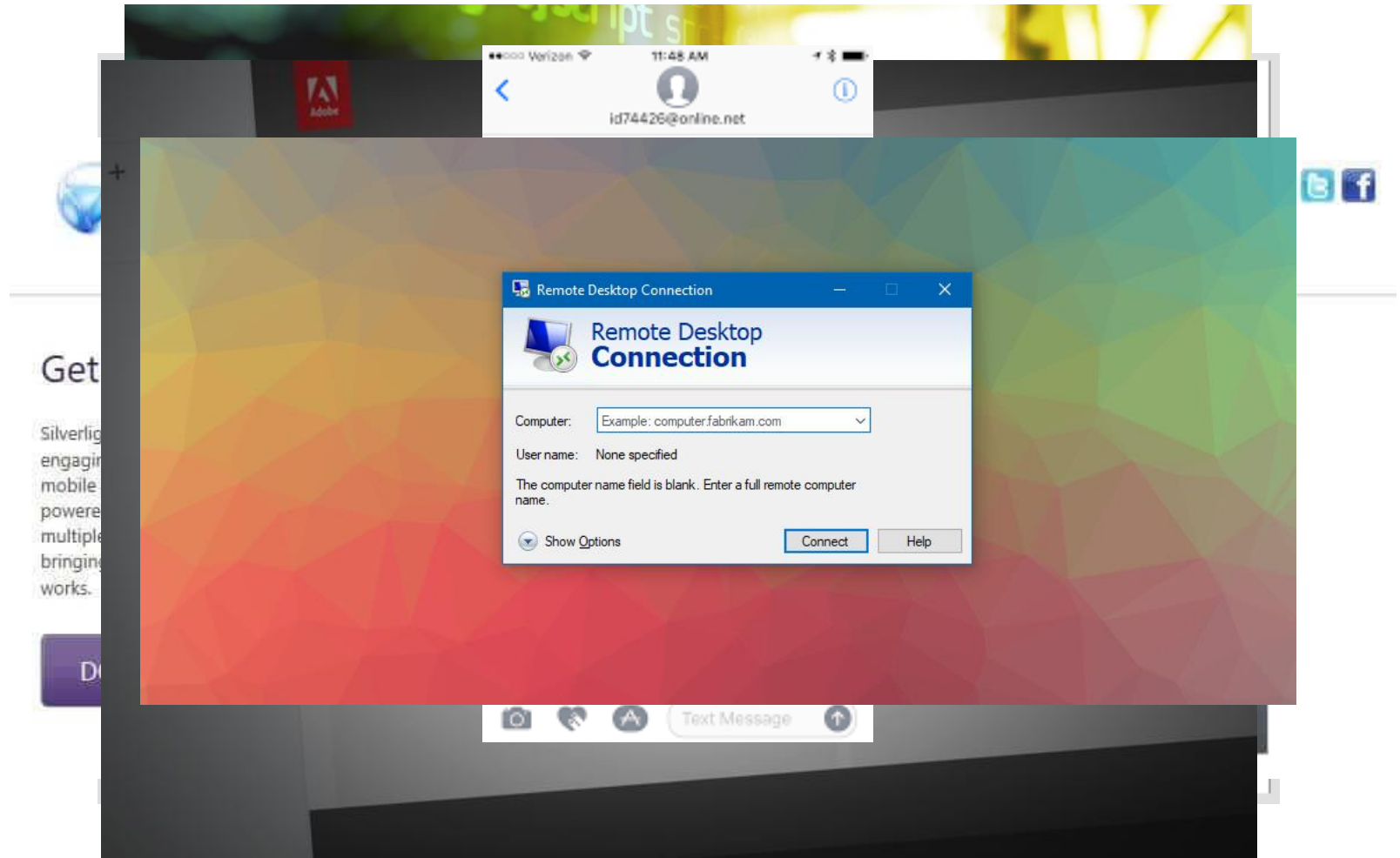
In 2021, REvil demanded more than \$70 million in its ransomware attack on Kaseya, its customers, and downstream customers in July 2021.



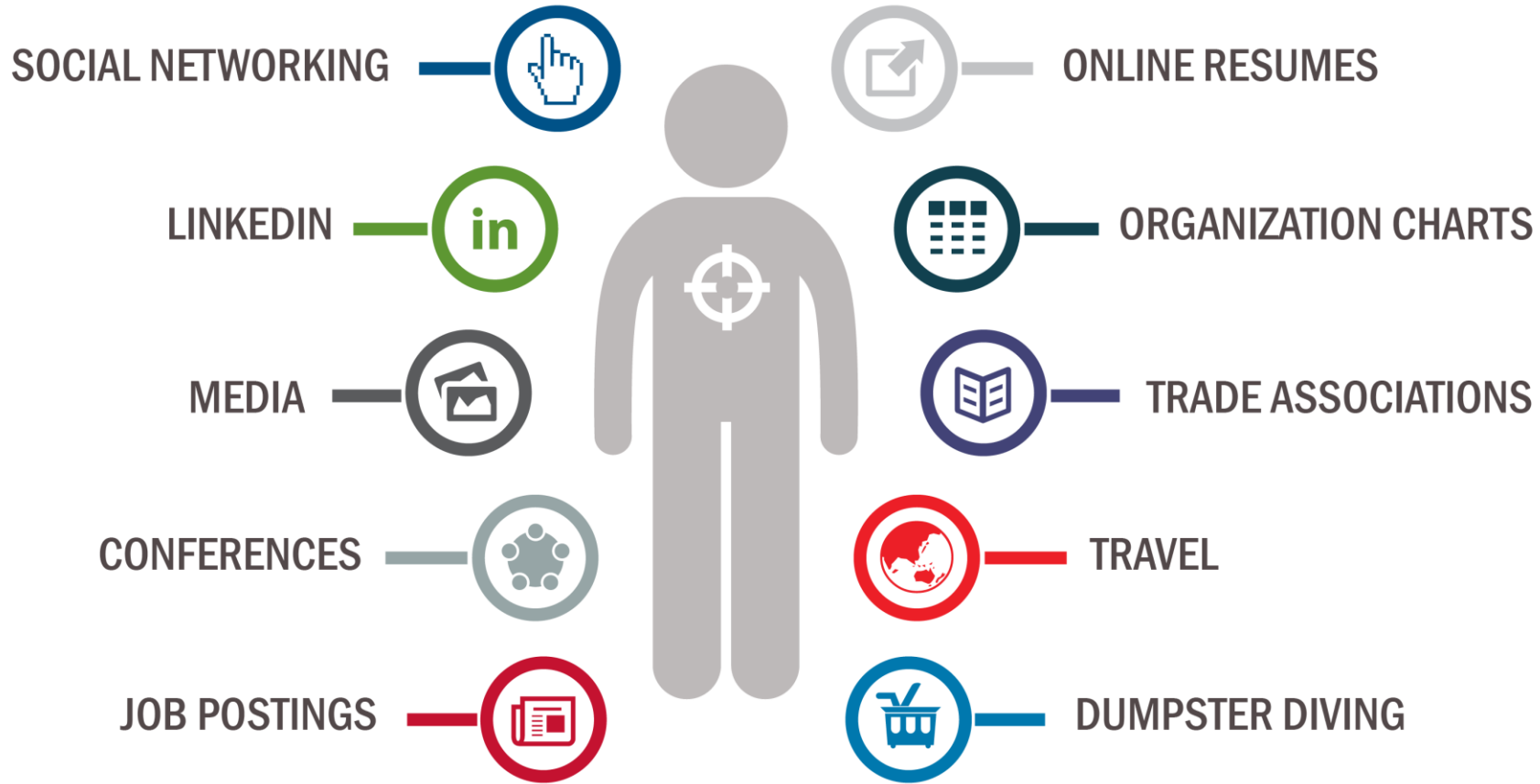
Methods of Infection

The following can all be vectors of infection for ransomware attacks:

- Phishing
- Compromised Websites
- Malvertising
- Exploit Kits
- Downloads
- Messaging Applications
- Brute Force via RDP



HOW ARE YOU TARGETED?



Theme

The 2022 Campaign theme, See Yourself in Cyber, emphasizes that while cybersecurity may seem like a complex subject, ultimately, it's really all about people. This October, we will focus on the “people” part of cybersecurity, providing information and resources to help Americans make smart decisions on the job, at home, at school, and in the future.



Action Steps



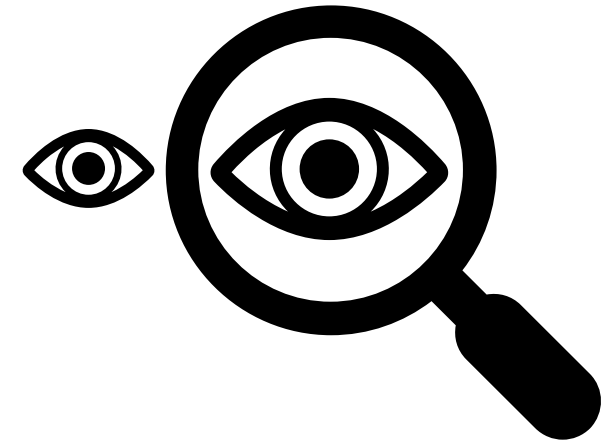
This year's campaign goal is to have everyone implement these four action steps to increase online security:

- **Enable Multi-Factor Authentication:** You need more than a password to protect your online accounts, and enabling MFA makes you significantly less likely to get hacked.
- **Use Strong Passwords:** Use passwords that are long, unique, and randomly generated.
- **Recognize and Report Phishing:** If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Update Your Software:** Don't delay – if you see a software updated notification, act promptly. Better yet, turn on automatic updates.








How to Protect Against Spam and Phishing

- **Be suspicious** of emails from unknown senders.
- **Do not** provide personal or corporate sensitive information requested via email.
- **Do not** use the contact information provided by the email or phone request. Contact the organization directly to verify.
- **Do not** send personal sensitive information on the internet without checking the security of the websites first.



How to Stay Safe Online

- **Use** strong passwords and multi-factor authentication, if available. 
- **Keep** the software on your devices up to date. 
 - Enable automatic updates
- **Check** privacy policies and security setting to see how your information is stored and shared. 
- Shop online with **trusted and reputable** companies. 
- **Don't** download attachments or click links that you are unsure of. 



How to Stay Safe Online

- **Avoid** connecting to public Wi-Fi



- Public Wi-Fi is typically not secure.
- If connected, do not conduct activities involving sensitive information.

- **Credit cards** > Debit cards

- Credit cards provide more protections when it comes to fraudulent activity.

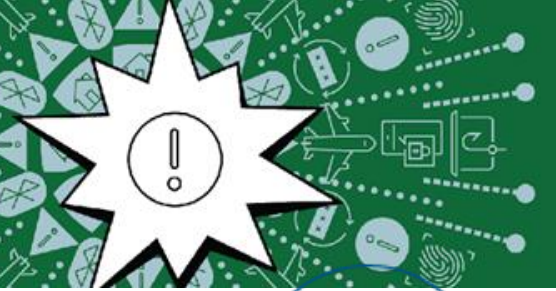


- **Be wary** of emails requesting personal information

- Organizations typically do not request this information via email.



How to Report Victims of Online Crime



If you or a child is a victim of online crime

1. Notify your local authorities and file a complaint with the Internet Crime Complaint Center at www.ic3.gov.
2. If you think a site has collected or marketed information from or to your kids in a way that violates the law, report it to the FTC at www.ftc.gov/complaint.
3. If someone has had inappropriate contact with your child, or a child you know, report it to www.cybertipline.com and the police.



Keeping Your Kids Safe Online



Take an active role in protecting your children

- ❖ Be involved, be present when your kids use connected devices.
- ❖ Supervision is very important for children of all ages.
- ❖ Set rules and create parental controls with strong passwords that enforce the rules when not able to supervise kids closely.
- ❖ Monitor computer and smart phone activity.
- ❖ Children should have separate accounts on shared computers and mobile devices when possible.



Resources

[Cyber Hygiene Services](https://www.cisa.gov/cyber-hygiene-services)

<https://www.cisa.gov/cyber-hygiene-services>

[CISA Shields Up](https://www.cisa.gov/shields-up)

<https://www.cisa.gov/shields-up>

[Cyber Resource Hub](https://www.cisa.gov/cyber-resource-hub)

<https://www.cisa.gov/cyber-resource-hub>

[Communications & Cyber Resiliency Toolkit](https://www.cisa.gov/communications-resiliency)

<https://www.cisa.gov/communications-resiliency>

[Cybersecurity Training & Exercises](https://www.cisa.gov/cybersecurity-training-exercises)

<https://www.cisa.gov/cybersecurity-training-exercises>



**CYBERSECURITY
AWARENESS**
MONTH 2022

Cybersecurity Services (Voluntary & No Cost)

Strategic

- **Cyber Resilience Review (Strategic)** -----
- **External Dependencies Management (Strategic)** -----
- **Cyber Infrastructure Survey (Strategic)** -----
- **Cybersecurity Evaluation Tool (Strategic/Technical)** -----

Tactical

- **Phishing Campaign Assessment (EVERYONE)** -----
- **Vulnerability Scanning / Hygiene (Technical)** -----
- **Web Application Scanning (Technical)** -----

**STRATEGIC
(C-Suite Level)**



**TECHNICAL
(Network/System Admin Level)**

Presenter's Name
August 4, 2022



**CYBERSECURITY
AWARENESS
MONTH 2022**

Questions & Contact Info



Contact Information

Jason Burt, CISSP

Region 4 Cybersecurity Advisor – **Florida, Alabama, Mississippi**

Jason.Burt@cisa.dhs.gov

(202) 578-9954 (Cell)

Yolanda Williams, CISSP

Region 4 Cybersecurity State Coordinator - **Florida**

Yolanda.Williams@cisa.dhs.gov

(202) 941-9687 (Cell)

Klint Walker, CISSP

Region 4 Cybersecurity Advisor - **Georgia, Tennessee, Kentucky**

Klint.Walker@hq.dhs.gov

(404) 895-1127 (Cell)



**CYBERSECURITY
AWARENESS
MONTH 2022**

Jason Burt
October 28, 2022



CYBERSECURITY AWARENESS MONTH 2022