CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CYBERSECURITY THREAT LANDSCAPE: MARITIME OPERATIONS

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

Divisions of CISA

- CISA consists of:

Cybersecurity Division

Infrastructure Security Division

Emergency Communications Division

National Risk Management Center

CISA Mission and Vision

Cybersecurity and Infrastructure Security Agency (CISA)

Mission:

- Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

Vision:

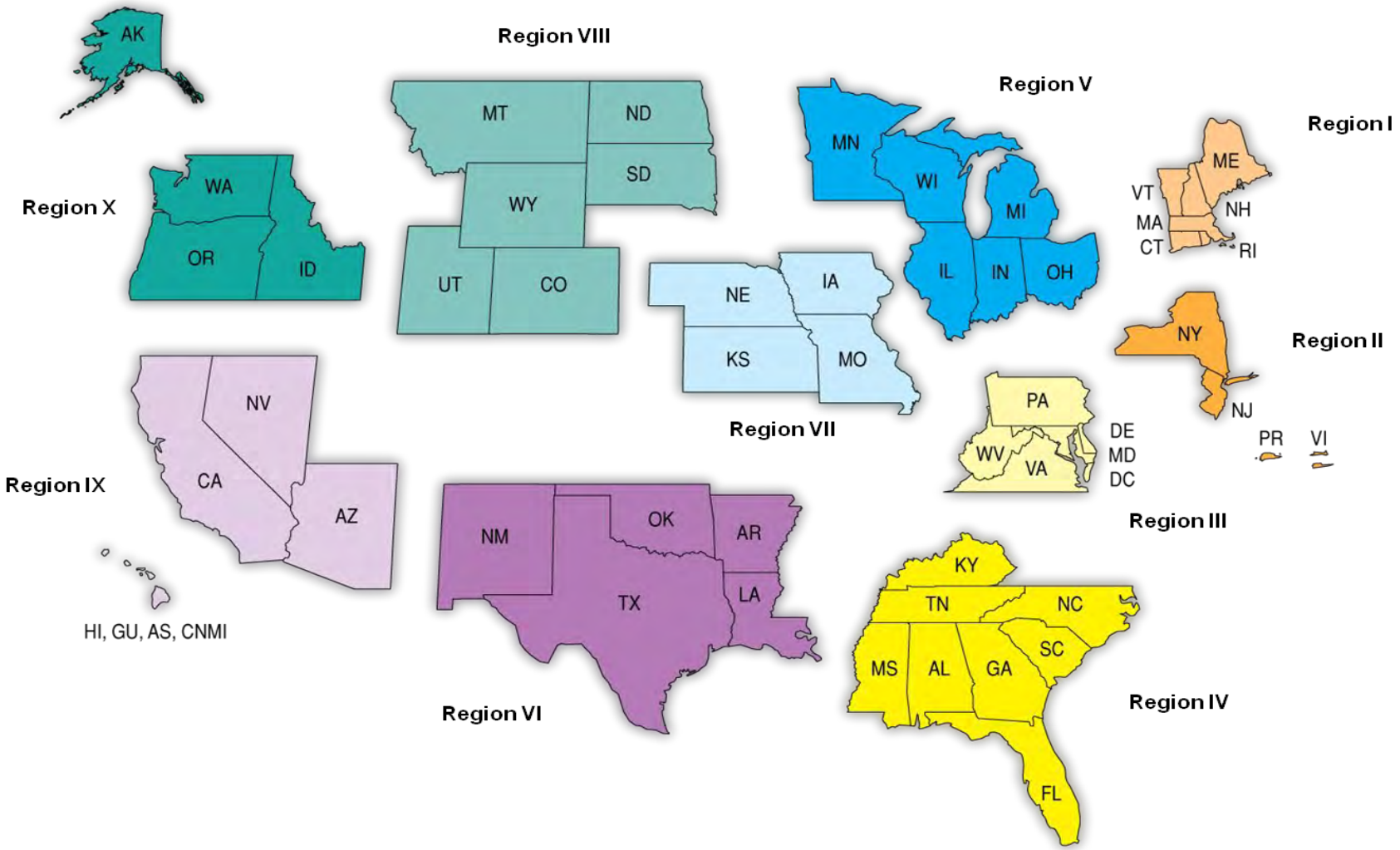
- A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive

Jason Burt
September 8, 2022

CYBERSECURITY ADVISOR PROGRAM

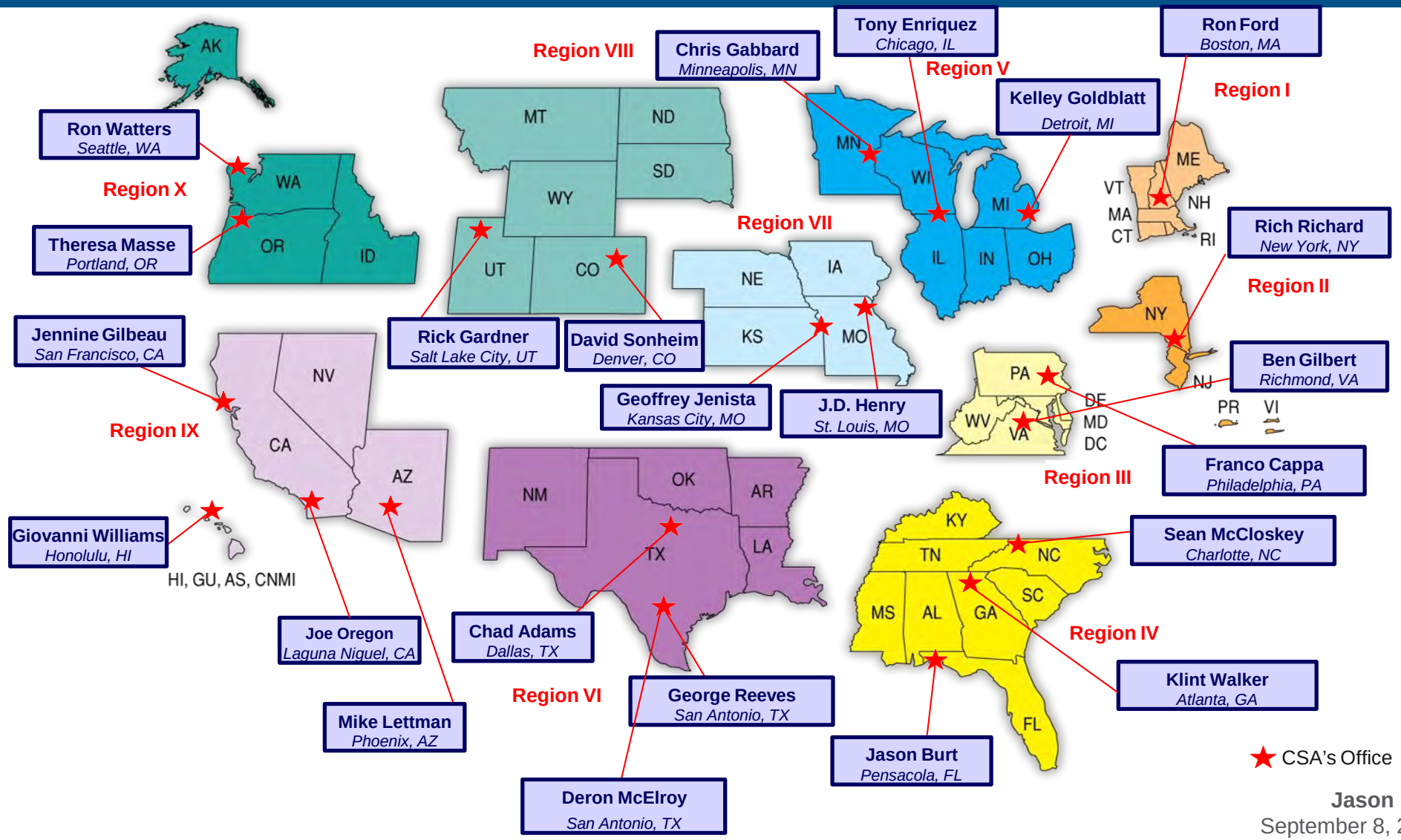
Jason Burt
September 8, 2022

CSA Regionally Deployed Personnel

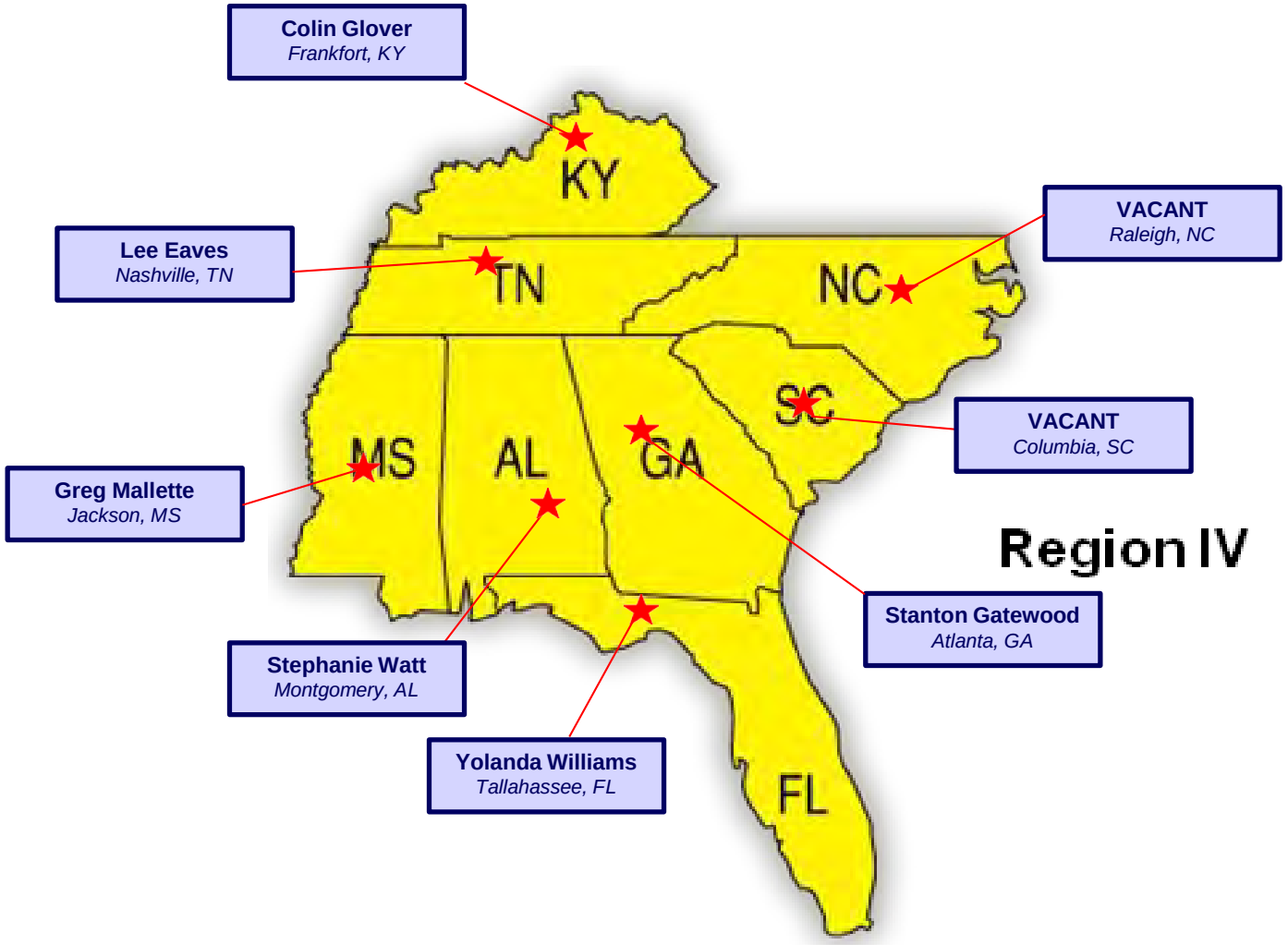


Jason Burt
September 8, 2022

CSA Regionally Deployed CSA's



Region 4 Cybersecurity State Coordinators



Jason Burt
September 8, 2022

Serving Critical Infrastructure

Jason Burt
September 8, 2022

Today's Risk Landscape

America remains at risk from a variety of threats:

PORT FACILITY

CYBERSECURITY RISKS

1. Facility Access
- Degrade or disrupt systems used to ID cargo and personnel

2. Terminal HQ – Data
- Access sensitive client & cargo info

3. Terminal HQ – Ransomware
- Manipulate or destroy data; disrupt ops

4. Operational Technology (OT) Systems
- Manipulate physical processes; cause physical damage and safety risks

5. Position, Navigation, and Timing (PNT)
- Disrupt vessel movements & cause collisions

6. Vessel Compromise
- Docked vessels via Wi-Fi; Networked Connections, and USB Devices

Jason Burt
September 8, 2022

MARITIME CYBER INCIDENTS

- 2020 - 900% Increase in Cyber attacks against Ships and Port Systems
- 2021 – 33% Increase in Cyber attacks against Ships and Port Systems
- Maritime and Logistics sectors typically share the least amount of incident-related Information

- June 2011 – Port of Antwerp (Belgium) – Drug Cartel installs Malware using Key Logger; Evidence of Prior Reconnaissance
- Jun 2017 – Port of Rotterdam (Netherlands) – Collateral Damage from Large-scale Malware (modified NotPetya Ransomware)
- 2018 – Port of Long Beach (U.S.) – Terminal for China Ocean Shipping Company hit with Ransomware
- 2018 – Port of Barcelona (Spain) – Internal IT Systems Contaminated
- 2018 – Port of San Diego (U.S.) – Highly sophisticated Cyber Attack
- March 2020 – Port of Marseilles (France) – Ransomware; Incidentally affected due to third party connection.

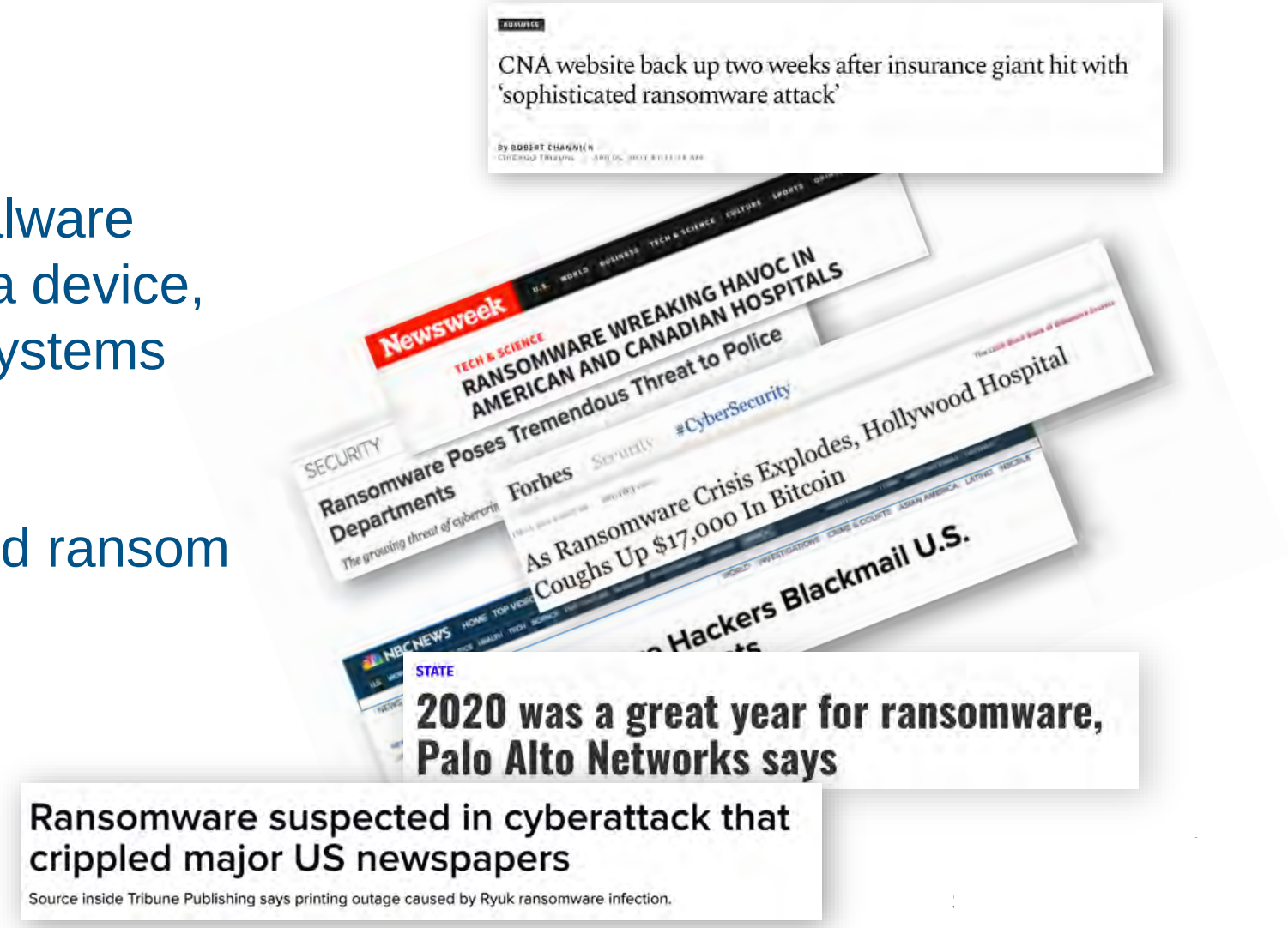
The Threat to Critical Infrastructure

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.



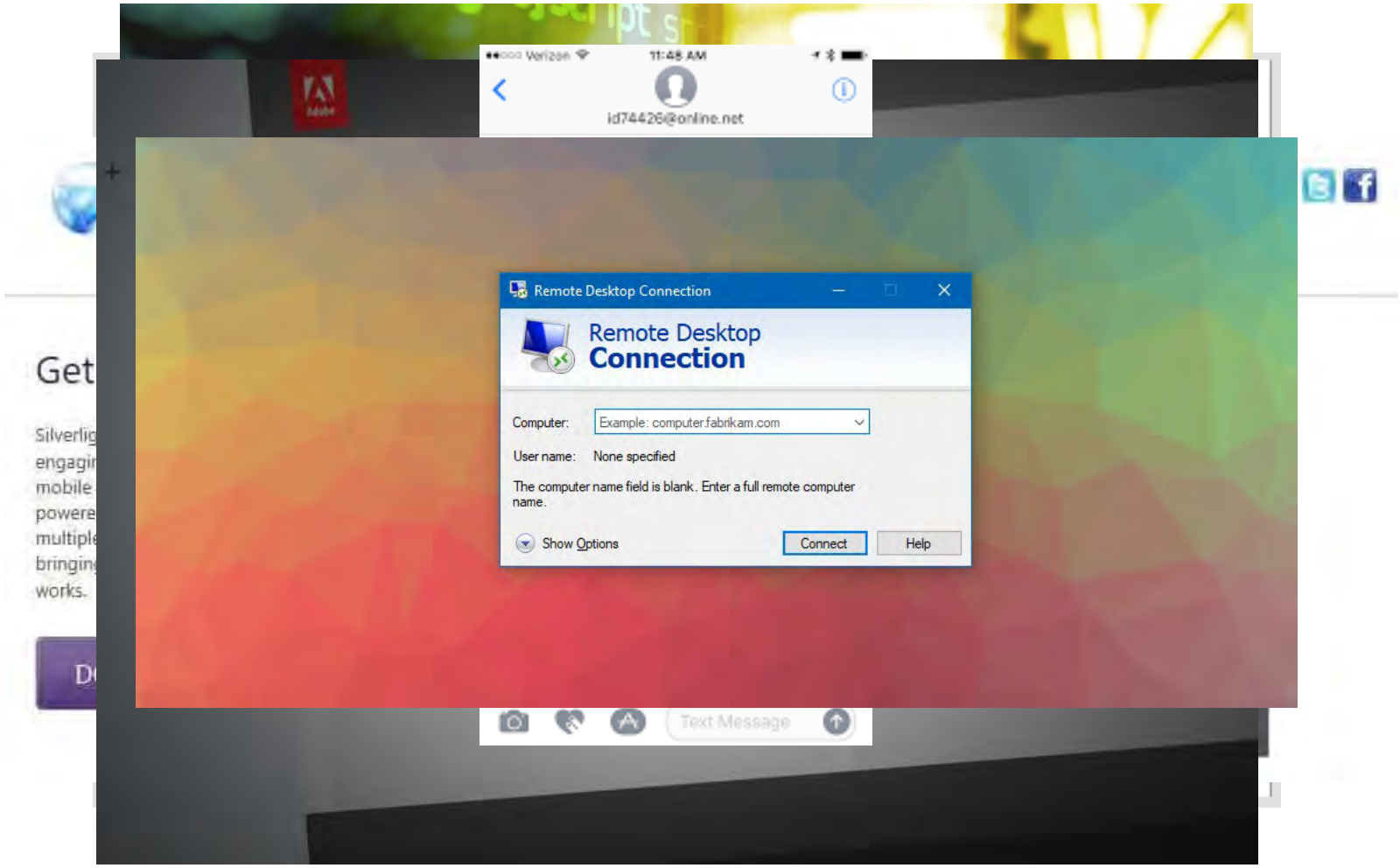
Infects…Encrypts…Extorts

- 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.

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



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 20201, 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.

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 Persistant 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 Compromises

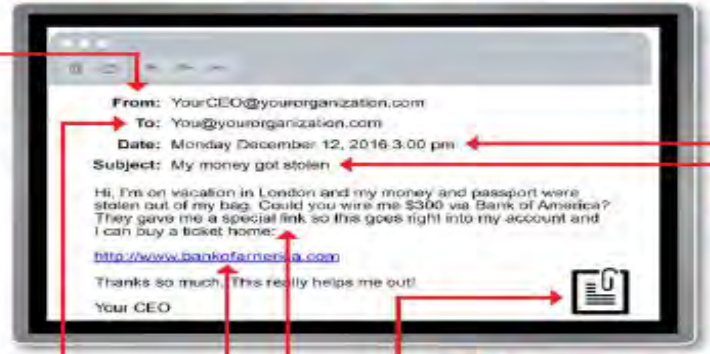
- Target (2014) – HVAC security
- Equifax – 3rd Party Software flaw
- Verizon – Flawed Analytic software
- SolarWinds & Kaseya Customers – Malware laced updates

- Polls indicate that over 50 percent of organizations have had a breach that was caused by one of their vendors
- Supply Chain Attacks Spiked 78%

HOW ARE YOU TARGETED?

Jason Burt
September 8, 2022

Social Engineering Red Flags



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.bankofamerica.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?

Especially under the prevailing conditions – Always Pause and Ask:

Is this message expected?

Do I recognize the sender of this email?

Is there something odd about the email address?

Verify the email address/domain by hovering the cursor over an email address or embedded link, without clicking; the actual destination appears in a text box or bubble.

Is there a needlessly urgent call to action in the email?

Is the action sought odd or unfamiliar?

Are my network access credentials requested after clicking to open a link?

NEVER enter user name and password in these circumstances!

Be Attentive – and Protect Yourself and the Network

Jason Burt
eptember 8, 2022

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.

Jason Burt
September 8, 2022

How to Protect Against Ransomware

- Keep all hardware, software and operating systems up to date.
- **Always** backup your data regularly and test/run drills to restore data from backups regularly.
- Educate your family and co-workers on safe internet browsing practices.
- For organizations specifically:
  - Practice good cyber hygiene, backup and update apps, and use multifactor authentication.
  - Implement “the concept of least privilege.”
  - Educate employees on cyber awareness best practices.

Jason Burt
September 8, 2022

How to Respond If You've Been Affected

- **Report it** immediately
  - If you're a part of an organization, be sure to report the issue to the proper Points of Contact.
- Prevent the spread of the infection by isolating the infected computers and systems.
- Try to identify the type of ransomware to help understand what you are working with.
- Work with cybersecurity professionals who are trained in resolving these issues.
- Recover your data from your backups **after** you test the backups to ensure the data on the backups is safe to restore.

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.

Jason Burt
September 8, 2022

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.

Jason Burt
September 8, 2022

Keeping Your Kids Safe Online

Take an active role in protecting your children

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

Jason Burt
September 8, 2022

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.




Jason Burt
September 8, 2022

CISA CYBER SERVICES

Jason Burt
September 8, 2022

Criticality of Periodic Assessments

- Periodic assessments are essential for resilience
- Can’t protect if you don’t know what needs protection
- Can’t fix what needs if you don’t know what’s wrong

Jason Burt
September 8, 2022

Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

Jason Burt
September 8, 2022

Range of Cybersecurity Services

STRATEGIC
(C-Suite Level)

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool Strategic/Technical)
- Phishing Campaign Assessment (EVERYONE)
- **Vulnerability Scanning / Hygiene (Technical)**
- Validated Architecture Design Review (Technical)
- Risk and Vulnerability Assessment (Technical)

TECHNICAL
(Network-Administrator Level)

Jason Burt
September 8, 2022

VULNERABILITY SCANNING / HYGIENE

Jason Burt
September 8, 2022

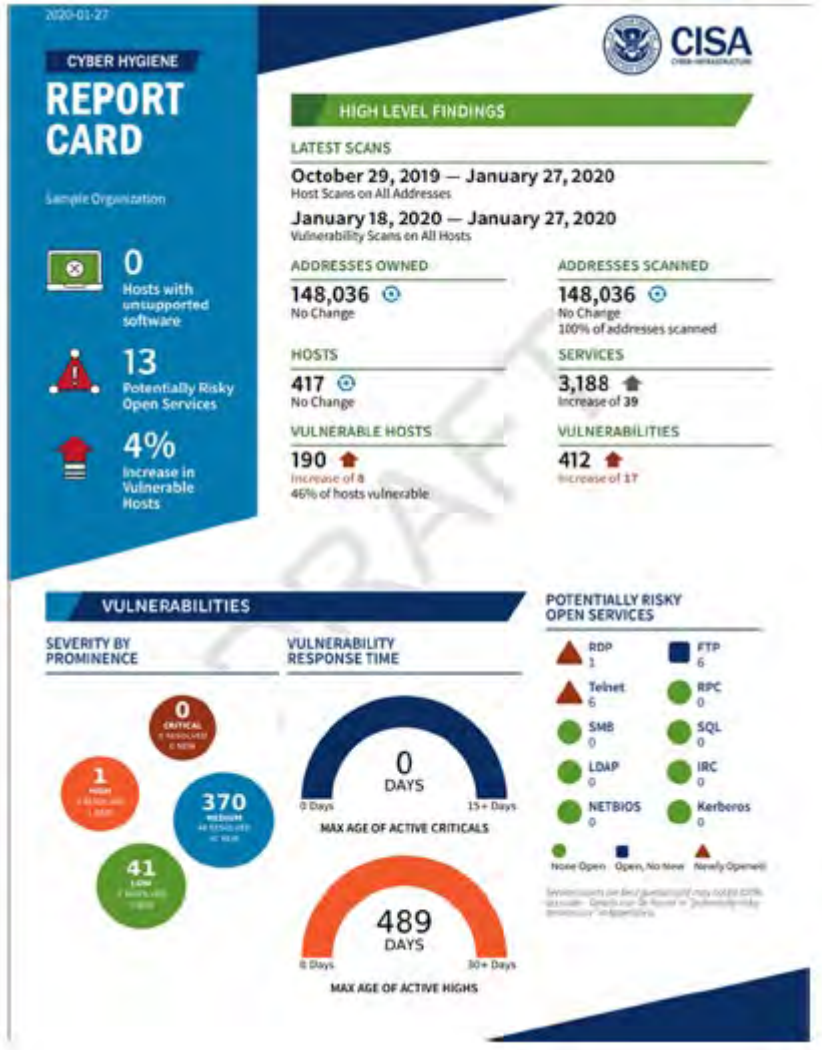
Cyber Hygiene Report Card

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services



Jason Burt
September 8, 2022

CYBER RESILIENCE REVIEW

Jason Burt
September 8, 2022

Cyber Resilience Review Domains

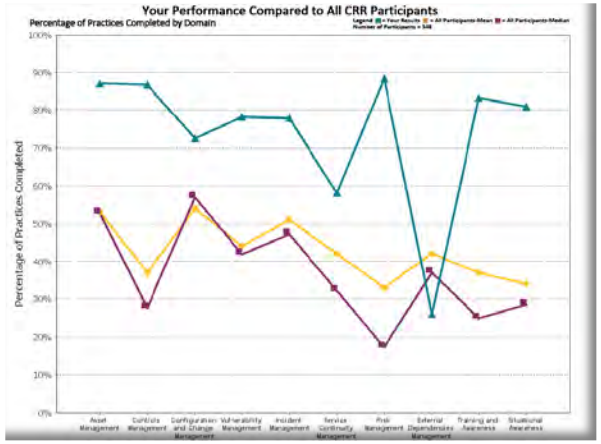
Asset Management Know your assets being protected & their requirements, e.g., CIA	**Risk Management** Know and address your biggest risks that considers cost and your risk tolerances
Configuration and Change Management Manage asset configurations and changes	**Service Continuity Management** Ensure workable plans are in place to manage disruptions
Controls Management Manage and monitor controls to ensure they are meeting your objectives	**Situational Awareness** Discover and analyze information related to immediate operational stability and security
External Dependencies Management Know your most important external entities and manage the risks posed to essential services	**Training and Awareness** Ensure your people are trained on and aware of cybersecurity risks and practices
Incident Management Be able to detect and respond to incidents	**Vulnerability Management** Know your vulnerabilities and manage those that pose the most risk

For more information: http://www.us-cert.gov/ccubedvp

Jason Burt
September 8, 2022

CRR Sample Report

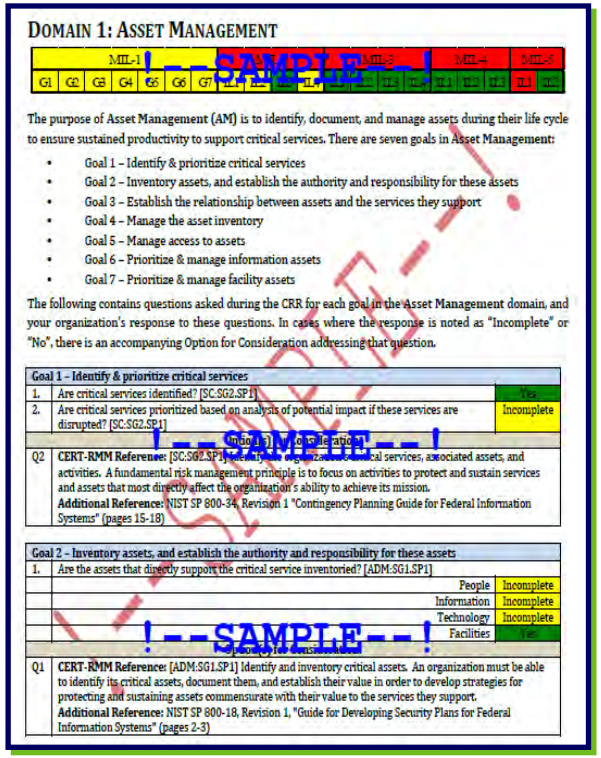
Each CRR report includes:



Comparison data with other CRR participants
**facilitated only*

A summary "snapshot" graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses



EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

Jason Burt
September 8, 2022

EDM Assessment Organization and Structure

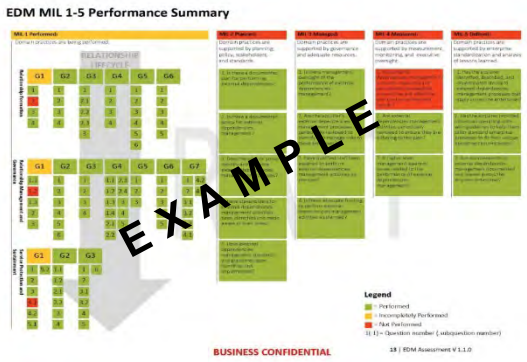
- Structure and scoring similar to Cyber Resilience Review
- Uses one Maturity Indicator Level (MIL) scale with three lifecycle domains.

Relationship Formation *Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.*
Relationship Management and Governance *Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk.*
Service Protection and Sustainment *Assesses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.*

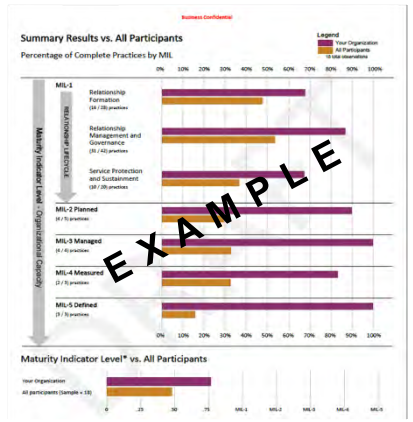
EDM Assessment Report

Each EDM report includes:

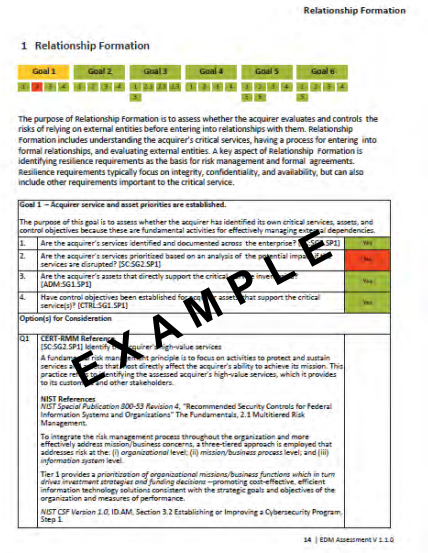
- Performance summary of existing capability managing external dependencies



- Comparison data with other EDM participants



- Sub-domain performance of existing capability managing external dependencies and options for consideration for all responses



Jason Burt
September 8, 2022

CYBER INFRASTRUCTURE SURVEY

Jason Burt
September 8, 2022

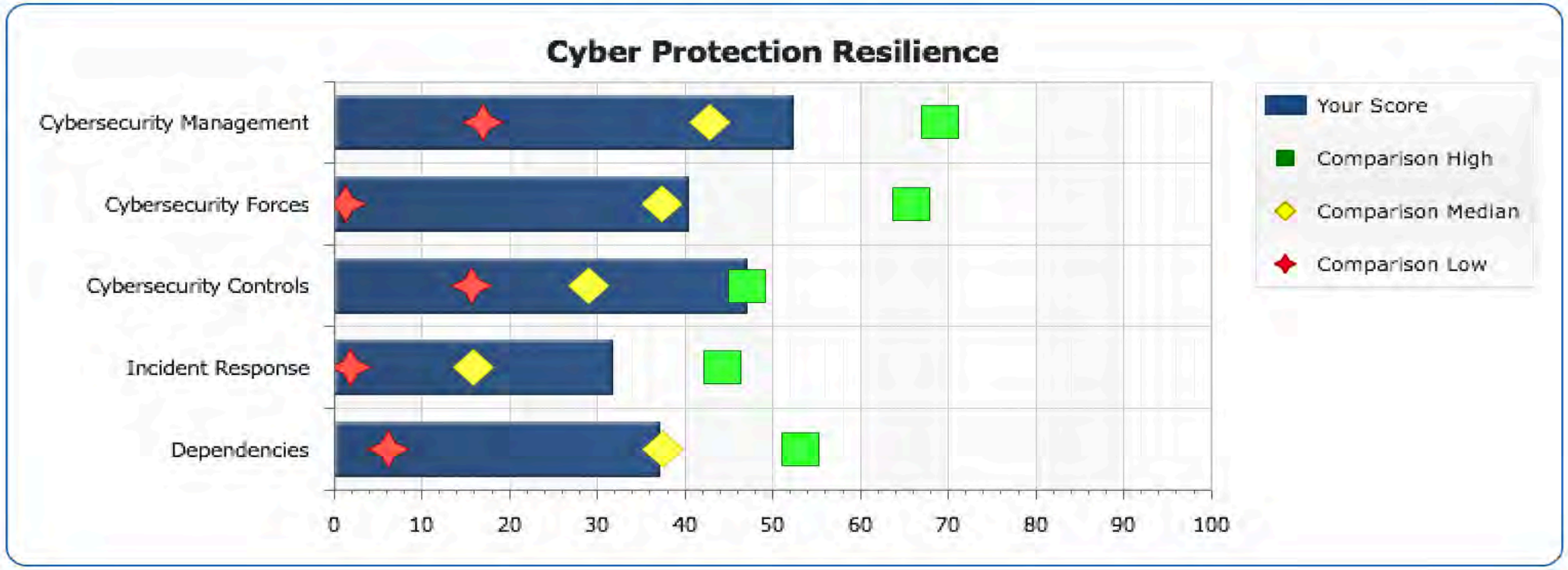
Cyber Infrastructure Survey (CIS)

- Purpose: Evaluate security controls, cyber preparedness, overall resilience.
- Delivery: CSA-facilitated
- Benefits:
  - Effective assessment of cybersecurity controls in place for a critical service,
  - Easy-to-use interactive dashboard to support cybersecurity planning and resource allocation.

Jason Burt

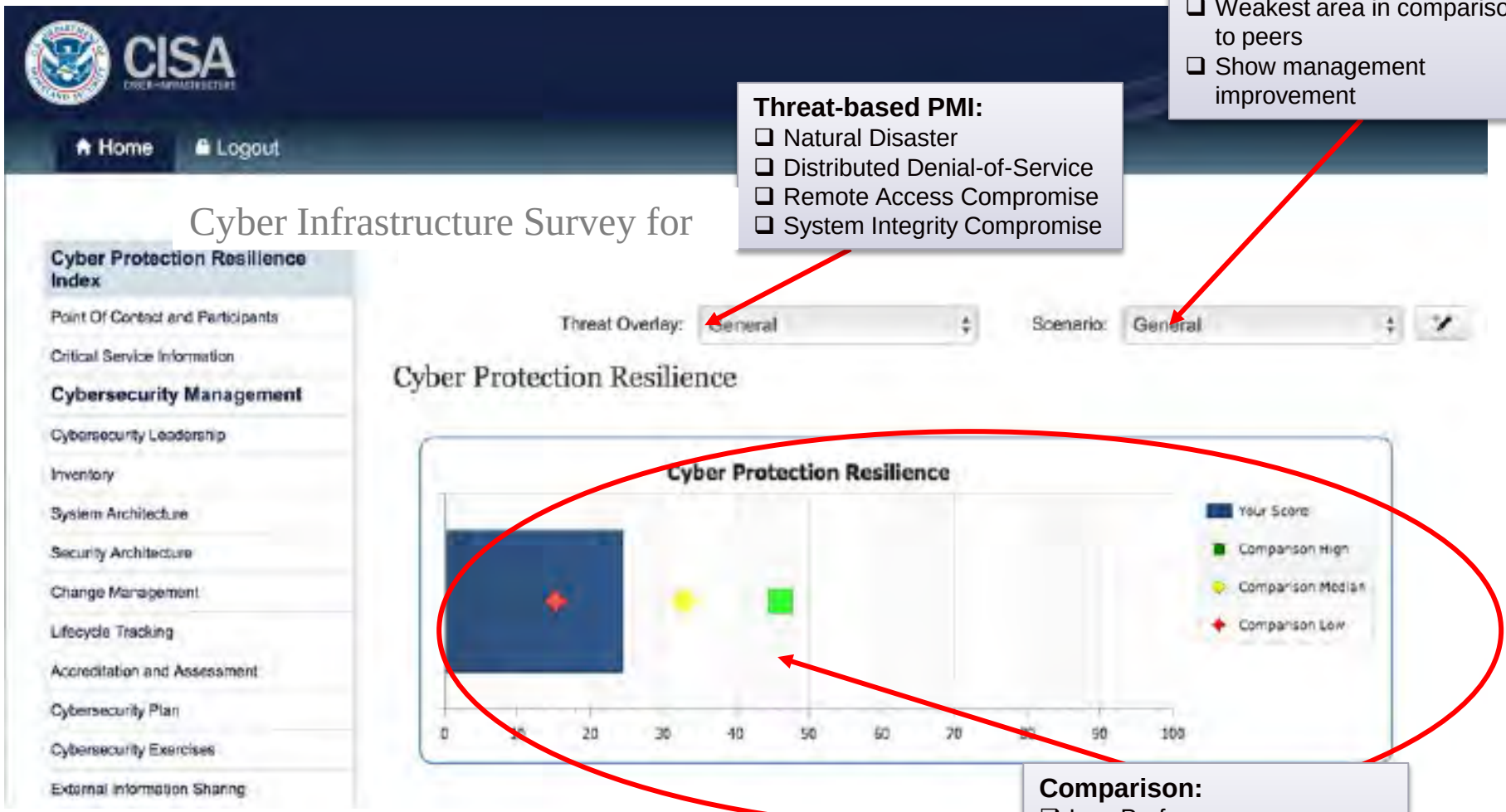
CIS Dashboard - Comparison

- Shows the low, median, and high performers
- Compares your organization to the aggregate



Jason Burt
September 8, 2022

Example of CIS Dashboard



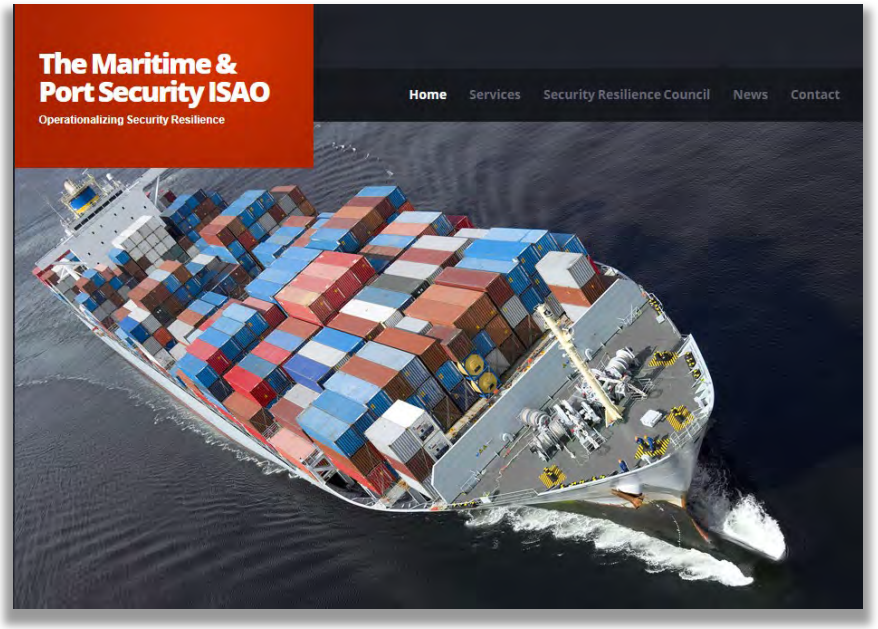
Threat-based PMI:
- ❑ Natural Disaster
- ❑ Distributed Denial-of-Service
- ❑ Remote Access Compromise
- ❑ System Integrity Compromise

Scenario:
- ❑ Where should we to invest?
- ❑ Weakest area in comparison to peers
- ❑ Show management improvement

Comparison:
- ❑ Low Performers
- ❑ Median Performers
- ❑ High Performers

MARITIME CYBERSECURITY RESOURCES

- Port and Maritime Cyber Resilience
  www.mpsisao.org
- CISA National Cyber Awareness System
  https://us-cert.cisa.gov/ncas
- CISA Stop Ransomware Campaign
  https://www.cisa.gov/stopransomware
- CISA Shields up Initiative
  https://www.cisa.gov/shields-up
- CISA Known Exploited Vulnerabilities Catalog
  https://www.cisa.gov/known-exploited-vulnerabilities-catalog



Jason Burt
September 8, 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)

Stephanie Watt, CISSM
Region 4 Cybersecurity State Coordinator - Alabama
Stephanie.Watt@cisa.dhs.gov
(202) 615-4615 (Cell)

Klint Walker, CISSP
Region 4 Cybersecurity Advisor - Georgia, Tennessee, Kentucky
Klint.Walker@hq.dhs.gov
(404) 895-1127 (Cell)