Human Element Of Cybersecurity

March 04, 2025

Giovanni Williams | Cybersecurity Advisor
Cybersecurity Infrastructure Security Agency Region 9
Hawaii | American Samoa

Importance of Human Elements of Cybersecurity

- Technology Alone Cannot Secure Organizations, as Human behavior plays a critical Role.
- Attackers Often Exploit Human Vulnerabilities rather than Technical Flaws
- Understanding and Mitigating Human Risk Can Significantly Reduce Security Incidents

What is Social Engineering and Why it works

What is social engineering:

- Psychological manipulation and exploits of human error or weakness rather than technical or digital system vulnerabilities, it is sometimes called "human hacking."

Why it works:

- **Authority Bias-** People are more likely to comply when messages come from an authoritative source.
- **Urgency and Fear-** Attackers create a sense of urgency to pressure victims into acting without thinking.
- **Trust and Familiarity-** Attackers use social connections or impersonate known contacts to gain trust.

Social Engineering Cycle

Social Engineering Types

- **Phishing-** Fraudulent Emails, Messages, or websites designed to trick victims into revealing sensitive information.
- **Vishing (Voice Phishing)-** Impersonating officials or employees over the phone to extract data.
- **Smishing- (SMS Phishing)-** Using Text messages to trick users into clicking malicious links.
- **Business Email Compromise (BEC)-** Spoofing executive emails to illicit fraudulent actions.
- **Tailgating/Piggybacking-** Implement strict physical and digital access controls to prevent unauthorized entry.

Social Engineering Indicators

- **Suspicious sender's address.** The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.
- **Generic greetings and signature.** Both a generic greeting—such as "Dear Valued Customer" or "Sir/Ma'am"—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.
- **Spoofed hyperlinks and websites.** If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.
- **Spelling and layout.** Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.
- **Suspicious attachments.** An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

Phishing Email Example

Work From Home Position

Reply | Reply All | Forward | ...

Thu 12/10/2020 10:36 AM

ES

Evan Ston
To

You forwarded this message on 12/10/2020 10:39 A.M.

Hello,
I am a staff in the college, a professor of Medicine shared me a link for students who might be interested in a PAID UNICEF PART TIME POSITION job to make up to $500 weekly,

Email for More info - freemanjohnny6s66@outlook.com

NOTE: This is strictly Work From Home Position

Do have a good day,
Thank you

Social Engineering Best Practices

- **Be suspicious** of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- **Do not provide** personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- **Do not reveal** personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- **Don't send** sensitive information over the internet before checking a website's security. (See Protecting Your Privacy for more information.)
  - **Pay attention** to the Uniform Resource Locator (URL) of a website. Look for URLs that begin with "https"—an indication that sites are secure—rather than "http."
  - **Look** for a closed padlock icon—a sign your information will be encrypted.
- If you are unsure whether an email request is legitimate, try to **verify** it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group. (See the APWG eCrime Research Papers).
- **Install and maintain** anti-virus software, firewalls, and email filters to reduce some of this traffic. (See Understanding Firewalls for Home and Small Office Use, Protecting Against Malicious Code, and Reducing Spam for more information.)
- **Take advantage** of any anti-phishing features offered by your email client and web browser.
- **Enforce** multifactor authentication (MFA). (See Supplementing Passwords for more information.)

What is a Malicious Insider

What is a Malicious Insider:

- **Employees**, contractors, or business partners who misuse their access for personal gain or to harm the organization.
- Can be **motivated** by financial gain, revenge, coercion, or Ideological reasons.

Malicious Insider Examples

- **Edward Snowden (2013)-** Leaked Classified Documents
- **Tesla Insider Sabotage (2018)-**Employee altered code in the manufacturing process and leaked sensitive data.
- **Marriot Data Breach- (2018-2020)-** An insider accessed guest records and exposed 5.2 million customer details.

Malicious Insider Indicators and Detection

- **Unusual Access Patterns-** Employees accessing sensitive data they don't normally use.
- **Frequent Policy Violations-** Bypassing security controls, excessive downloading of files.
- **Behavioral Changes-** Disgruntled employees expressing resentment or showing financial distress.

Malicious Insider Best Practices

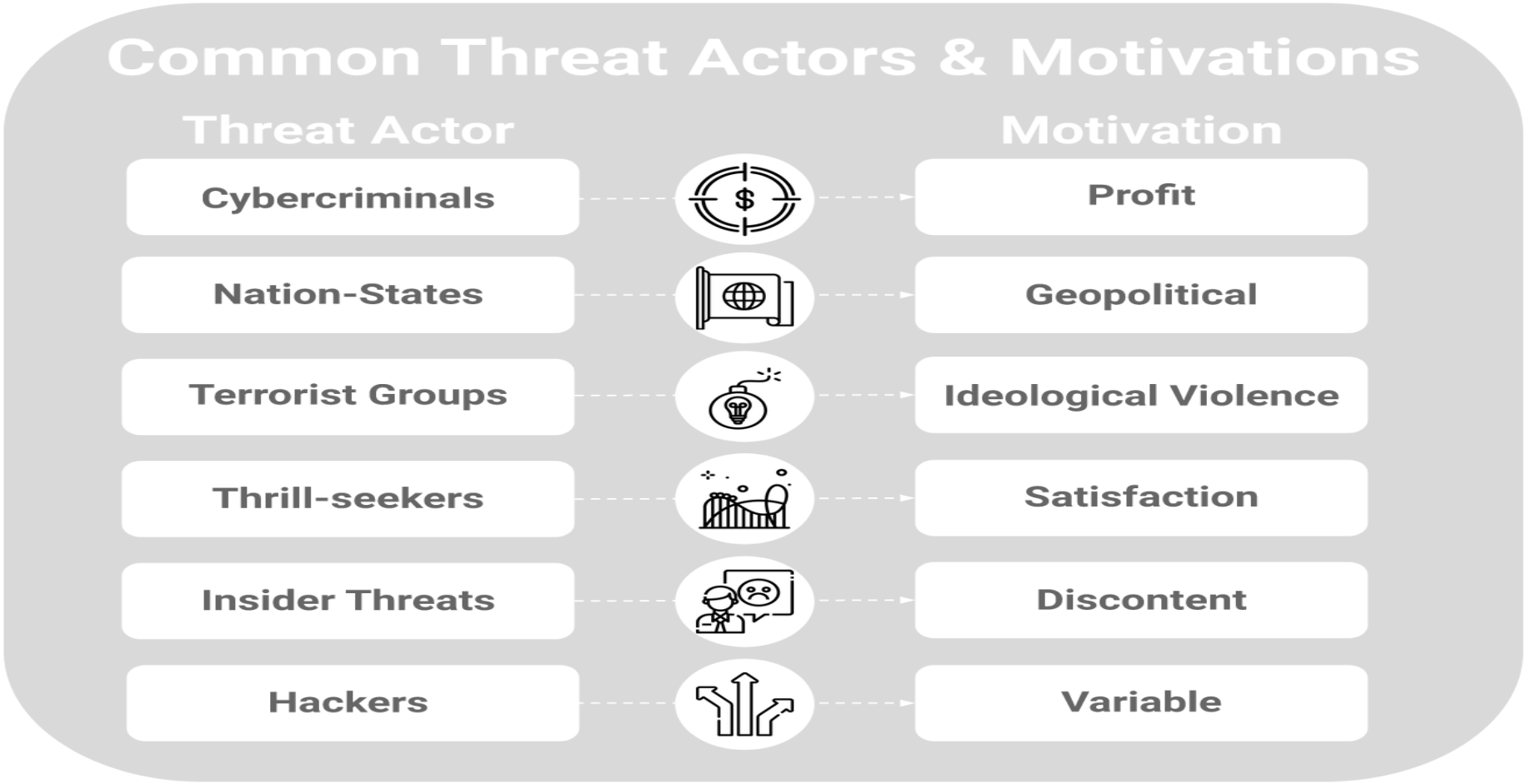
- **Zero Trust Architecture-** Limit access to only what employees need for their roles.
- **User Behavior Analytics (UBA)-** AI-driven tools to detect anomalous activity.
- **Exit/Termination Procedures–** Ensure Immediate revocation of access when an employee leave or is terminated.
- **Regular Security Audits-** Monitor Privilege escalations and data access logs.

Cyber Criminal Activity

What is Cyber Criminal Activity:

- Organized groups or individuals who target organizations for financial gain, disruption, or espionage and don't care how large or small an organization.

Cyber Criminal Motivations



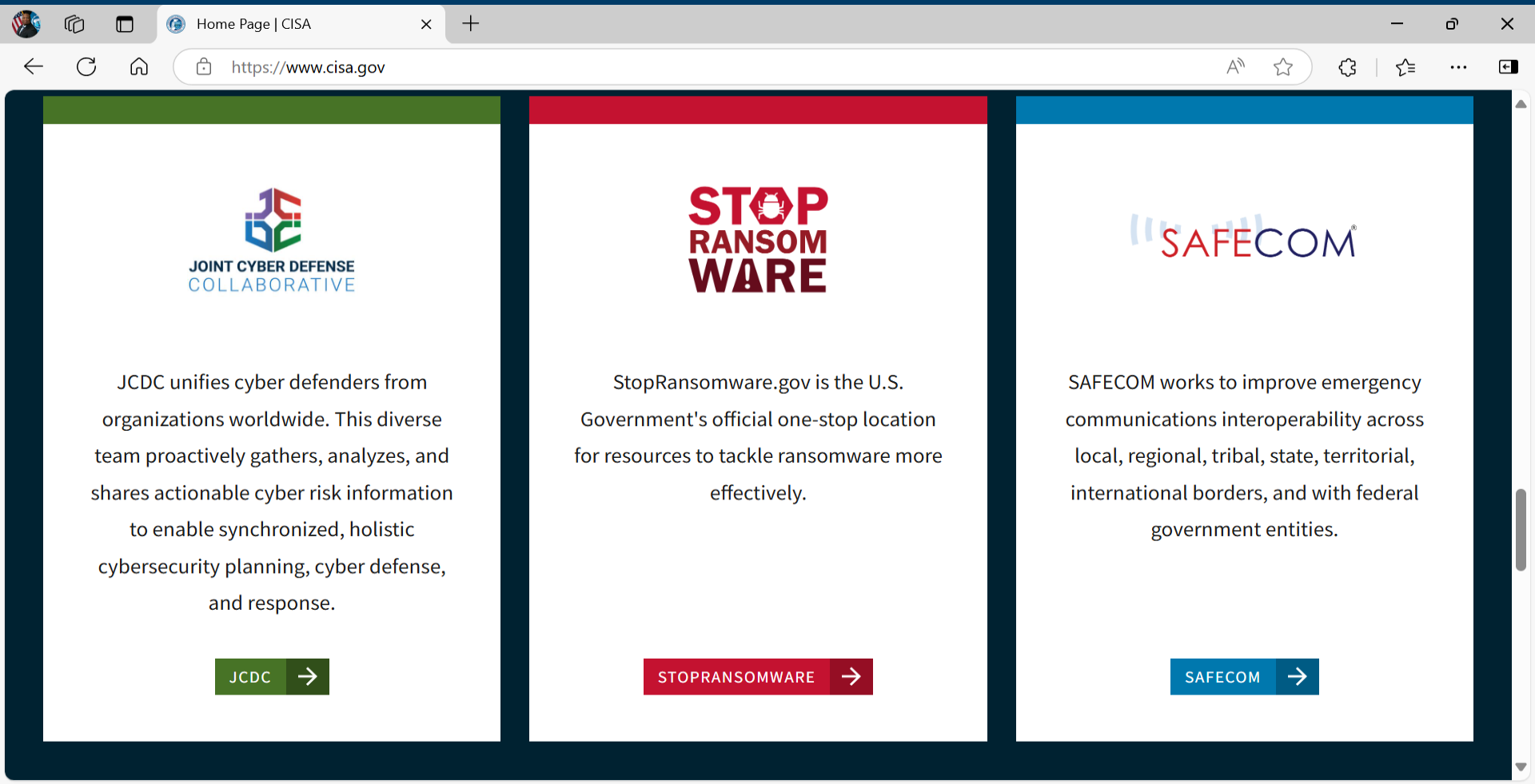
Best Practices to Prevent Cyber Criminals

1. **Enforce** strong password policies and require multi-factor authentication (MFA) for all accounts. Regularly patch and update software and systems to mitigate vulnerabilities.
2. **Subscribe** to cybersecurity threat intelligence feeds to stay informed about emerging threats and criminal tactics.
3. **Develop** and regularly **test** an incident response plan to ensure the organization can quickly contain and recover from cybercriminal activity.
4. **Limit** the ability of attackers to move laterally within the network by segmenting sensitive systems and data.
5. **Encrypt** sensitive data both at rest and in transit to protect it from theft or tampering.

What to do if you think you are a victim

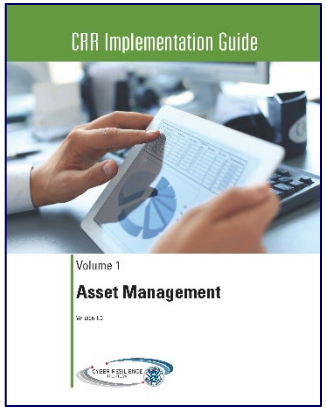
- **Initiate** your Internal Response Process
- If you believe you might have revealed sensitive information about your organization, **report it** to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, **contact** your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately **change** any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- **Watch** for other signs of identity theft. (See Preventing and Responding to Identity Theft for more information.)
- **Consider** reporting the attack to the police and file a report with the Federal Trade Commission.

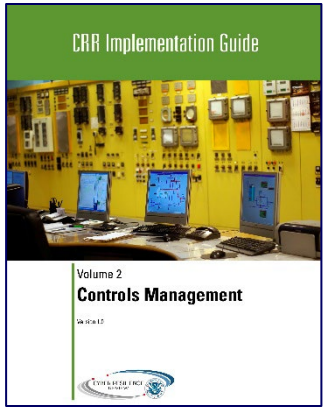
WWW.CISA.GOV

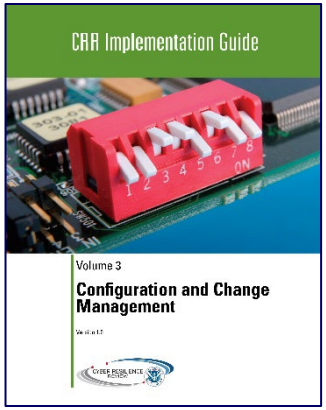


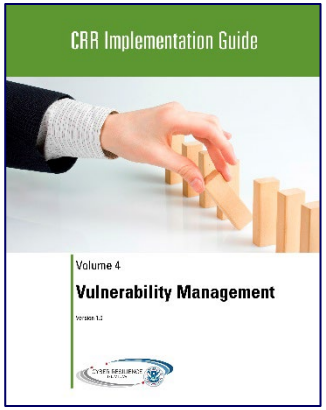
Visit: https://www.cisa.gov

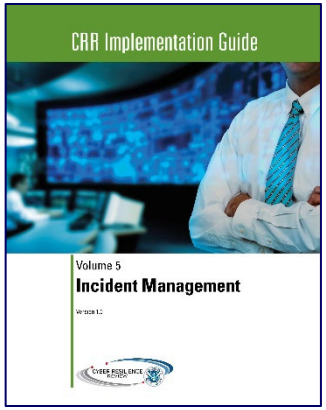
Available Resource Guides

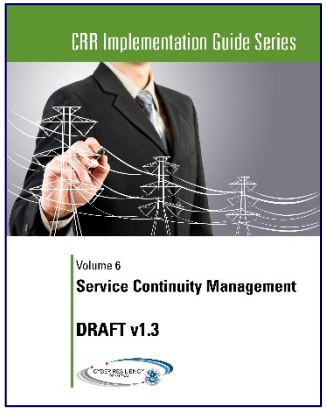


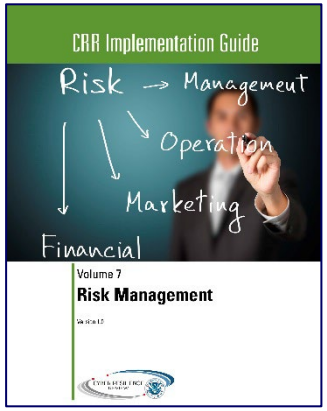


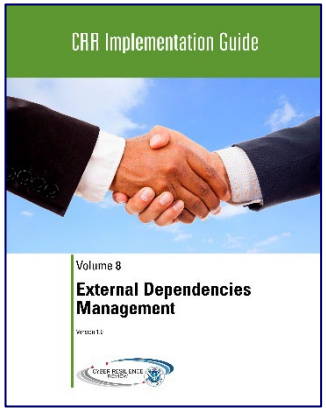


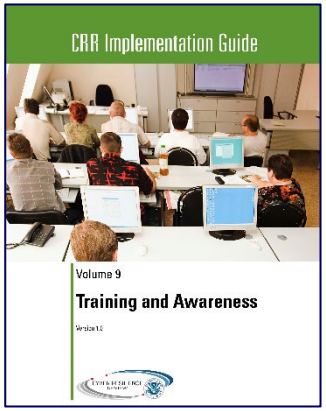


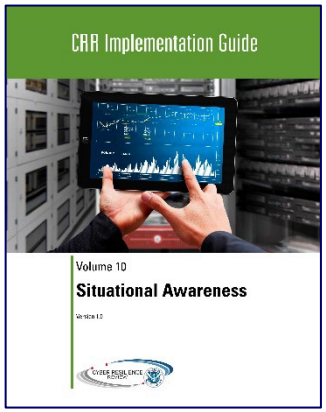






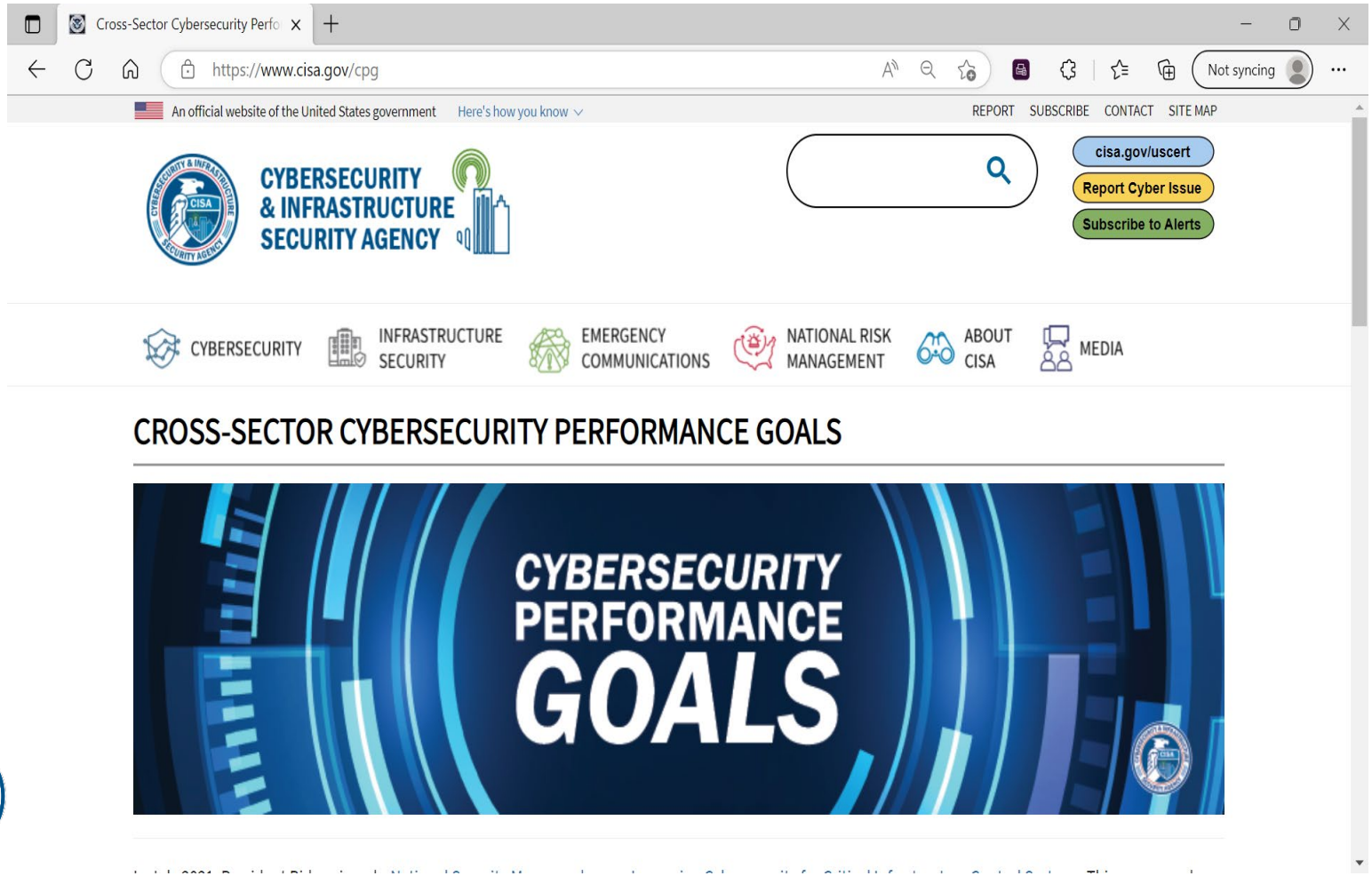






Cybersecurity Performance Goals

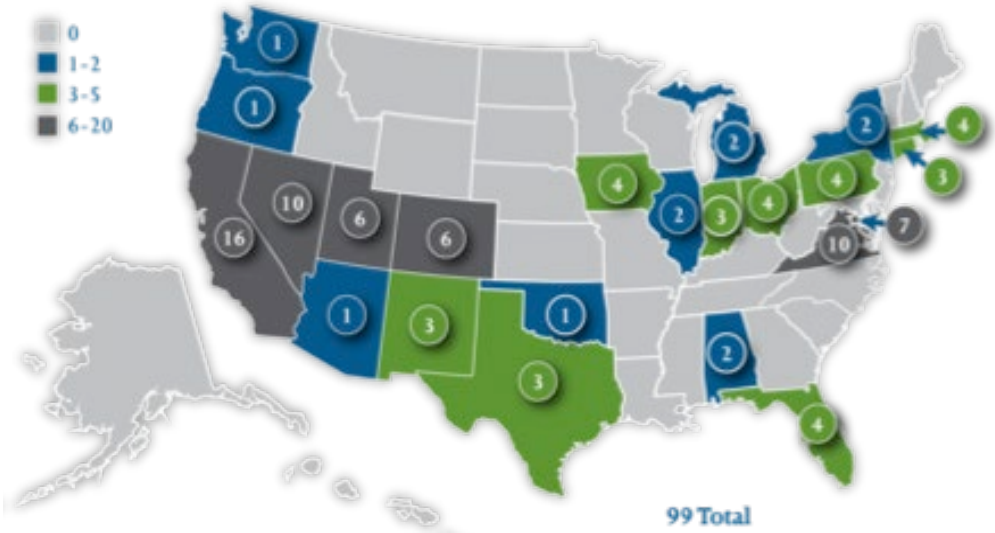
Released in 2022, foundation steps to get started on the road to cyber resilience.



Cyber Exercises and Planning

CISA's National Cyber Exercise and Planning Program develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

- Cyber Storm Exercise –CISA's flagship national-level biennial exercise
- Exercise Planning and Conduct
- Cyber Exercise Consulting and Subject Expertise Support
- Cyber Planning Support
- Off-the-Shelf Resources

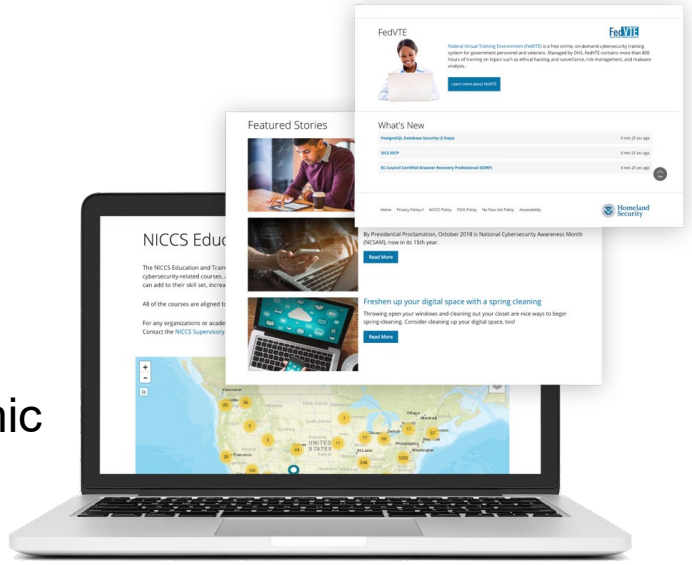


Cybersecurity Training Resources

CISA offers easily accessible education and awareness resources through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Searchable Training Catalog with 4,400 plus cyber-related courses offered by nationwide cybersecurity educators
- Interactive National Cybersecurity Workforce Framework
- Cybersecurity Program information: FedVTE, Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
- Tools and resources for cyber managers
- Upcoming cybersecurity events list



For more information, visit Cybersecurity Training & Exercises | CISA

Recap

- **Social Engineering attacks** rely on psychological manipulation.
- **Malicious Insiders** pose internal risk that require detection and access control.
- **Cyber Criminals u**se various techniques to exploit individuals and organizations.
- **Awareness, Training** and security best practices help mitigate these threats.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Questions? Next Steps?

Contact your local Cybersecurity Advisor!

Giovanni Williams
Cybersecurity Advisor, Region 9
Hawaii | American Samoa
Cybersecurity and Infrastructure Security Agency
202.503.5614
giovanni.williams@cisa.dhs.gov

Krishna A. Easton
Cybersecurity State Coordinator, Region 9
Hawaii
Cybersecurity and Infrastructure Security Agency
301.848.1794
krishna.easton@cisa.dhs.gov