Introduction to Cybersecurity Infrastructure Security Agency (CISA) & Resilience Resources

October 8, 2024

Giovanni Williams | Supervisory Cybersecurity Advisor
Cybersecurity Infrastructure Security Agency Region 4
Alabama | Florida | Georgia | Kentucky | Mississippi | North Carolina | South Carolina | Tennessee

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

A secure and resilient critical infrastructure for the American people.

MISSION

Lead the National effort to understand and manage cyber and physical risk to our critical infrastructure.

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

CISA is the Nation’s lead civilian cybersecurity agency and the national coordinator for critical infrastructure security and resilience efforts.

We work with partners to:
DEFEND TODAY and **SECURE TOMORROW**

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

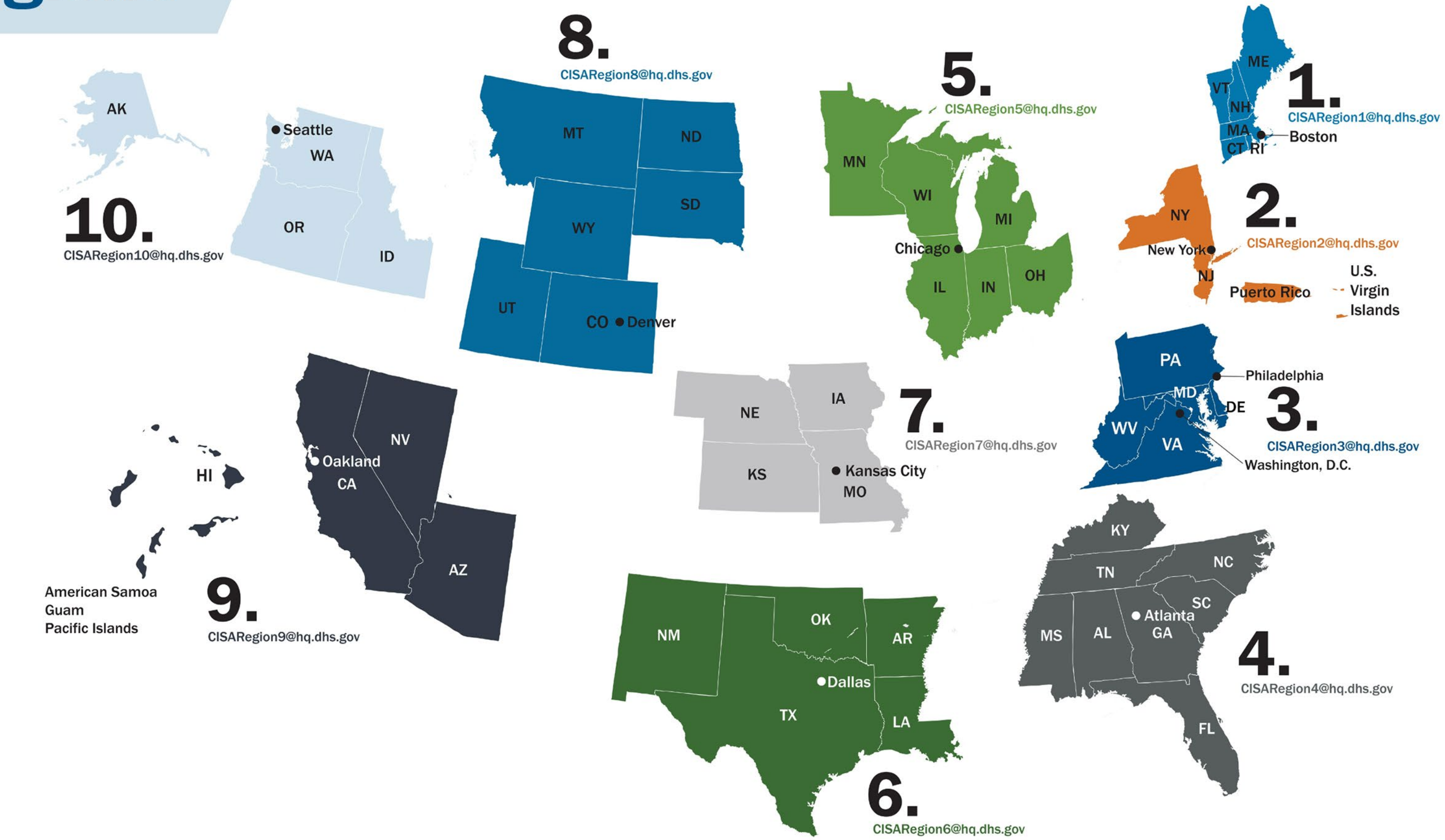
Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

- FEDERAL NETWORK PROTECTION
- PROACTIVE CYBER PROTECTION
- INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
- EMERGENCY COMMUNICATIONS

CISA Regions

1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Irving, TX
7	Kansas City, MO
8	Lakewood, CO
9	Oakland, CA
10	Seattle, WA
CS	Pensacola, FL



The Significance of Critical Infrastructure

Critical infrastructure refers to the assets, systems, and networks, whether physical or cyber, so vital to the Nation that their incapacitation or destruction would have a debilitating effect on **national security, the economy, public health or safety, and our way of life.**

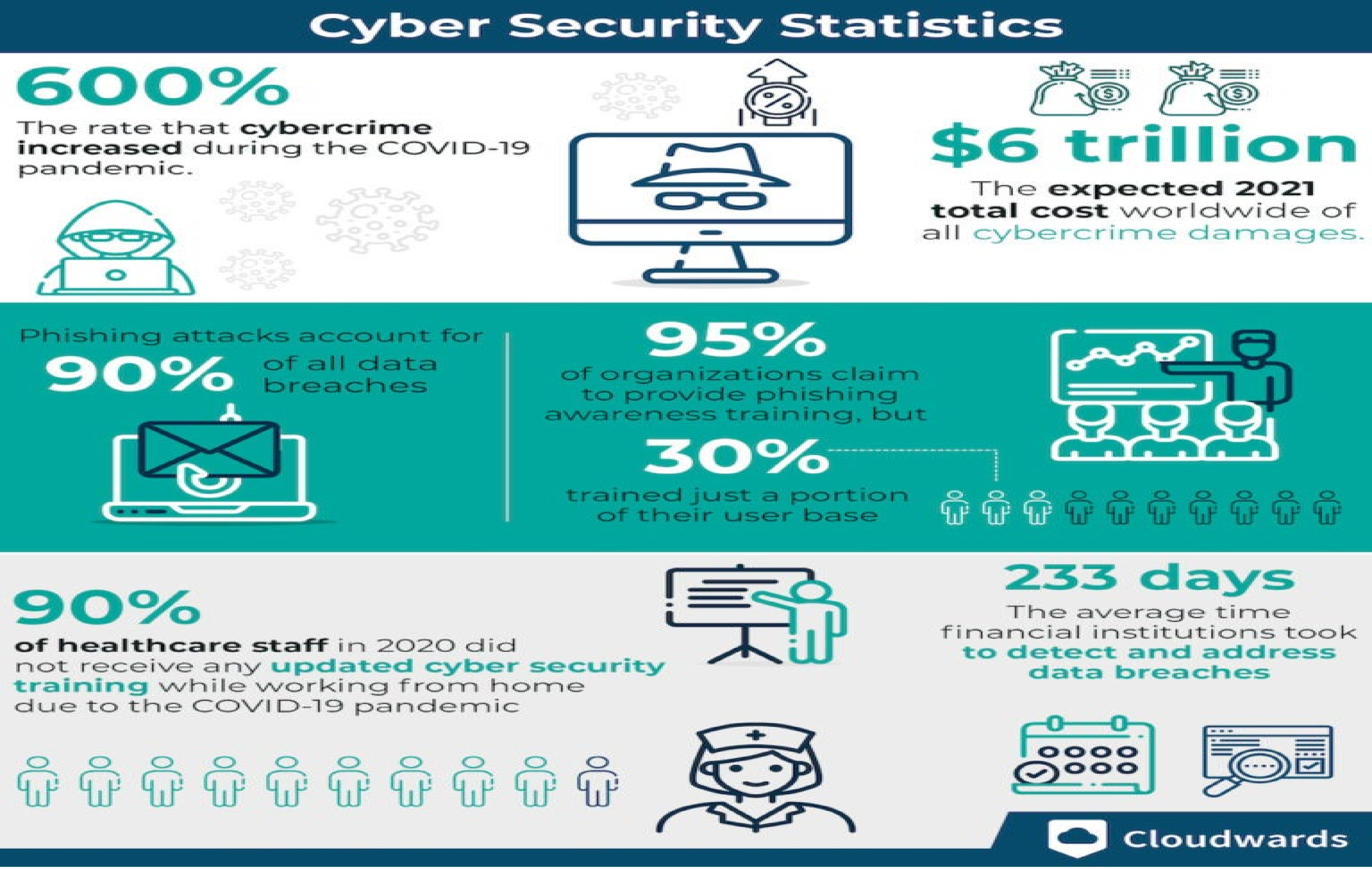
16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

CHEMICAL	DHS (CISA)
COMMERCIAL FACILITIES	DHS (CISA)
COMMUNICATIONS	DHS (CISA)
CRITICAL MANUFACTURING	DHS (CISA)
DAMS	DHS (CISA)
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	DHS (CISA)
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & DHS (FPS)
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	DHS (CISA)
NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
TRANSPORTATIONS SYSTEMS	(TSA & USCG)
WATER	EPA

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 Security Statistics

600%

The rate that **cybercrime increased** during the COVID-19 pandemic.

$6 trillion

The **expected 2021 total cost** worldwide of all cybercrime damages.

Phishing attacks account for **90%** of all data breaches

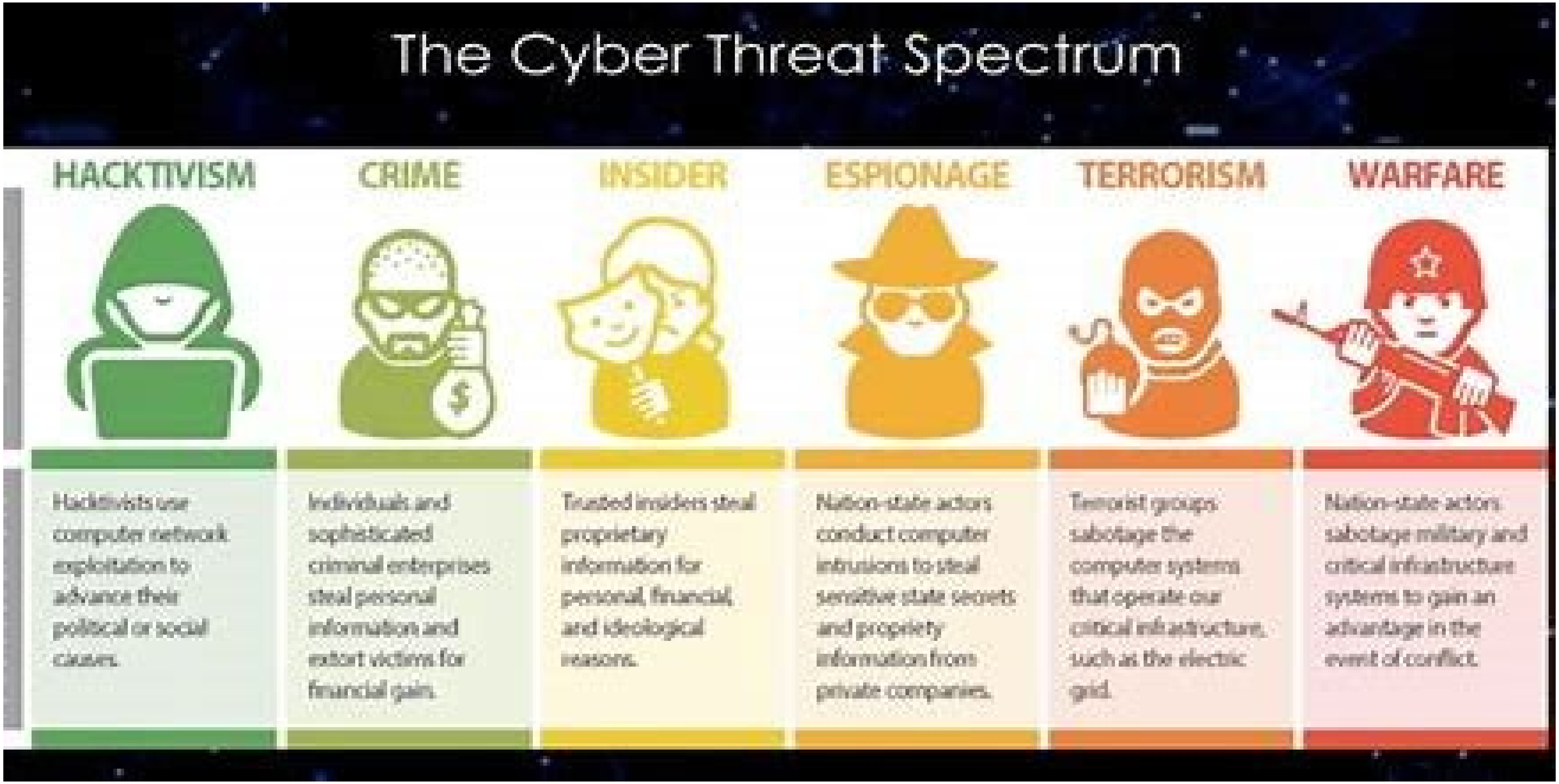
95% of organizations claim to provide phishing awareness training, but **30%** trained just a portion of their user base

90% **of healthcare staff** in 2020 did not receive any **updated cyber security training** while working from home due to the COVID-19 pandemic

233 days The average time financial institutions took **to detect and address data breaches**

Cloudwards

Who's after your data



The Cyber Threat Spectrum

HACKTIVISM

Hacktivists use computer network exploitation to advance their political or social causes.

CRIME

Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.

INSIDER

Trusted insiders steal proprietary information for personal, financial, and ideological reasons.

ESPIONAGE

Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.

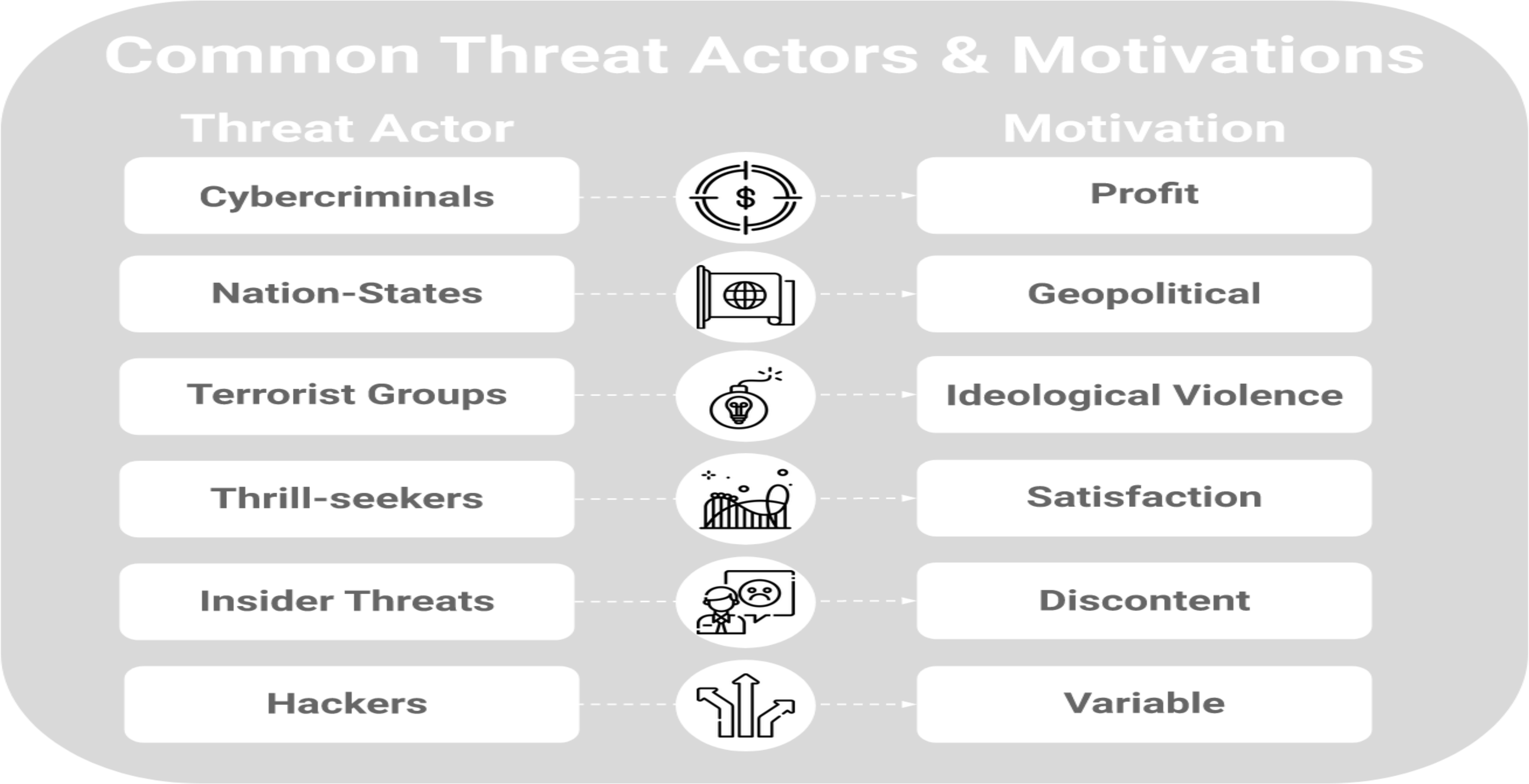
TERRORISM

Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.

WARFARE

Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

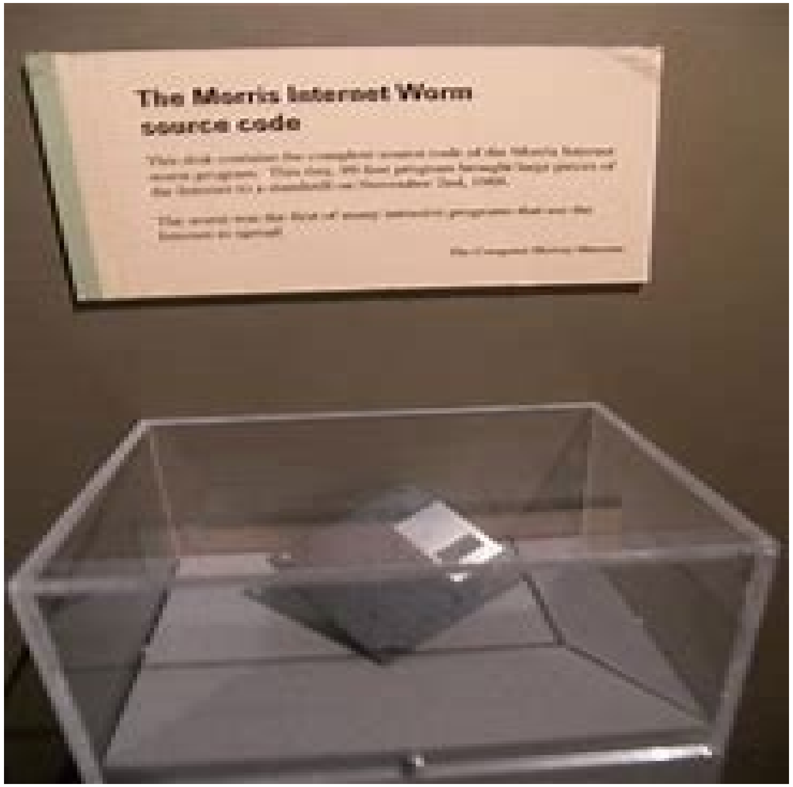
Why they want your data



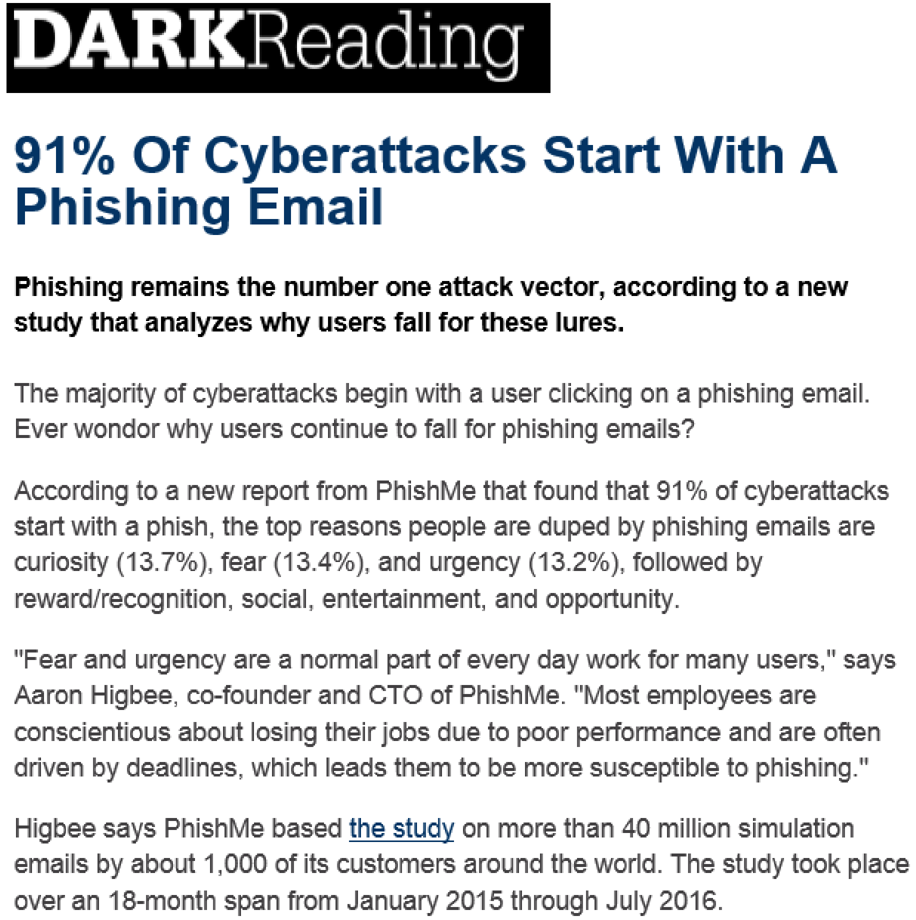
Common Threat Actors & Motivations

Threat Actor	Motivation
Cybercriminals	Profit
Nation-States	Geopolitical
Terrorist Groups	Ideological Violence
Thrill-seekers	Satisfaction
Insider Threats	Discontent
Hackers	Variable

Threat Actors can be Sophisticated…



But They Don’t Always Need To Be



DARKReading

91% Of Cyberattacks Start With A Phishing Email

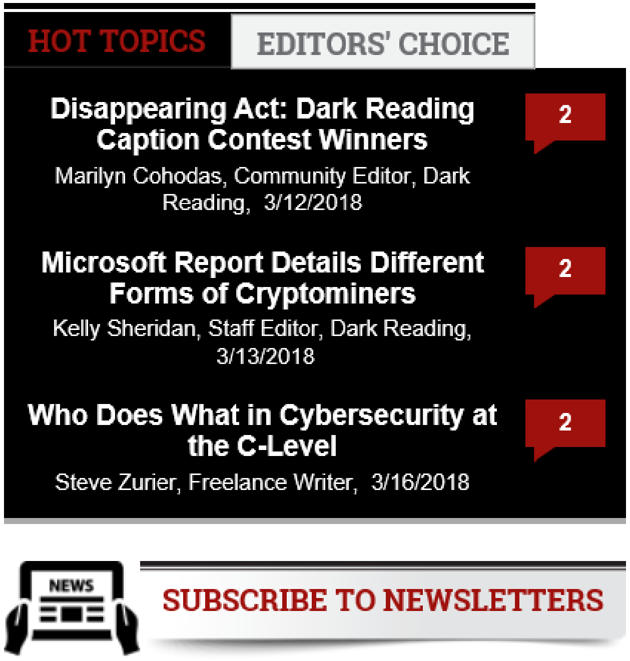
Phishing remains the number one attack vector, according to a new study that analyzes why users fall for these lures.

The majority of cyberattacks begin with a user clicking on a phishing email. Ever wondor why users continue to fall for phishing emails?

According to a new report from PhishMe that found that 91% of cyberattacks start with a phish, the top reasons people are duped by phishing emails are curiosity (13.7%), fear (13.4%), and urgency (13.2%), followed by reward/recognition, social, entertainment, and opportunity.

"Fear and urgency are a normal part of every day work for many users," says Aaron Higbee, co-founder and CTO of PhishMe. "Most employees are conscientious about losing their jobs due to poor performance and are often driven by deadlines, which leads them to be more susceptible to phishing."

Higbee says PhishMe based the study on more than 40 million simulation emails by about 1,000 of its customers around the world. The study took place over an 18-month span from January 2015 through July 2016.



HOT TOPICS | EDITORS' CHOICE

Disappearing Act: Dark Reading Caption Contest Winners 2
Marilyn Cohodas, Community Editor, Dark Reading, 3/12/2018

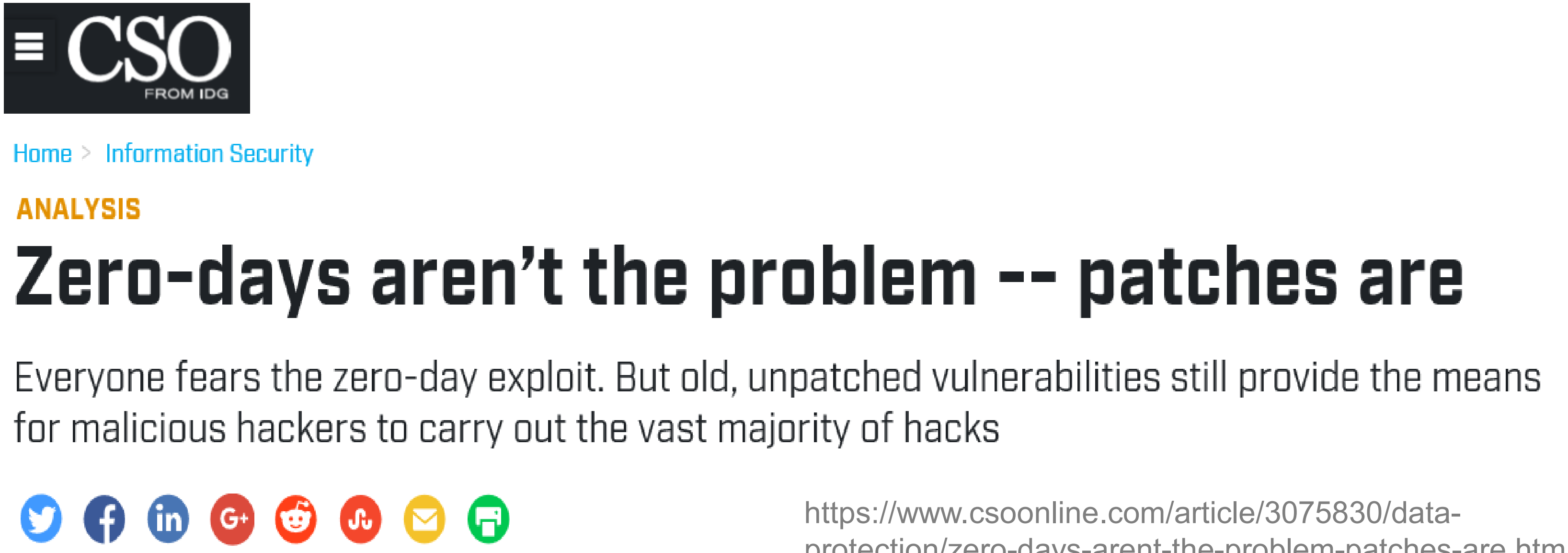
Microsoft Report Details Different Forms of Cryptominers 2
Kelly Sheridan, Staff Editor, Dark Reading, 3/13/2018

Who Does What in Cybersecurity at the C-Level 2
Steve Zurier, Freelance Writer, 3/16/2018

SUBSCRIBE TO NEWSLETTERS

https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

Updates Updates Updates



Home > Information Security

ANALYSIS

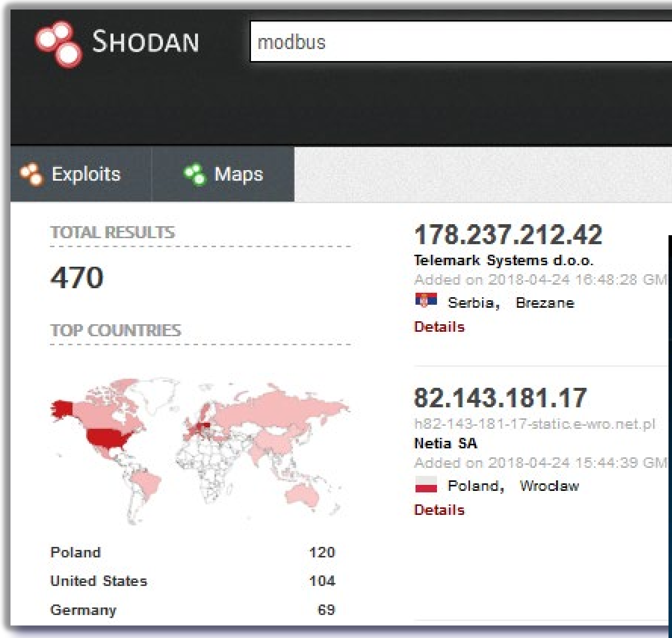
Zero-days aren't the problem -- patches are

Everyone fears the zero-day exploit. But old, unpatched vulnerabilities still provide the means for malicious hackers to carry out the vast majority of hacks

https://www.csoonline.com/article/3075830/data-protection/zero-days-arent-the-problem-patches-are.html

. . . Most hackers follow the path created by a very few smart ones -- and zero days make up a very small percentage of attacks. It turns out that patching vulnerable software, if implemented consistently, would stop most hackers cold and significantly reduce risk.

With Tools Aimed Directly At You



SHODAN modbus Explore Developer Pricing Enterprise Ac

Exploits Maps

TOTAL RESULTS

470

TOP COUNTRIES

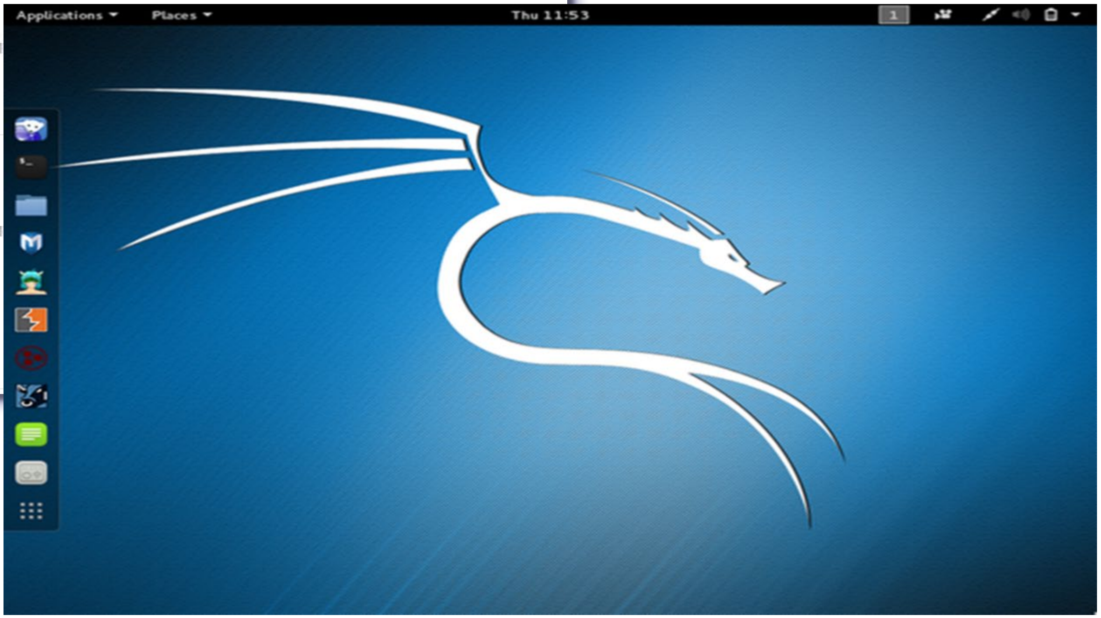
Poland	120
United States	104
Germany	69

178.237.212.42
Telemark Systems d.o.o.
Added on 2018-04-24 16:48:28 GM
Serbia, Brezane
Details

82.143.181.17
h82-143-181-17-static.e-wro.net.pl
Netia SA
Added on 2018-04-24 15:44:39 GM
Poland, Wroclaw
Details

metasploit®

John the Ripper

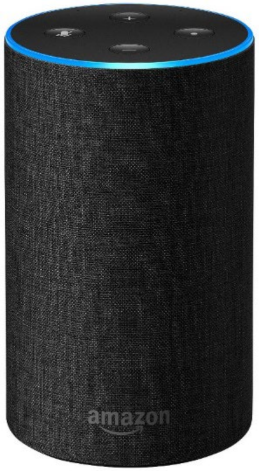


netsparker
web application security scanner

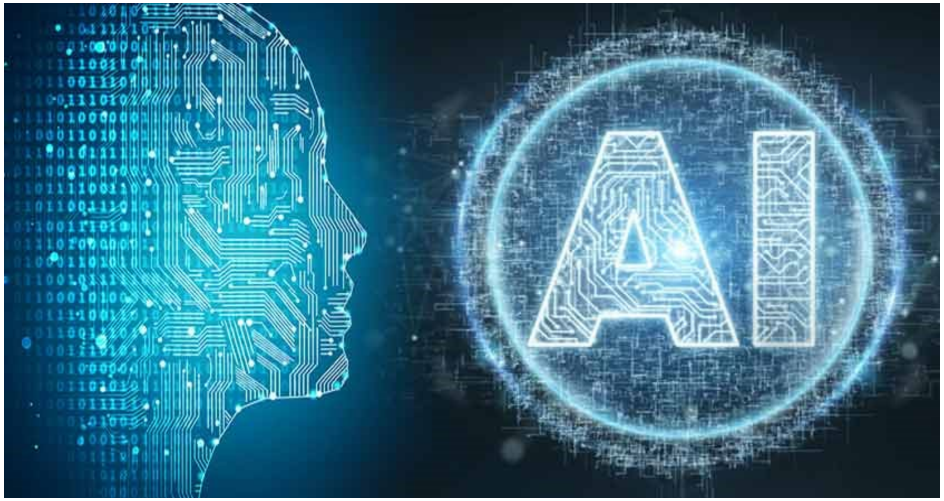
w3af
Web Application Attack and Audit Framework

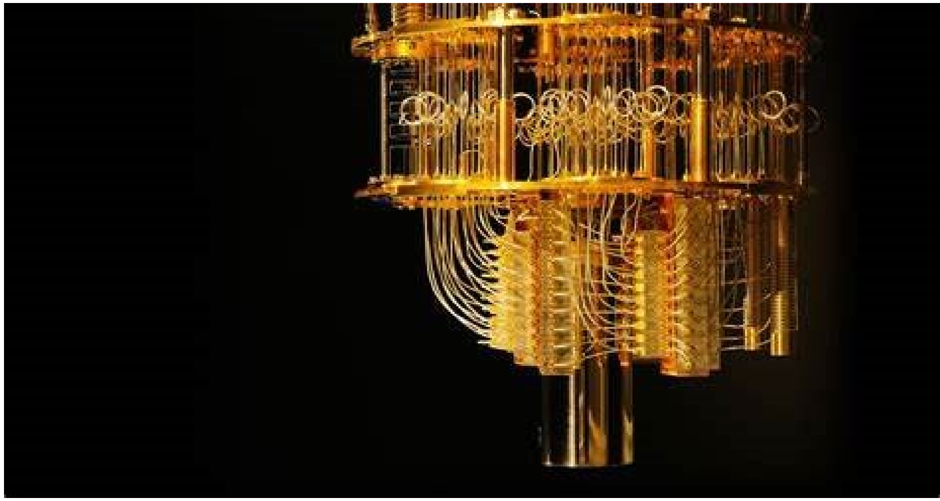
AIRCRACK-NG

Against an Expanding Attack Surface



Future Technology





Final Technology

CISA Resources

CISA provides more than 40 cybersecurity tools and resources for public and private sector stakeholders,

Visit: https://www.cisa.gov

Cybersecurity Advisor Program

In support of the CISA mission, Cybersecurity Advisors:

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

Protective Security Advisors

- Protective Security Advisors (PSA) have five mission areas that directly support the protection of critical infrastructure:
  - Plan, coordinate, and conduct security surveys and assessments
  - Plan and conduct outreach activities
  - Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) events
  - Respond to incidents
  - Coordinate and support improvised explosive device awareness and risk mitigation training

Sampling of Cybersecurity Offerings

- **Preparedness Activities**
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Known Exploited Vulnerability Catalog
  - Information Products and Recommended Practices
  - Cybersecurity Evaluations
    - Cyber Resilience Reviews (CRR™)
    - Cyber Infrastructure Surveys
    - Phishing Campaign Assessment
    - Vulnerability Scanning
    - Risk and Vulnerability Assessments (aka “Pen” Tests)
    - External Dependency Management Reviews
    - Cyber Security Evaluation Tool (CSET™)
    - Validated Architecture Design Review (VADR)

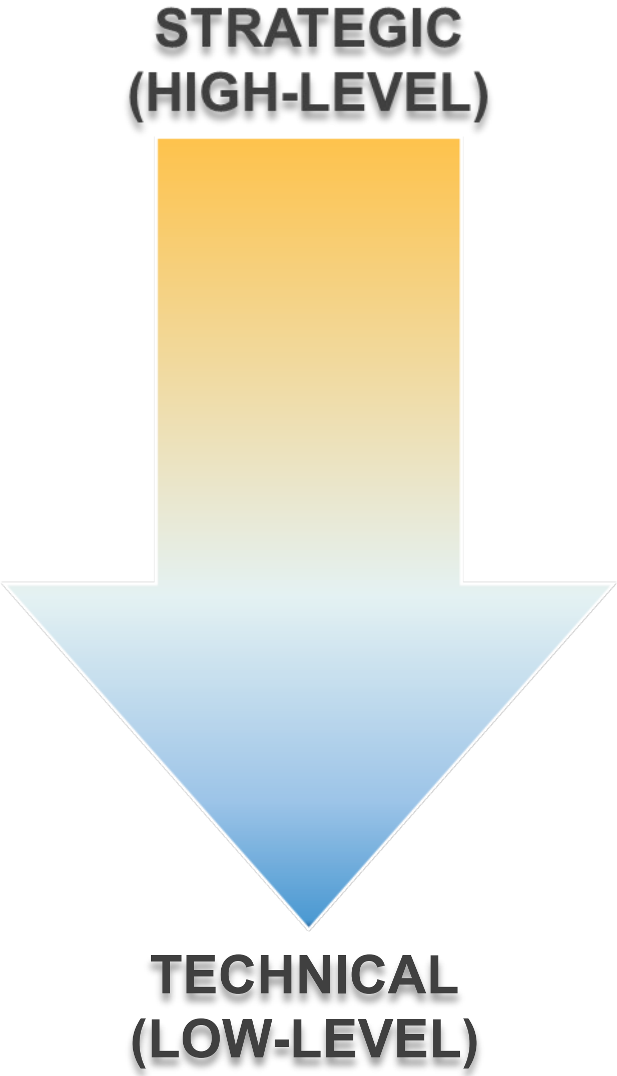
- **Response Assistance**
  - Remote / On-Site Assistance
  - Malware Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination

- **Cybersecurity Advisors**
  - Assessments
  - Working group collaboration
  - Best Practices private-public
  - Incident assistance coordination

- **Protective Security Advisors**
  - Assessments
  - Incident liaisons between government and private sector
  - Support for National Special Security Events

Range of Cybersecurity Assessments

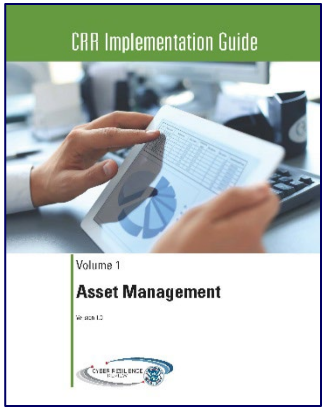
- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Phishing Campaign Assessment (PCA)
- Cyber Tabletop Exercises (CTTX)
- Vulnerability Scanning Service (VSS)
- Web Application Scanning (WAS)
- Remote Penetration Test (RPT)
- Risk & Vulnerability Assessment (RVA)
- Red Team Assessment (RTA)



STRATEGIC (HIGH-LEVEL)

TECHNICAL (LOW-LEVEL)

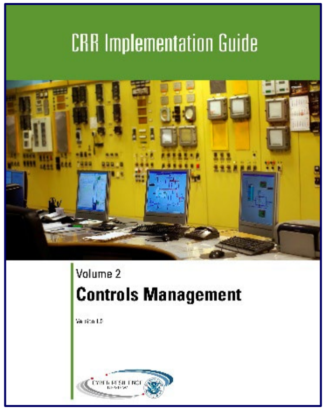
Available Resource Guides


CRR Implementation Guide

Volume 1

Asset Management

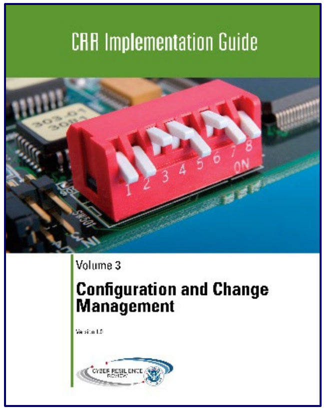
Version 1.0


CRR Implementation Guide

Volume 2

Controls Management

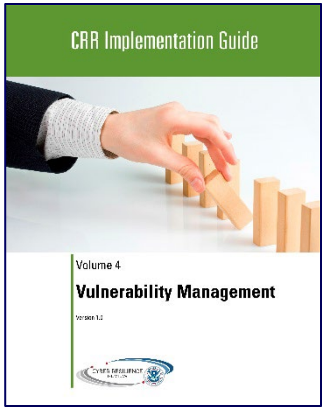
Version 1.0


CRR Implementation Guide

Volume 3

Configuration and Change Management

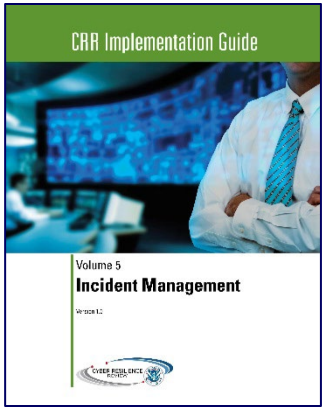
Version 1.0


CRR Implementation Guide

Volume 4

Vulnerability Management

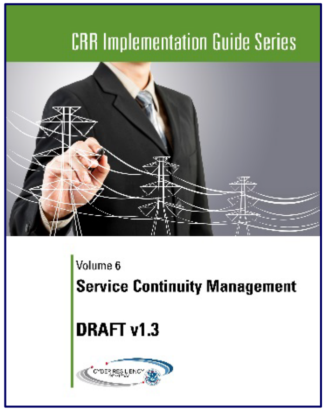
Version 1.0


CRR Implementation Guide

Volume 5

Incident Management

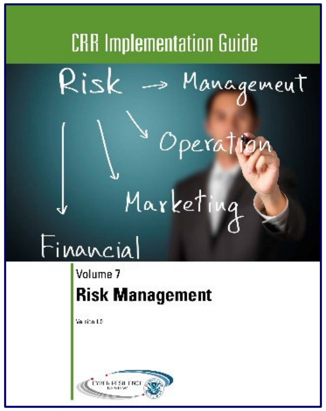
Version 1.0


CRR Implementation Guide Series

Volume 6

Service Continuity Management

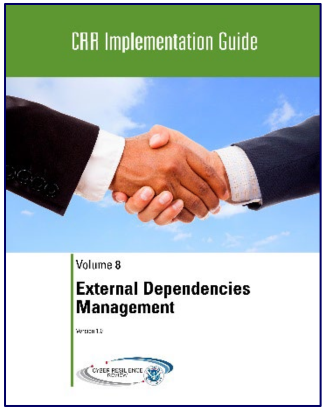
DRAFT v1.3


CRR Implementation Guide

Volume 7

Risk Management

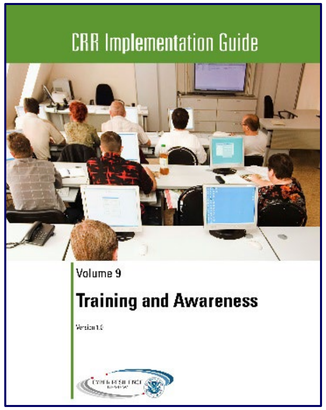
Version 1.0


CRR Implementation Guide

Volume 8

External Dependencies Management

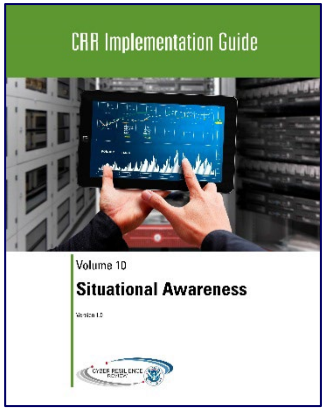
Version 1.0


CRR Implementation Guide

Volume 9

Training and Awareness

Version 1.0


CRR Implementation Guide

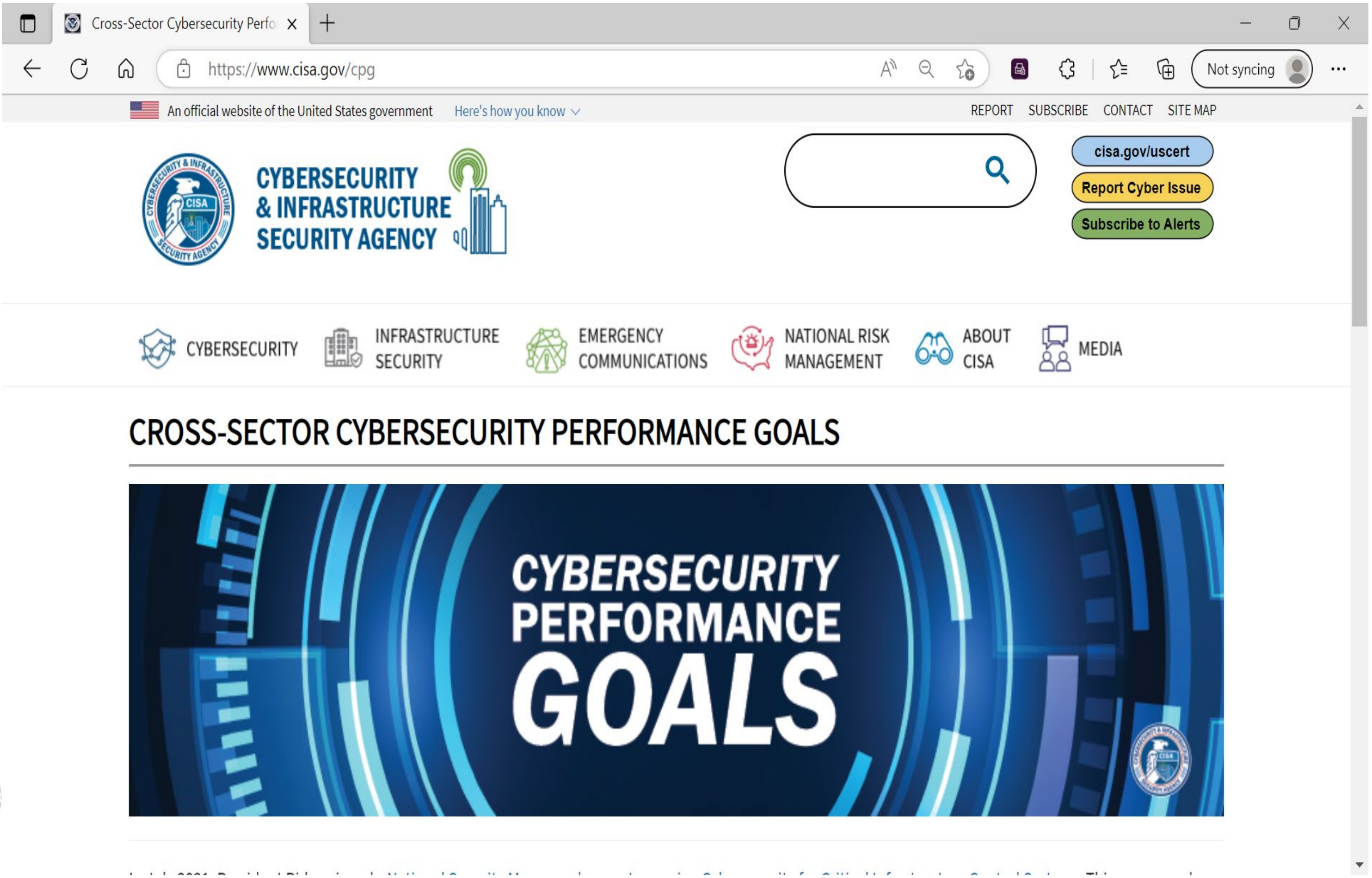
Volume 10

Situational Awareness

Version 1.0

Cybersecurity Performance Goals

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



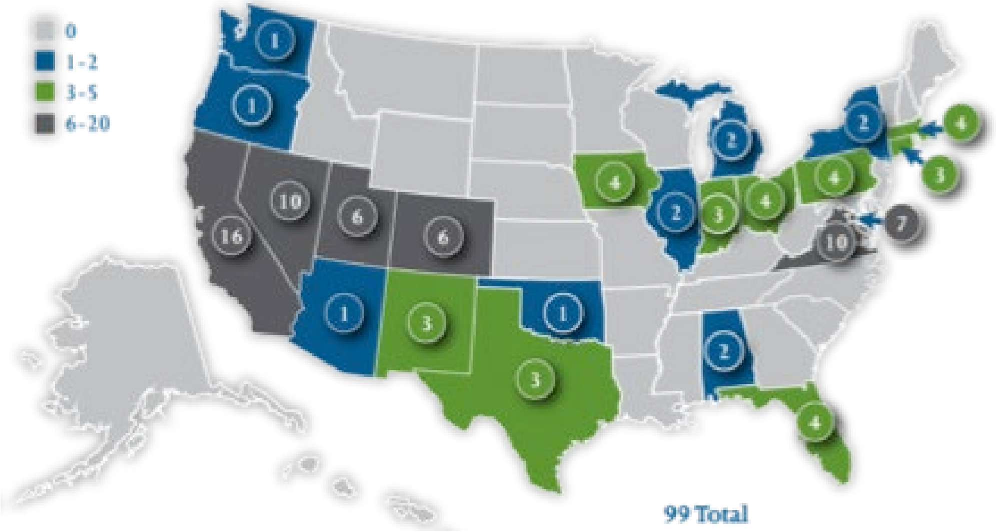
CROSS-SECTOR CYBERSECURITY PERFORMANCE GOALS

CYBERSECURITY PERFORMANCE GOALS

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

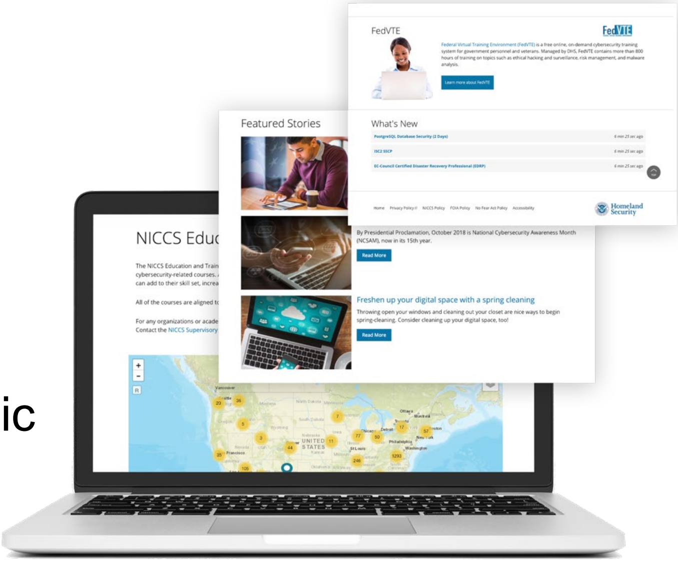


Cybersecurity Training Resources

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



FedVTE

Federal Virtual Training Environment (FedVTE) is a free online, on-demand cybersecurity training system for government personnel and veterans. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis.

What's New

PostgreSQL Database Security (2 Days)	6 min 25 sec ago
ISC2 SSCP	6 min 25 sec ago
EC-Council Certified Disaster Recovery Professional (EDRP)	6 min 25 sec ago

Featured Stories

By Presidential Proclamation, October 2018 is National Cybersecurity Awareness Month (NCSAM), now in its 15th year.

Freshen up your digital space with a spring cleaning

Throwing open your windows and cleaning out your closet are nice ways to begin spring-cleaning. Consider cleaning up your digital space, too!

NICCS Educ

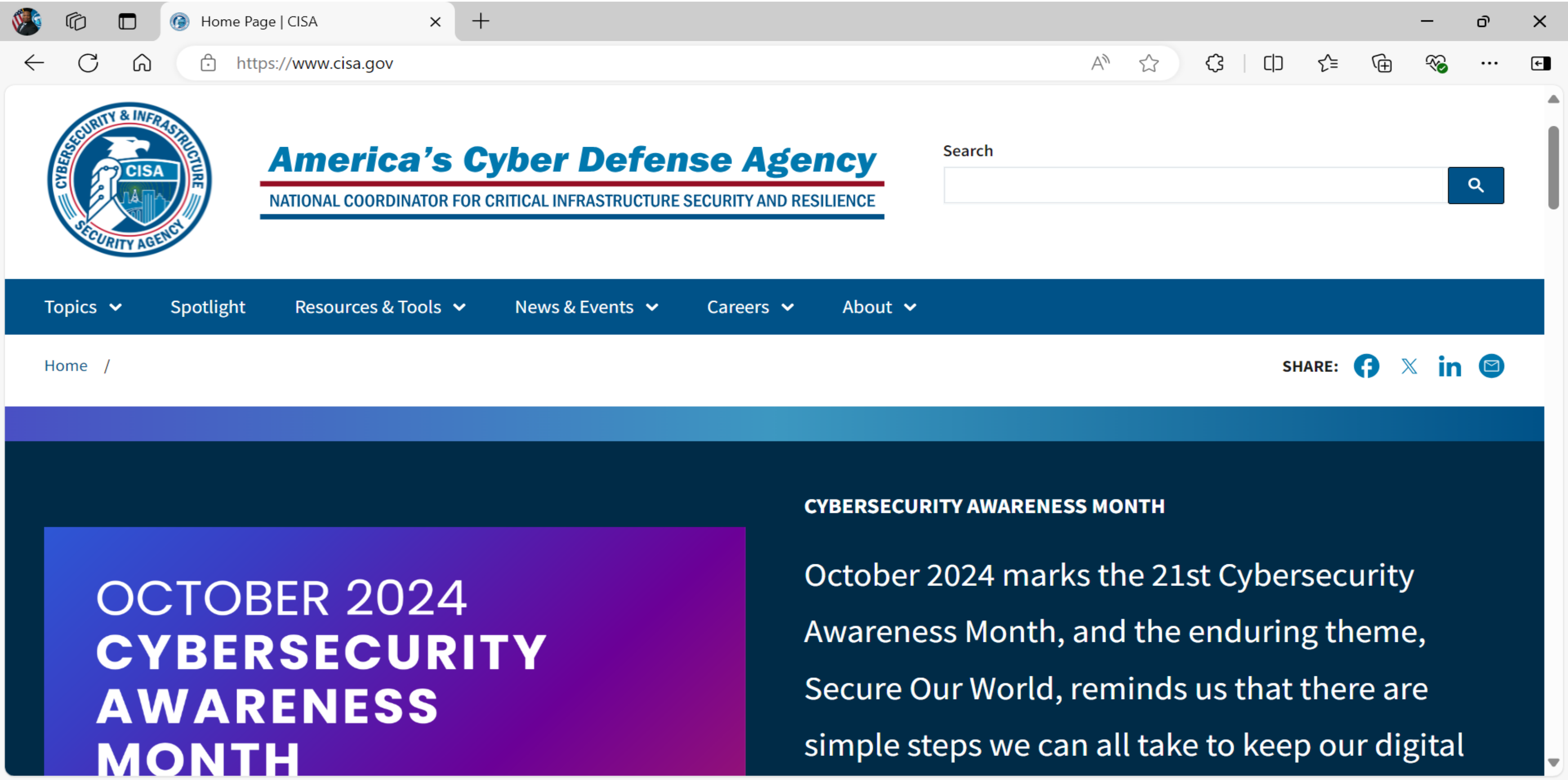
The NICCS Education and Train
cybersecurity-related courses. A
can add to their skill set, increa

All of the courses are aligned to

For any organizations or acade
Contact the NICCS Supervisory

For more information, visit Cybersecurity Training & Exercises | CISA

CISA.GOV



Home Page | CISA

https://www.cisa.gov

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home /

SHARE:

OCTOBER 2024 CYBERSECURITY AWARENESS MONTH

CYBERSECURITY AWARENESS MONTH

October 2024 marks the 21st Cybersecurity Awareness Month, and the enduring theme, Secure Our World, reminds us that there are simple steps we can all take to keep our digital

Visit: https://www.cisa.gov

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Questions? Next Steps?

Contact your local Cybersecurity Advisor!

Giovanni Williams
Supervisory Cybersecurity Advisor, Region 4
Alabama | Florida | Georgia | Kentucky | Mississippi | North Carolina | South Carolina | Tennessee
Cybersecurity and Infrastructure Security Agency
202.503.5614
giovanni.williams@cisa.dhs.gov