CYBER INCIDENT DETECTION

RESOURCES FOR SMALL AND MIDSIZE BUSINESSES

Nebraska Tourism Conference
October 22, 2019

CISA
CYBER+INFRASTRUCTURE

Greg Hollingsead
October 21, 2019

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

Lead the Nation’s efforts to understand and manage risk to our critical infrastructure.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

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

CORE COMPETENCIES

Partnership Development

CISA fosters collaborative partnerships that enable partners in the government and private sector to make informed and voluntary risk management decisions and investments.

Every day, CISA employees: Share information with critical infrastructure partners and stakeholder and serve as the national hub for cybersecurity and communications information data sharing in near-real-time.

Sector outreach: CISA works with government officials and critical infrastructure stakeholders to plan, develop and facilitate exercises that build capacity, improve security and bolster resilience.

CORE COMPETENCIES

Information and Data Sharing

Each and every day, CISA shares information with critical infrastructure partners and stakeholders and serves as the national hub for cybersecurity and communications information and data sharing in near real-time.

CISA performs a suite of functions that provide customers with comprehensive risk management capabilities, products, and services. These functions include:

- Information Sharing
- Risk & Vulnerability Assessments
- Watch Floor Operation
- Operational Planning, Training, & Exercises
- Data Synthesis & Analysis

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

The Reality of Cyber Attacks

- All businesses, regardless of size, are at risk. Small businesses may feel like they are not targets for cyber attacks either due to their size or the perception that they don't have anything worth stealing.
- Only a small percentage of cyber attacks are considered targeted attacks, meaning the attacker group is going after a particular company or group of companies in order to steal specific data.
- The majority of cyber criminals are indiscriminate; they target vulnerable computer systems regardless of whether the systems are part of a Fortune 500 company, a small business, or belong to a home user.

Small Business Cyber Attacks

Small businesses, which are making the leap to computerized systems and digital records, are attractive targets for hackers.

- Small businesses store significant amounts of sensitive data from customer information to intellectual property.
- While large businesses can dedicate resources to cybersecurity, small businesses face the same cybersecurity challenges and threats with limited resources, capacity, and personnel.
- In 2018, the U.S. Secret Service and Verizon Communications Inc.'s forensic analysis unit, which investigates attacks, responded to a combined 1024 data breaches, up from 321 in 20017. Of those, 76 percent were at companies with 100 employees or fewer.
- Visa estimates about 95 percent of the credit-card data breaches it discovers are on its smallest business customers.

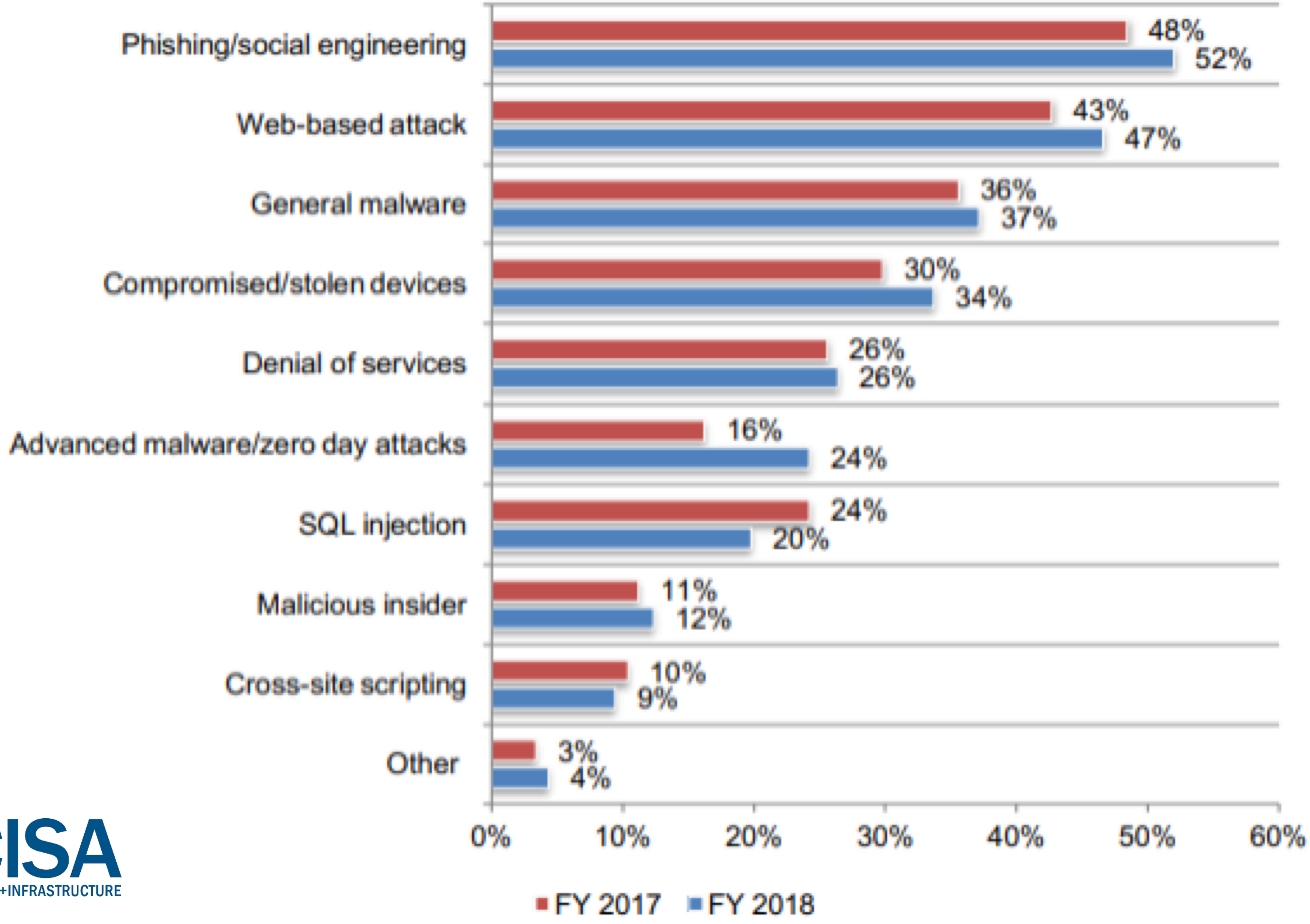
The Importance of (Quick) Detection

Every organization is a potential target, *regardless of size.*
Risks include:

- Data compromise or loss
- Weakened trust
- Costly recovery
- Business failure – 60% of SMBs within 6 months.

*U.S. companies take an average of **206 days** to detect a data breach.*

Common Types of Attack



Source: Ponemon Institute

CISA
CYBER+INFRASTRUCTURE

Cyber Tips For Your Busines

- ***Assess risk and identify weaknesses*** – If your sensitive information is linked to the Internet, then make sure you understand how it's being protected.
- ***Create a incident response and disaster recovery plan*** – Establish security practices and policies to protect your organization's sensitive information and its employees, patrons, and stakeholders.
- ***Educate employees*** – Make sure that employees are routinely educated about new and emerging cyber threats and how to protect your organization's data. Hold them accountable to the Internet security policies and procedures, and require that they use strong passwords and regularly change them. https://NICCS.us-cert.gov

Cyber Tips For Your Busines

- ***Back up critical information*** – Establish a schedule to perform critical data backups to ensure that critical data is not lost in the event of a cyber attack or natural disaster. Store all backups in remote locations away from the office, and encrypt sensitive data about the organization and its customers. Invest in data loss protection software and use two-factor authentication where possible.
- ***Secure your Internet connection*** – Use and regularly update antivirus software and antispyware on all computers. Automate patch deployments across your organization, utilize a firewall, encrypt data in transit, and secure your Wi-Fi network. Protect all pages on your public-facing websites.

Cyber Tips For Your Busines

Nearly 59 percent of U.S. small and medium-sized businesses do not have a contingency plan that outlines procedures for responding to and reporting data breach losses.

- ***Create a business continuity plan*** – A continuity plan ensures that of nature, accidents, and technological or attack-related emergencies. Business functions can continue to be performed during a wide range of emergencies, including localized acts templates for this type of plan at http://www.fema.gov/planning-templates.

Pre-Incident Cybersecurity Planning

Before a breach occurs, you should:

- Publish employee cybersecurity policies and a cyber incident response plan
- Assemble a Cyber Incident Response Team
- Understand your legal obligations
- Train your staff
- Know how you will (likely) respond

Understand Legal Obligations

- Data security and/or privacy obligations?
- Notification obligations?

Building Your Cyber Response Team

- Who will be in charge?

- What kinds of expertise will you need?

Responding To A Cyber Incident Impacting Your Business

Greg Hollingsead
October 21, 2019

Secure Your Operations

As soon as you learn of the breach,

- *Mobilize* your response team
- *Understand* where and how the breach occurred
- *Act* immediately to prevent further data loss
- *Preserve* evidence of the breach

Ransomware Attack

Actions for Today – Make Sure You're Not Tomorrow's Headline:

- Backup your data, system images, and configurations and keep the backups offline
- Update and patch systems
- Make sure your security solutions are up to date
- Review and exercise your cyber incident response plan
- Pay attention to ransomware events and apply lessons learned

CISA
CYBER+INFRASTRUCTURE

Ransomware Attack

Actions to Recover If Impacted – Don't Let a Bad Day Get Worse:

- Ask for help! Contact CISA, the FBI, or the Secret Service
- Work with an experienced advisor to help recover from a cyber attack
- Isolate the infected systems and phase your return to operations
- Review the connections of any business relationships (customers, partners, vendors) that touch your network
- Apply business impact assessment findings to prioritize recovery

NCCIC Cyber Incident Reporting

- NCCIC provides real-time threat analysis and incident reporting capabilities
  - 24x7 contact number: 1-888-282-0870 https://forms.us-cert.gov/report/

- **When to report**:
  - If there is a suspected or confirmed cyber attack or incident that:
    - Affects core government or critical infrastructure functions
    - Results in the loss of data, system availability, or control of systems
    - Indicates malicious software is present on critical systems

- **Malware Submission Process**:

- Please send all submissions to the Advance Malware Analysis Center (AMAC) at: submit@malware.us-cert.gov
  - Must be provided in password-protected zip files using password “infected”
  - Web-submission: https://malware.us-cert.gov

CISA
CYBER+INFRASTRUCTURE

Secure Your Environment Going Forward

Don’t Let Yourself be an Easy Mark:

- Practice good cyber hygiene; backup, update, whitelist apps, limit privilege, and use multifactor authentication
- Segment your networks; make it hard for the bad guy to move around and infect multiple systems
- Develop containment strategies; if bad guys get in, make it hard for them to get stuff out
- Know your system’s baseline for recovery
- Review disaster recovery procedures and validate goals with executives

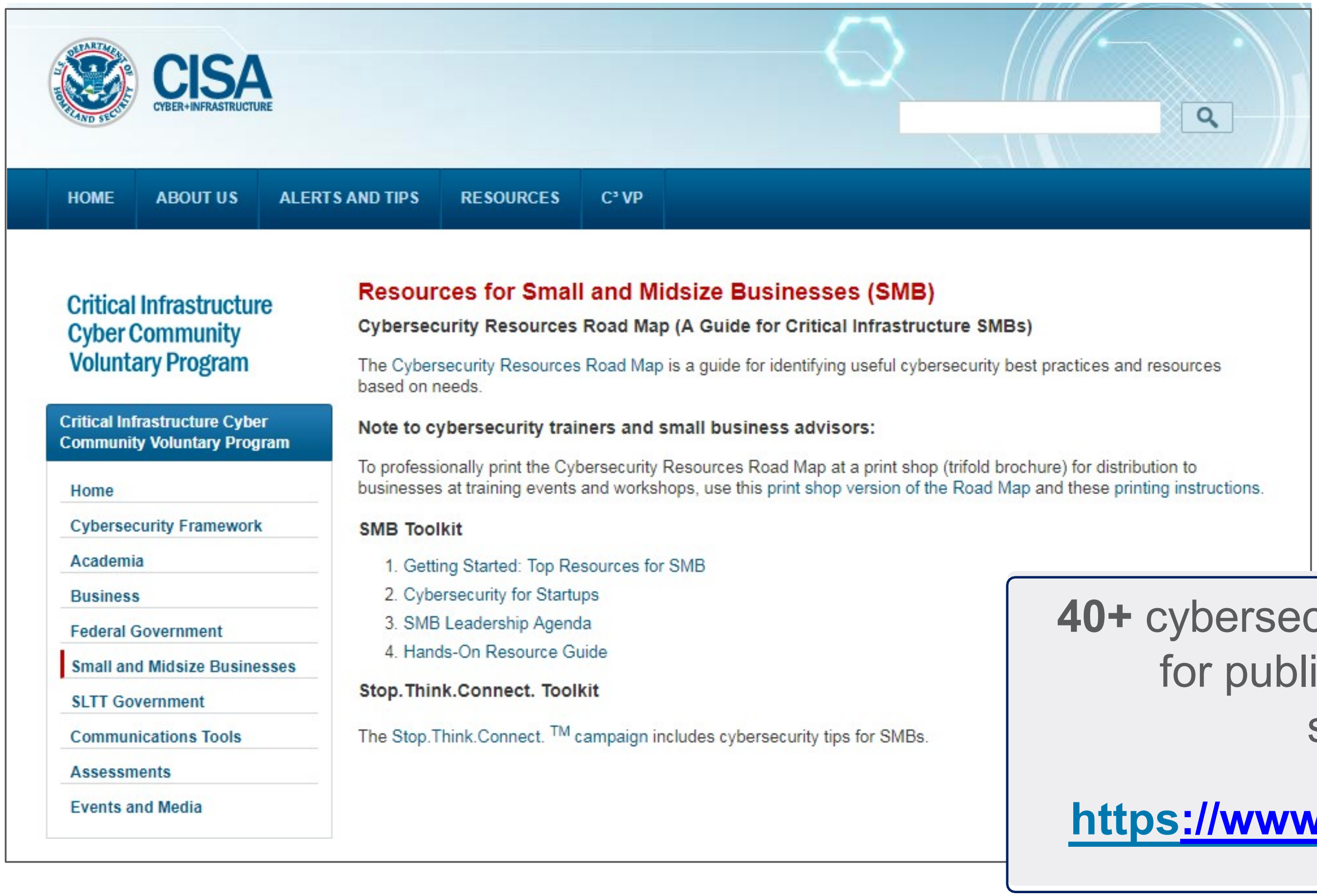
Cyber Information Sharing

Where can you get your "news?"

- Industry associations
- Information Sharing and Analysis Centers (ISACs)
- Information Sharing and Analysis Organizations (ISAOs)
- National Cyber Awareness System (NCAS)

Learn more: https://www.dhs.gov/cisa/information-sharing-and-awareness

CISA Website



Critical Infrastructure Cyber Community Voluntary Program

Critical Infrastructure Cyber Community Voluntary Program

- Home
- Cybersecurity Framework
- Academia
- Business
- Federal Government
- Small and Midsize Businesses
- SLTT Government
- Communications Tools
- Assessments
- Events and Media

Resources for Small and Midsize Businesses (SMB)

Cybersecurity Resources Road Map (A Guide for Critical Infrastructure SMBs)

The Cybersecurity Resources Road Map is a guide for identifying useful cybersecurity best practices and resources based on needs.

Note to cybersecurity trainers and small business advisors:

To professionally print the Cybersecurity Resources Road Map at a print shop (trifold brochure) for distribution to businesses at training events and workshops, use this print shop version of the Road Map and these printing instructions.

SMB Toolkit

1. Getting Started: Top Resources for SMB
2. Cybersecurity for Startups
3. SMB Leadership Agenda
4. Hands-On Resource Guide

Stop.Think.Connect. Toolkit

The Stop.Think.Connect. TM campaign includes cybersecurity tips for SMBs.

40+ cybersecurity tools and resources for public and private sector stakeholders

https://www.us-cert.gov/ccubedvp

CISA
CYBER+INFRASTRUCTURE

Greg Hollingsead
October 21, 2019

Cybersecurity Resources Road Map

Goals:

- Make it easy to identify and access useful resources based on need
- Encourage stakeholders to elevate their efforts toward a more holistic risk management approach

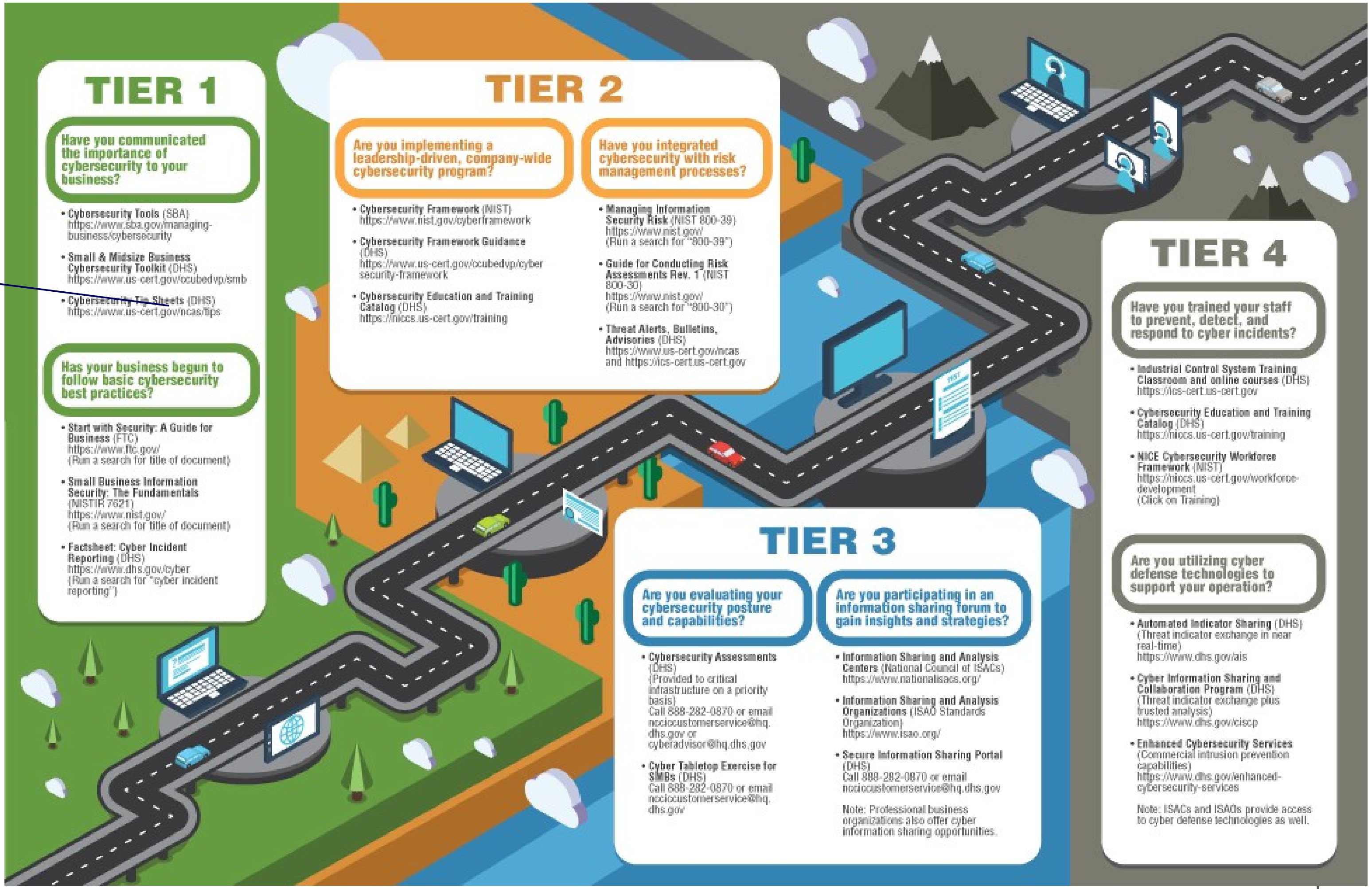
https://www.us-cert.gov/ccubedvp/smb

ABOUT THIS GUIDE
ADDITIONAL RESOURCES
CYBERSECURITY RESOURCES ROAD MAP
A GUIDE FOR CRITICAL INFRASTRUCTURE
SMALL AND MIDSIZE BUSINESSES
TIER 1
Have you communicated the importance of cybersecurity to your business?
Has your business begun to follow basic cybersecurity best practices?
TIER 2
Are you implementing a leadership-driven, company-wide cybersecurity program?
Have you integrated cybersecurity with risk management processes?
TIER 3
Are you evaluating your cybersecurity posture and capabilities?
Are you participating in an information sharing forum to gain insights and strategies?
TIER 4
Have you trained your staff to prevent, detect, and respond to cyber incidents?
Are you utilizing cyber defense technologies to support your operation?

Cybersecurity Resources Road Map

NCAS Cybersecurity Tip Sheets

https://www.us-cert.gov/ncas/tips



TIER 1

Have you communicated the importance of cybersecurity to your business?

- **Cybersecurity Tools** (SBA) https://www.sba.gov/managing-business/cybersecurity
- **Small & Midsize Business Cybersecurity Toolkit** (DHS) https://www.us-cert.gov/ccubedvp/smb
- **Cybersecurity Tip Sheets** (DHS) https://www.us-cert.gov/ncas/tips

Has your business begun to follow basic cybersecurity best practices?

- **Start with Security: A Guide for Business** (FTC) https://www.ftc.gov/ (Run a search for title of document)
- **Small Business Information Security: The Fundamentals** (NISTIR 7621) https://www.nist.gov/ (Run a search for title of document)
- **Factsheet: Cyber Incident Reporting** (DHS) https://www.dhs.gov/cyber (Run a search for "cyber incident reporting")

TIER 2

Are you implementing a leadership-driven, company-wide cybersecurity program?

- **Cybersecurity Framework** (NIST) https://www.nist.gov/cyberframework
- **Cybersecurity Framework Guidance** (DHS) https://www.us-cert.gov/ccubedvp/cybersecurity-framework
- **Cybersecurity Education and Training Catalog** (DHS) https://niccs.us-cert.gov/training

Have you integrated cybersecurity with risk management processes?

- **Managing Information Security Risk** (NIST 800-39) https://www.nist.gov/ (Run a search for "800-39")
- **Guide for Conducting Risk Assessments Rev. 1** (NIST 800-30) https://www.nist.gov/ (Run a search for "800-30")
- **Threat Alerts, Bulletins, Advisories** (DHS) https://www.us-cert.gov/ncas and https://ics-cert.us-cert.gov

TIER 3

Are you evaluating your cybersecurity posture and capabilities?

- **Cybersecurity Assessments** (DHS) (Provided to critical infrastructure on a priority basis) Call 888-282-0870 or email ncciocustomerservice@hq.dhs.gov or cyberadvisor@hq.dhs.gov
- **Cyber Tabletop Exercise for SMBs** (DHS) Call 888-282-0870 or email ncciocustomerservice@hq.dhs.gov

Are you participating in an information sharing forum to gain insights and strategies?

- **Information Sharing and Analysis Centers** (National Council of ISACs) https://www.nationalisacs.org/
- **Information Sharing and Analysis Organizations** (ISAO Standards Organization) https://www.isao.org/
- **Secure Information Sharing Portal** (DHS) Call 888-282-0870 or email ncciocustomerservice@hq.dhs.gov

Note: Professional business organizations also offer cyber information sharing opportunities.

TIER 4

Have you trained your staff to prevent, detect, and respond to cyber incidents?

- **Industrial Control System Training Classroom and online courses** (DHS) https://ics-cert.us-cert.gov
- **Cybersecurity Education and Training Catalog** (DHS) https://niccs.us-cert.gov/training
- **NICE Cybersecurity Workforce Framework** (NIST) https://niccs.us-cert.gov/workforce-development (Click on Training)

Are you utilizing cyber defense technologies to support your operation?

- **Automated Indicator Sharing** (DHS) (Threat indicator exchange in near real-time) https://www.dhs.gov/ais
- **Cyber Information Sharing and Collaboration Program** (DHS) (Threat indicator exchange plus trusted analysis) https://www.dhs.gov/ciscp
- **Enhanced Cybersecurity Services** (Commercial intrusion prevention capabilities) https://www.dhs.gov/enhanced-cybersecurity-services

Note: ISACs and ISAOs provide access to cyber defense technologies as well.

CISA Webinars

Webinars on resources, best practices, and emerging threats, such as:

- *Russian Activity Against Critical Infrastructure*
- *Chinese Cyber Activity Targeting Managed Service Providers*
- *Combating Ransomware*
- *Cybersecurity Framework Use Cases among SMBs*
- *Creating a Culture of Cybersecurity at Work*

National Cybersecurity & Communications Integration Center (NCCIC)
AWARENESS BRIEFINGS
Cybersecurity and Infrastructure Security Agency (CISA)
AWARENESS BRIEFINGS
CHINESE CYBER ACTIVITY TARGETING MANAGED SERVICE PROVIDERS

The National Initiative for Cybersecurity Careers and Studies (NICCS)

Nation’s One Stop Shop for Cybersecurity Careers and Studies!

The National Initiative for Cybersecurity Careers and Studies (NICCS) is a national resource for cybersecurity awareness, education, training, and career opportunities.

https://niccs.us-cert.gov/

Training

- NICCS Training Catalog
- FedVTE

Workforce Framework

- NICE Cybersecurity Workforce Framework

Education

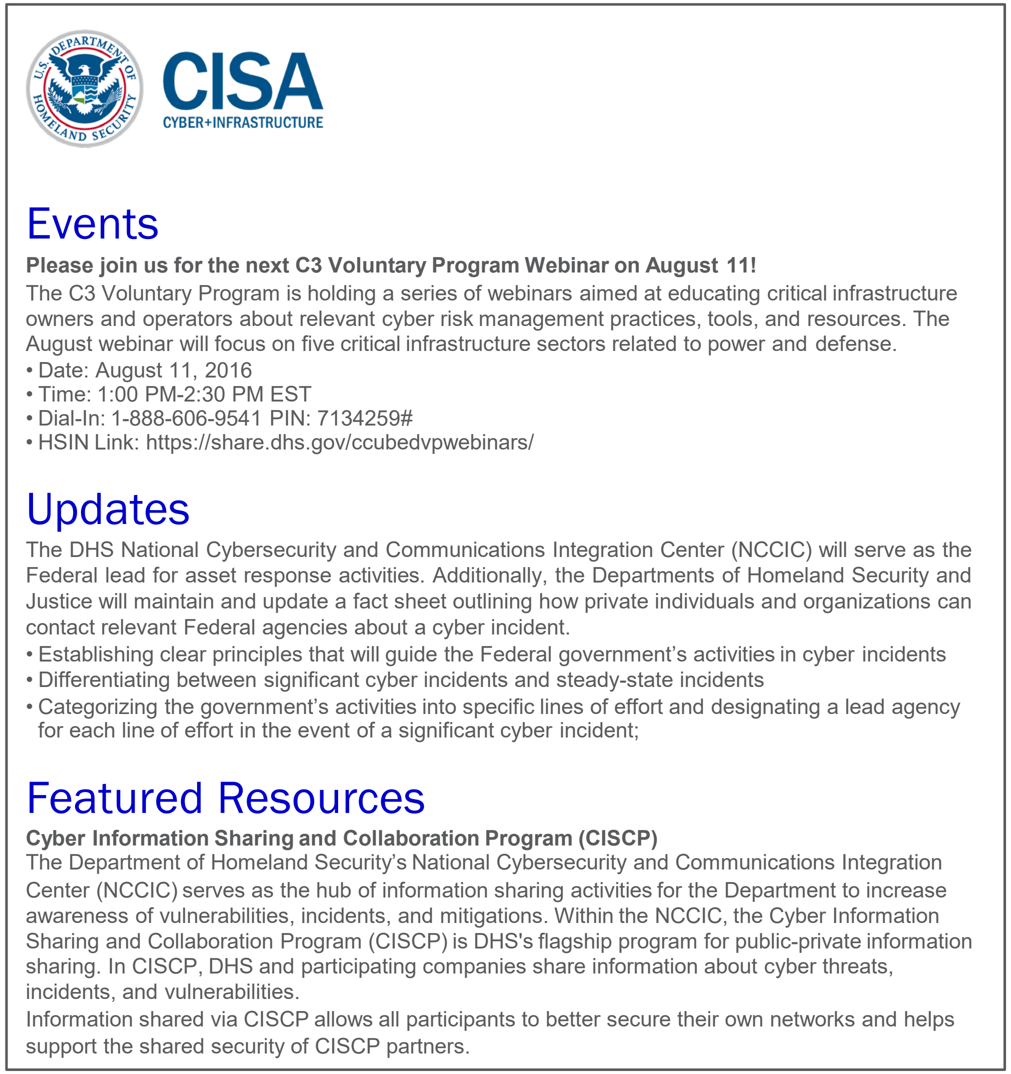
- K-12 Cybersecurity Curricula
- Designated institutions with top cybersecurity programs
- Cybersecurity scholarships

CISA Cybersecurity Community Bulletin

- Featuring:
- Upcoming Events
- Program Updates
- Featured Resources
- Partner Spotlight
- Social Media Toolkit

https://www.us-cert.gov/ccubedvp

Subscribe to Alerts



Events

Please join us for the next C3 Voluntary Program Webinar on August 11!

The C3 Voluntary Program is holding a series of webinars aimed at educating critical infrastructure owners and operators about relevant cyber risk management practices, tools, and resources. The August webinar will focus on five critical infrastructure sectors related to power and defense.

- Date: August 11, 2016
- Time: 1:00 PM-2:30 PM EST
- Dial-In: 1-888-606-9541 PIN: 7134259#
- HSIN Link: https://share.dhs.gov/ccubedvpwebinars/

Updates

The DHS National Cybersecurity and Communications Integration Center (NCCIC) will serve as the Federal lead for asset response activities. Additionally, the Departments of Homeland Security and Justice will maintain and update a fact sheet outlining how private individuals and organizations can contact relevant Federal agencies about a cyber incident.

- Establishing clear principles that will guide the Federal government's activities in cyber incidents
- Differentiating between significant cyber incidents and steady-state incidents
- Categorizing the government's activities into specific lines of effort and designating a lead agency for each line of effort in the event of a significant cyber incident;

Featured Resources

Cyber Information Sharing and Collaboration Program (CISCP)

The Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) serves as the hub of information sharing activities for the Department to increase awareness of vulnerabilities, incidents, and mitigations. Within the NCCIC, the Cyber Information Sharing and Collaboration Program (CISCP) is DHS's flagship program for public-private information sharing. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities.

Information shared via CISCP allows all participants to better secure their own networks and helps support the shared security of CISCP partners.

Partner Websites

- NIST: https://www.nist.gov/itl/smallbusinesscyber
- SBA: https://www.sba.gov/managing-business/cybersecurity
- FTC: https://www.ftc.gov/tips-advice/business-center/small-busines
- NCSA: https://staysafeonline.org/cybersecure-business/detect-incidents/

For more information:
https://www.cisa.gov

Contact the NCCIC:
Email: NCCIC@hq.dhs.gov
Phone: (888) 282-0870