

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Tony Enriquez
Cybersecurity Advisor
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

June 23, 2020



CISA
CYBER+INFRASTRUCTURE

The Nation's Risk Advisors

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure



CISA
CYBER+INFRASTRUCTURE

CISA

Cybersecurity Advisor Program



CISA
CYBER+INFRASTRUCTURE

Cybersecurity Advisor Program

CISA mission: Lead the Nation's efforts to understand and manage risk to our critical infrastructure.

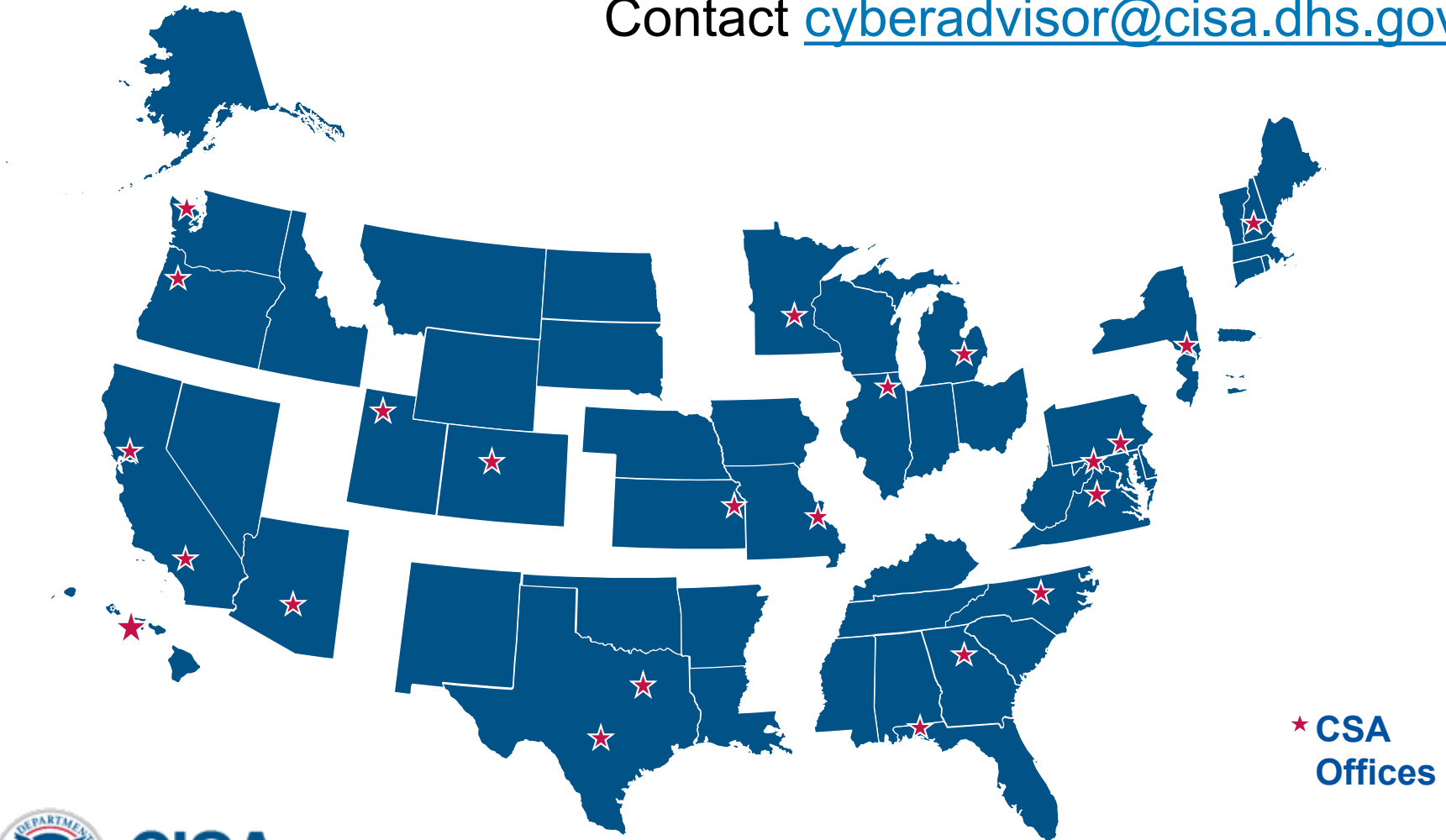
In support of that mission: Cybersecurity Advisors (CSAs):

- **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.



CSA Deployed Personnel

Contact cyberadvisor@cisa.dhs.gov



★ CSA
Offices



CISA
CYBER+INFRASTRUCTURE

Cybersecurity and Resilience



CISA
CYBER+INFRASTRUCTURE

Who is targeting you?

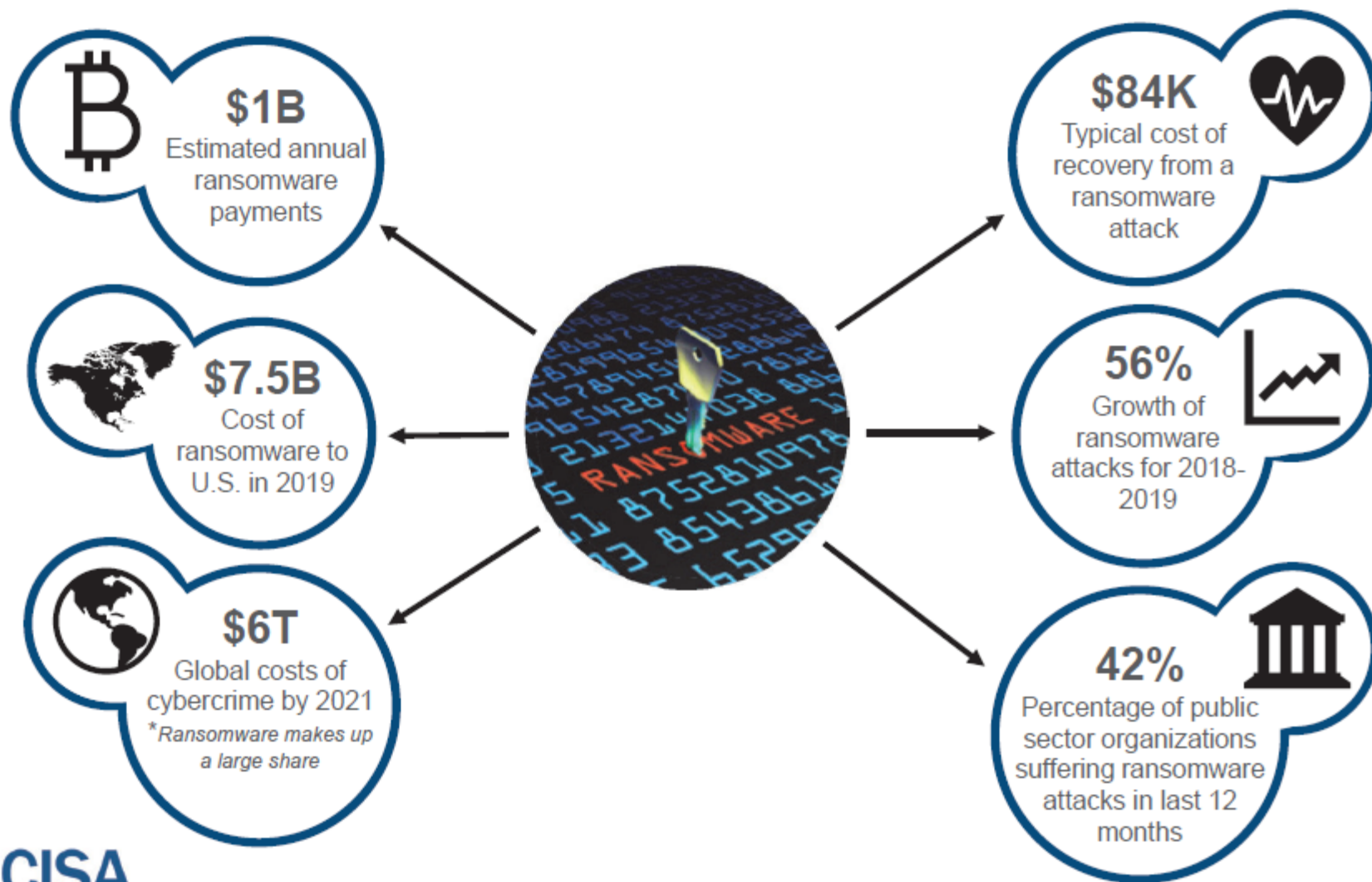


CISA
CYBER+INFRASTRUCTURE

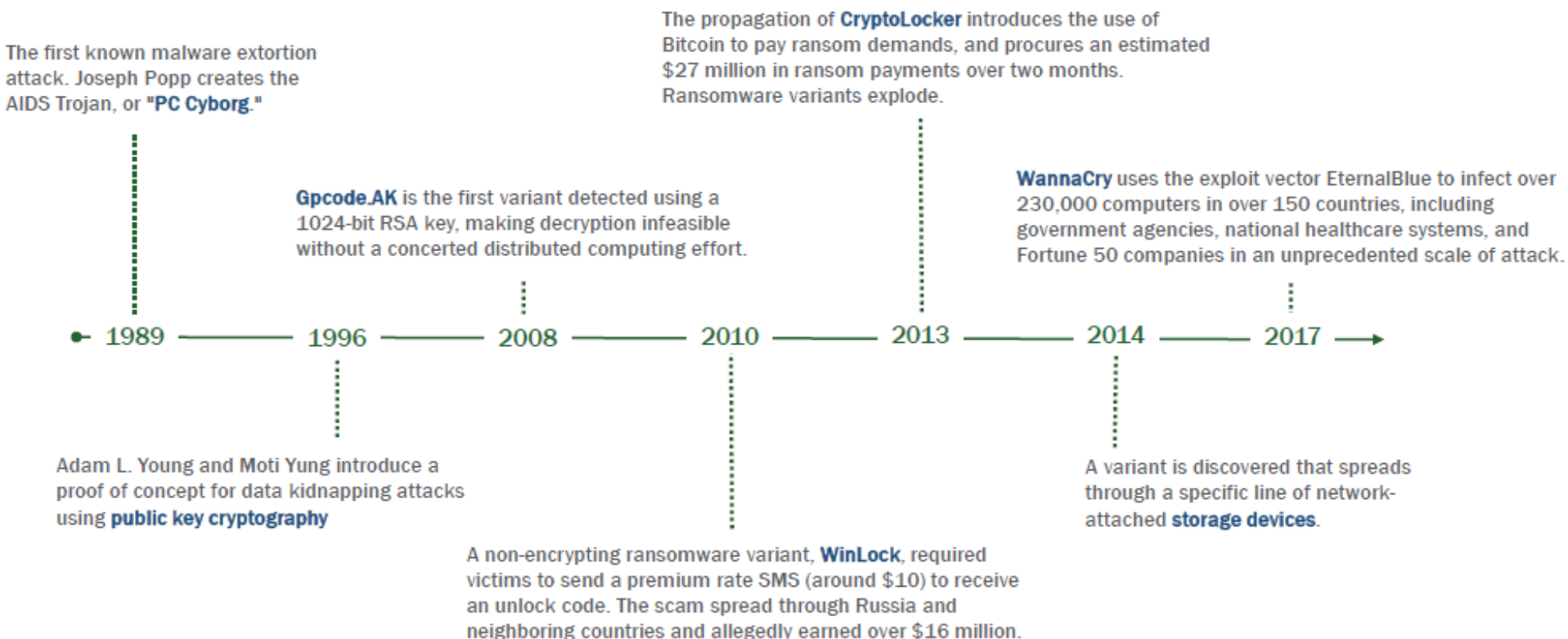
What is Ransomware?

- Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

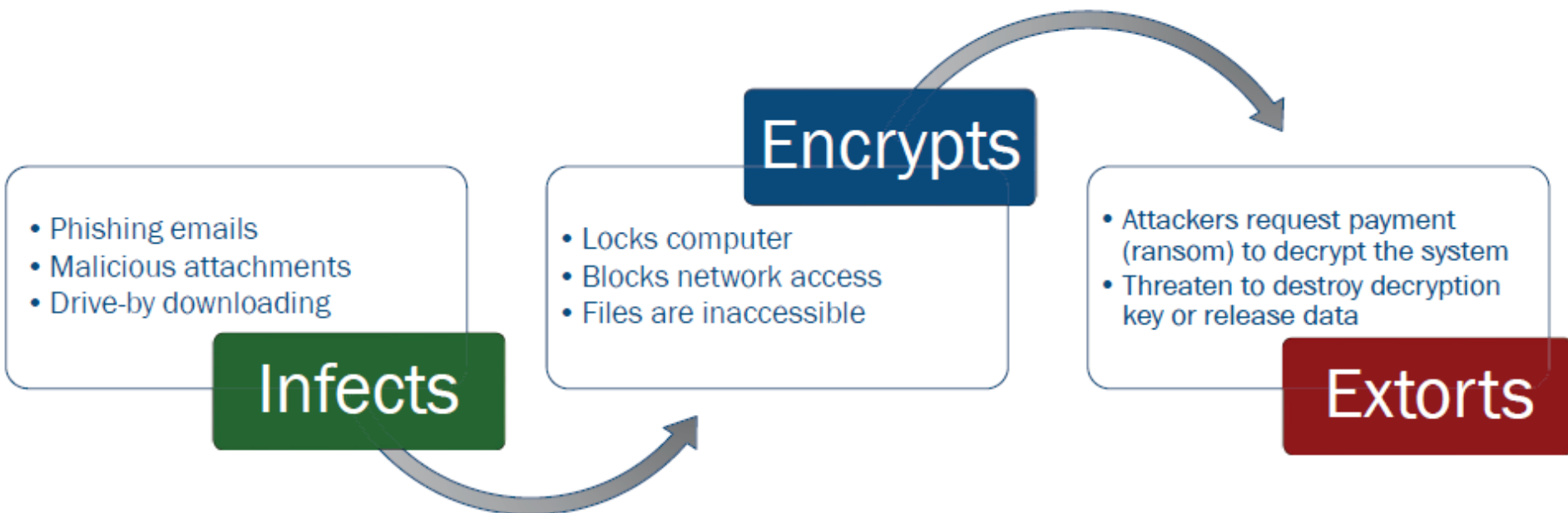
Ransomware by the Numbers



Evolution of Ransomware



Ransomware Patterns of Behavior



What can you do today to defend yourselves?



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

1. Backup your data offline
2. Manage patches
3. Update security solutions
4. Prepare your incident response plan
5. Maintain global situational awareness

**Most
commonly
targeted
sectors**



Education

Government
Agencies



Healthcare

Energy &
Utilities



Retail

Finance



CISA
CYBER+INFRASTRUCTURE

What if become a victim?



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

1. Ask for help!
2. Work with experts
3. Isolate infection
4. Review the connections
5. Prioritize recovery

**Most
commonly
targeted
sectors**



Education

Government
Agencies



Healthcare

Energy &
Utilities



Retail



Finance



CISA
CYBER+INFRASTRUCTURE

August 21, 2019

CISA INSIGHTS

Ransomware Outbreak



Actions to Secure Your Environment Going Forward – Don't Let Yourself be an Easy Mark:

1. Practice good cyber hygiene
2. Segment networks
3. Develop containment strategies
4. Know your system's baseline
5. Review recovery procedures

**Most
commonly
targeted
sectors**



Education

Government
Agencies



Healthcare

Energy &
Utilities



Retail

Finance



CISA
CYBER+INFRASTRUCTURE

Ransomware Resources

<https://www.us-cert.gov/Ransomware>

- Training (Webinar under Training)
- Mitigations
- Best Practices
- Ransomware Alerts

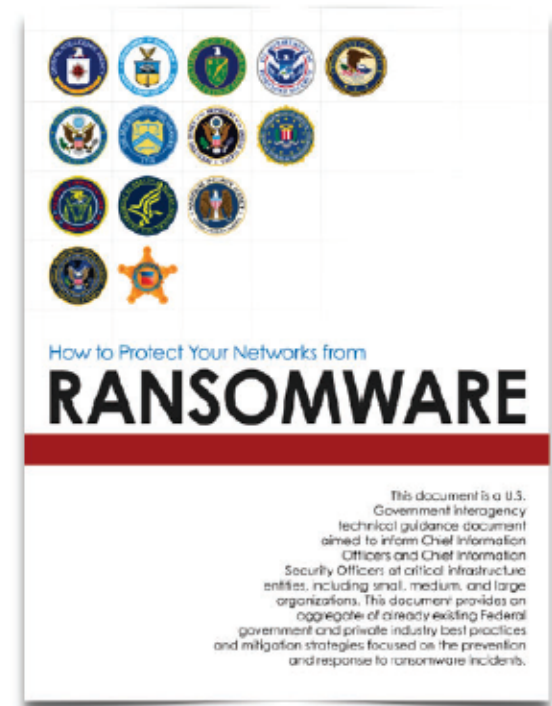
“Don’t Wake Up to a Ransomware Attack” provides essential knowledge to prepare you and your organization to prevent, mitigate, and respond to the ever-growing threat of ransomware attacks.

- This course is specifically designed to be accessible to a non-technical audience including managers and business leaders, as well as provide an organizational perspective and strategic overview useful to technical specialists.

Ransomware Resources

- <https://www.justice.gov/criminal-ccips/file/872771/download>

- Isolate the infected computer immediately
- Isolate or power-off affected devices
- Immediately secure backup data or systems
- Contact law enforcement
- Secure partial portions of the ransomed data that might exist
- Change all online account passwords and network passwords
- Delete Registry values and files



Ransomware Resources

- CISA Security Tip – Protecting Against Ransomware
 - <https://www.us-cert.gov/ncas/tips/ST19-001>
- CISA Webinar – Combating Ransomware
 - <https://www.youtube.com/watch?v=D8kC07tu27A>
- Joint Ransomware Statement
 - https://www.us-cert.gov/sites/default/files/2019-07/Ransomware_Statement_S508C.pdf

Additional Resources



Your success depends on *Cyber Readiness*. Both depend on **YOU**.

THE LEADER'S GUIDE

Reducing your organization's cyber risks requires a holistic approach - similar to the approach you would take to address other operational risks. As with other risks, cyber risks can threaten:



YOUR ABILITY TO OPERATE / ACCESS INFO



YOUR REPUTATION / CUSTOMER TRUST



YOUR BOTTOM LINE



YOUR ORGANIZATION'S SURVIVAL

Managing cyber risks requires building a culture of cyber readiness.

Essential Elements of a Culture of Cyber Readiness:

Yourself

- The Leader

Drive cybersecurity strategy, investment and culture



Your awareness of the basics drives cybersecurity to be a major part of your operational resilience strategy, and that strategy requires an investment of time and money.

Your investment drives actions and activities that build and sustain a culture of cybersecurity.

Your Staff

- The Users

Develop security awareness and vigilance



Your staff will often be your first line of defense, one that must have - and continuously grow - the skills to practice and maintain readiness against cybersecurity risks.

Your Systems

- What Makes You Operational

Protect critical assets and applications



Information is the life-blood of any business; it is often the most valuable of a business' intangible assets.

Know where this information resides, know what applications and networks store and process that information, and build security into and around these.

Your Surroundings

- The Digital Workplace

Ensure only those who belong on your digital workplace have access



The authority and access you grant employees, managers, and customers into your digital environment needs limits, just as those set in the physical work environment do.

Setting approved access privileges requires knowing who operates on your systems and with what level of authorization and accountability.

Your Data

- What the Business is Built On

Make backups and avoid the loss of information critical to operations



Even the best security measures can be circumvented with a patient, sophisticated adversary. Learn to protect your information where it is stored, processed, and transmitted.

Have a contingency plan, which generally starts with being able to recover systems, networks, and data from known, accurate backups.

Your Actions Under Stress

Limit damage and quicken restoration of normal operations



The strategy for responding to and recovering from compromise: plan, prepare for, and conduct drills for cyberattacks as you would a fire. Make your reaction to cyberattacks and system failures an extension of your other business contingency plans.

This requires having established procedures, trained staff, and knowing how - and to whom - to communicate during a crisis.

VOL.1 FALL 2019

[CISA.gov/Cyber-Essentials](https://www.cisa.gov/Cyber-Essentials)

For tech specs on building a Culture of Cyber Readiness, flip page ►



CISA
CYBER+INFRASTRUCTURE

Additional Resources



Backup Data

Employ a backup solution that automatically and continuously backs up critical data and system configurations.



Multi-Factor Authentication

Require multi-factor authentication (MFA) for accessing your systems whenever possible. MFA should be required of all users, but start with privileged, administrative and remote access users.



Patch & Update Management

Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly.



THE IT PROFESSIONAL'S GUIDE

✓ *Actions for leaders.*
✓ *Discuss with IT staff or service providers.*

Essential Actions for Building a Culture of Cyber Readiness:

Youself Drive cybersecurity strategy, investment and culture	Your Staff Develop security awareness and vigilance	Your Systems Protect critical assets and applications	Your Surroundings Ensure only those who belong on your digital workplace have access	Your Data Make backups and avoid loss of info critical to operations	Your Actions Under Stress Limit damage and quicken restoration of normal operations
<p>Organizations living the culture have:</p> <ul style="list-style-type: none"> ✓ Led investment in basic cybersecurity. ✓ Determined how much of their operations are dependent on IT. ✓ Built a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information. ✓ Approached cyber as a business risk. ✓ Led development of cybersecurity policies. 	<p>Organizations living the culture have:</p> <ul style="list-style-type: none"> ✓ Leveraged basic cybersecurity training to improve exposure to cybersecurity concepts, terminology and activities associated with implementing cybersecurity best practices. ✓ Developed a culture of awareness to encourage employees to make good choices online. ✓ Learned about risks like phishing and business email compromise. ✓ Identified available training resources through professional associations, academic institutions, private sector and government sources. ✓ Maintained awareness of current events related to cybersecurity, using lessons-learned and reported events to remain vigilant against the current threat environment and agile to cybersecurity trends. 	<p>Organizations living the culture have:</p> <ul style="list-style-type: none"> ✓ Learned what is on their network. Maintained inventories of hardware and software assets to know what is in-play and at-risk from attack. ✓ Leveraged automatic updates for all operating systems and third-party software. ✓ Implemented secure configurations for all hardware and software assets. ✓ Removed unsupported or unauthorized hardware and software from systems. ✓ Leveraged email and web browser security settings to protect against spoofed or modified emails and unsecured webpages. ✓ Created application integrity and whitelisting policies so that only approved software is allowed to load and operate on their systems. 	<p>Organizations living the culture have:</p> <ul style="list-style-type: none"> ✓ Learned who is on their network. Maintained inventories of network connections (user accounts, vendors, business partners, etc.). ✓ Leveraged multi-factor authentication for all users, starting with privileged, administrative and remote access users. ✓ Granted access and admin permissions based on need-to-know and least privilege. ✓ Leveraged unique passwords for all user accounts. ✓ Developed IT policies and procedures addressing changes in user status (transfers, termination, etc.). 	<p>Organizations living the culture have:</p> <ul style="list-style-type: none"> ✓ Learned what information resides on their network. Maintained inventories of critical or sensitive information. ✓ Established regular automated backups and redundancies of key systems. ✓ Learned how their data is protected. ✓ Leveraged malware protection capabilities. ✓ Leveraged protections for backups, including physical security, encryption and offline copies. ✓ Learned what is happening on their network. Managed network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. 	<p>Organizations living the culture have:</p> <ul style="list-style-type: none"> ✓ Led development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often. ✓ Leveraged business impact assessments to prioritize resources and identify which systems must be recovered first. ✓ Learned who to call for help (outside partners, vendors, government / industry responders, technical advisors and law enforcement). ✓ Led development of an internal reporting structure to detect, communicate and contain attacks. ✓ Leveraged in-house containment measures to limit the impact of cyber incidents when they occur.

VOL.1 FALL 2019

Consistent with the NIST Cybersecurity Framework and other standards, these actions are the starting point to Cyber Readiness. To learn more, visit [CISA.gov/Cyber-Essentials](https://www.cisa.gov/Cyber-Essentials).



CISA
CYBER+INFRASTRUCTURE

Incident Reporting

CISA provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870;
- cisaservice@cisadhs.gov
- WWW.CISA.GOV

Report Cyber Issue

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

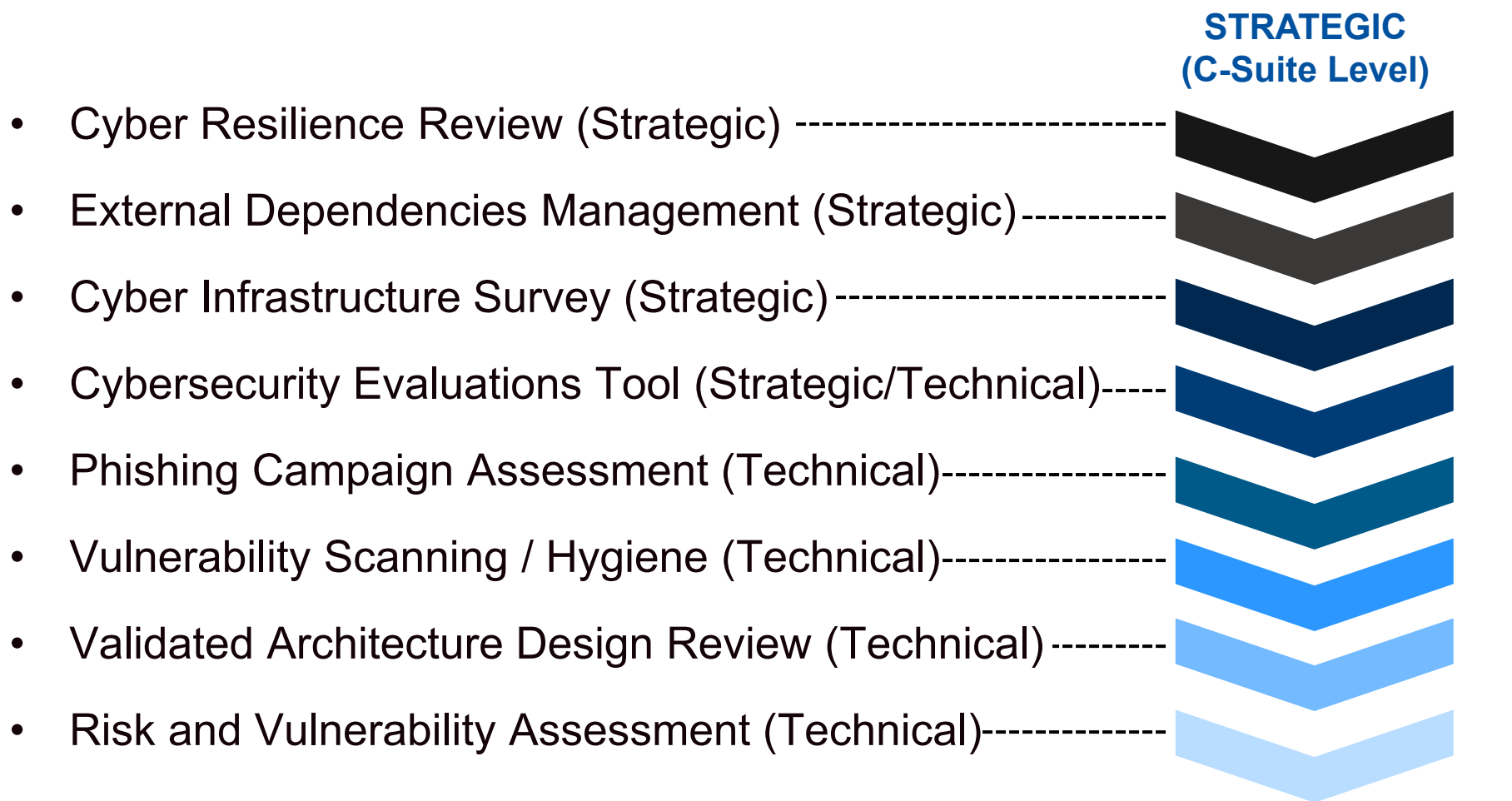
Malware Submission Process:

- 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

Range of Cybersecurity Assessments



CISA
CYBER+INFRASTRUCTURE

**TECHNICAL
(Network-Administrator Level)**

Cyber Resource Hub

Cybersecurity > Cyber Resource Hub

Cybersecurity

Combating Cyber Crime

Securing Federal Networks

Protecting Critical Infrastructure

Cyber Incident Response

Cyber Safety

Cybersecurity Assessments

Cybersecurity Governance

Cybersecurity Insurance

Detection and Prevention

Information Sharing

Stakeholder Engagement and
Cyber Infrastructure Resilience

Education

Access FedVTE Cybersecurity
Training Today

CISA Insights

CYBER RESOURCE HUB

Original release date: March 15, 2019 | Last revised: May 29, 2020

In order to assist a variety of stakeholders to ensure the cybersecurity of our Nation's critical infrastructure, CISA offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. CISA's cybersecurity assessment services are offered solely on a voluntary basis and are available upon request.

[Expand All Sections](#)

Vulnerability Scanning

+

Phishing Campaign Assessment

+

Risk and Vulnerability Assessment

+

Cyber Resilience Review

+

External Dependencies Management Assessment

+

Cyber Infrastructure Survey

+

Remote Penetration Testing

+

Web Application Scanning

+



CISA
CYBER+INFRASTRUCTURE

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

National Cyber Awareness System

[About Us](#)[Alerts and Tips](#) ▾[Resources](#)[Industrial Control Systems](#)

National Cyber Awareness System

Five products in the National Cyber Awareness System offer a variety of information for users with varied technical expertise. Those with more technical interest can read the Alerts, Analysis Reports, Current Activity, or Bulletins. Users looking for more general-interest pieces can read the Tips.

A subscription to any or all of the National Cyber Awareness System products ensures that you have access to timely information about security topics and threats. To learn more or to subscribe, visit the [subscription system](#). You can also visit our [Mailing Lists and Feeds](#) page to learn more about how to subscribe or use our syndicated feeds. If you're having trouble subscribing, read the [FAQ](#).



Check out our [tips](#) and [security publications](#) for additional security information.



Current Activity

Provides up-to-date information about high-impact types of security activity affecting the community at large.

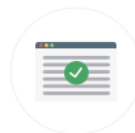
[View Current Activity](#) >



Alerts

Provide timely information about current security issues, vulnerabilities, and exploits.

[View Alerts](#) >



Bulletins

Provide weekly summaries of new vulnerabilities. Patch information is provided when available.

[View Bulletins](#) >



Analysis Reports

Provide in-depth analysis on a new or evolving cyber threat.

[View Analysis Reports](#) >



CISA
CYBER+INFRASTRUCTURE

<https://www.us-cert.gov/ncas>

Contacts and Questions?



Tony Enriquez

Region V Cybersecurity Advisor

antonio.enriquez@hq.dhs.gov

For inquiries or further information,
contact cyberadvisor@cisa.dhs.gov