U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

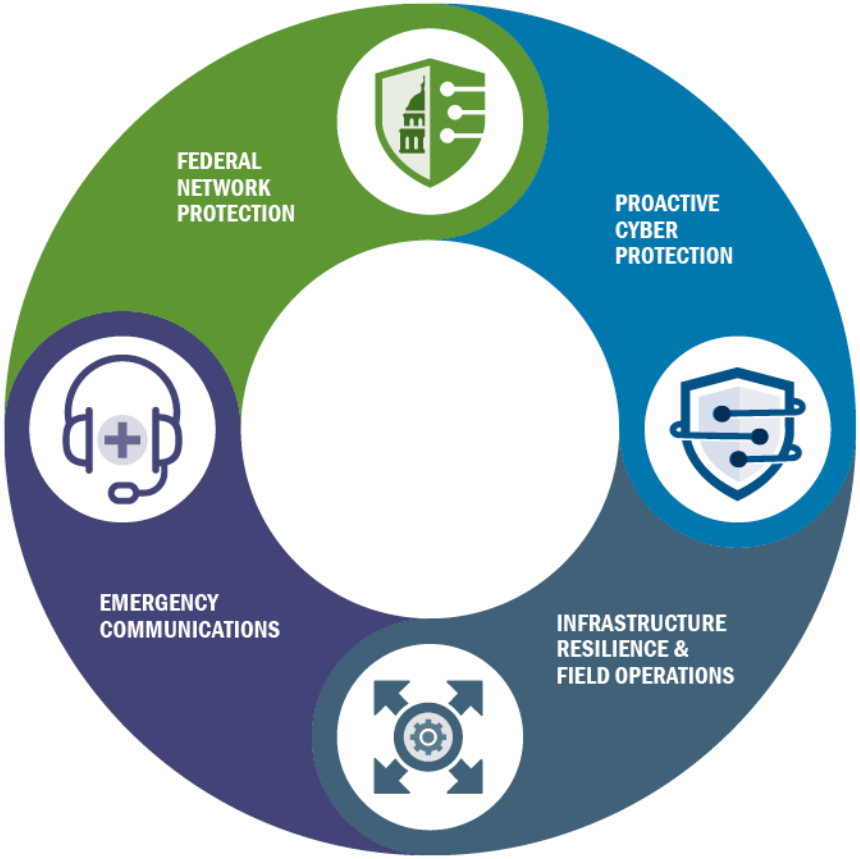
Tony Enriquez
Cybersecurity Advisor
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

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

Cybersecurity Advisor Program

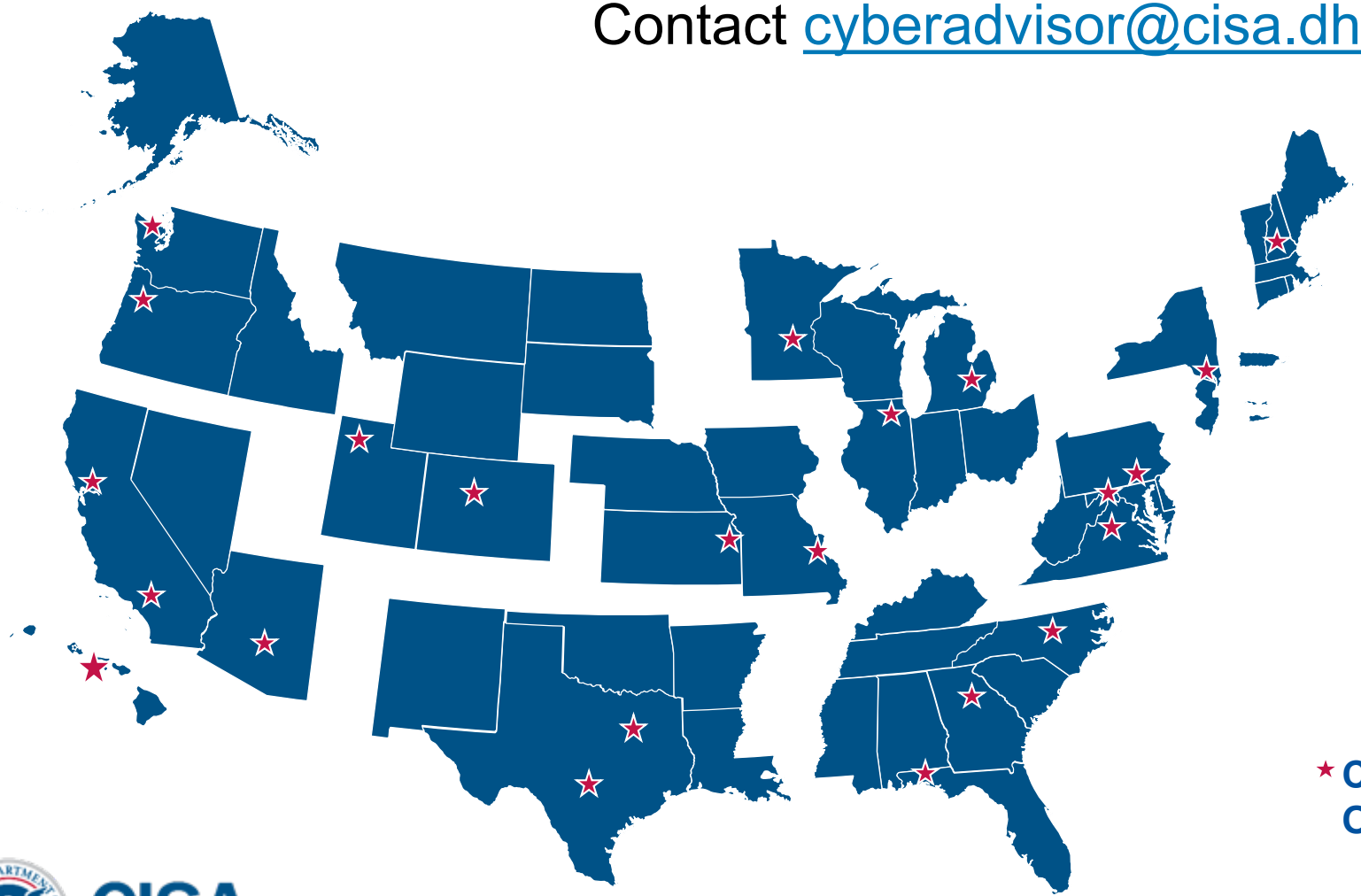
CISA mission: Lead the Nation's efforts to understand and manage risk to our critical infrastructure.

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



CISA
CYBER+INFRASTRUCTURE

Cybersecurity and Resilience

Who is targeting you?

CISA
CYBER+INFRASTRUCTURE

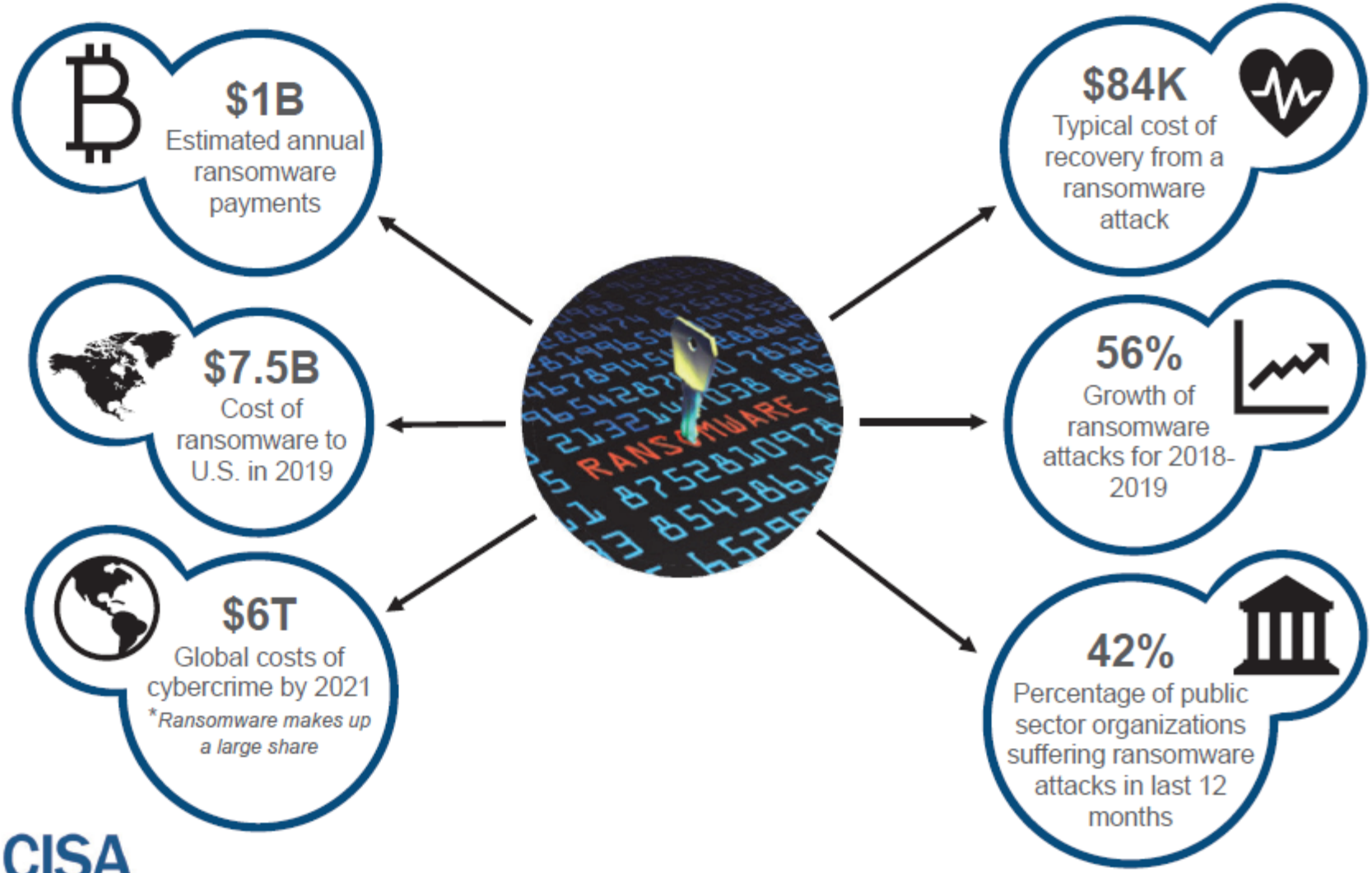
What is Ransomware?

- 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.

CISA
CYBER+INFRASTRUCTURE

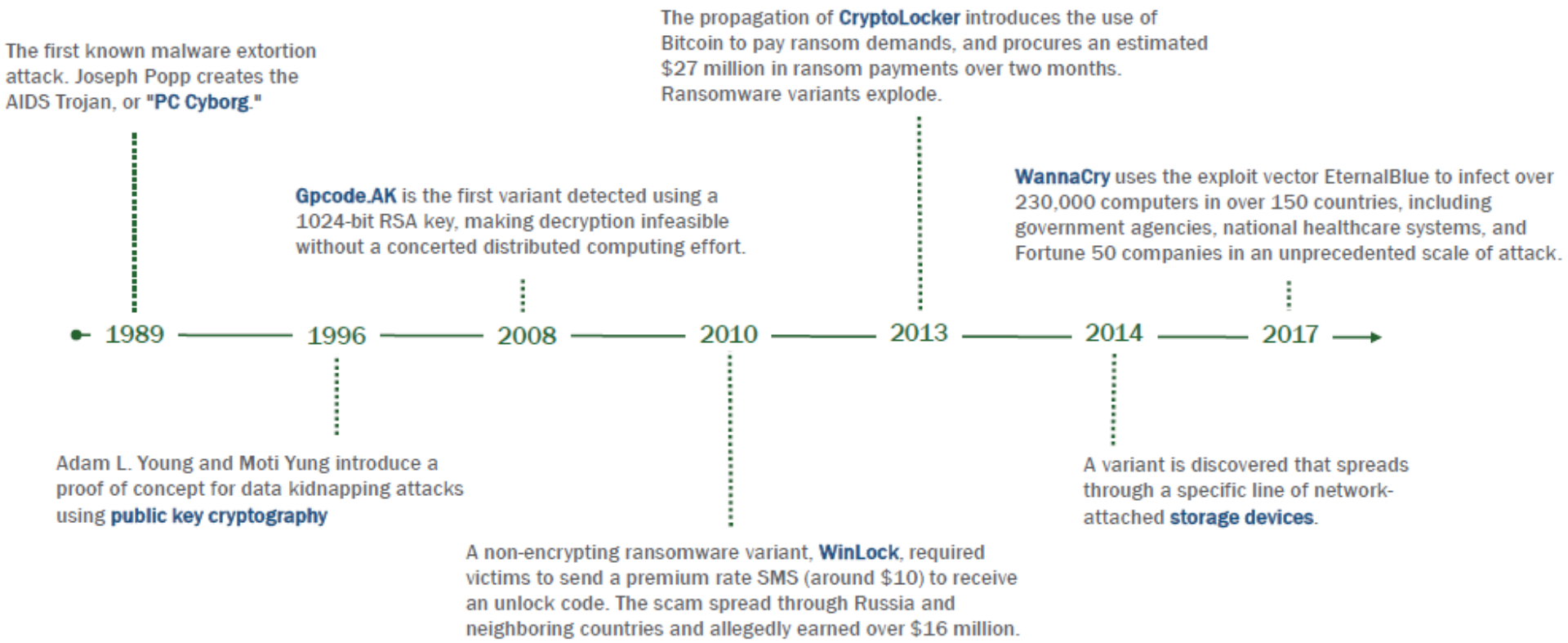
https://www.us-cert.gov/Ransomware

Ransomware by the Numbers



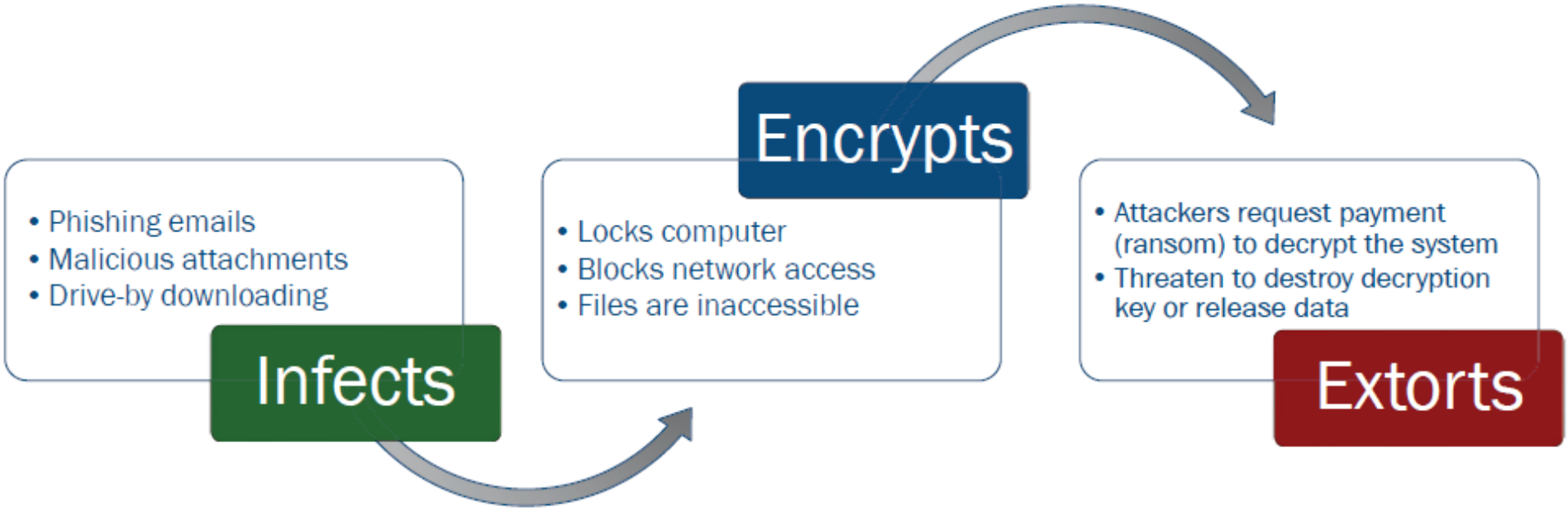
CISA
CYBER+INFRASTRUCTURE

Evolution of Ransomware



CISA
CYBER+INFRASTRUCTURE

Ransomware Patterns of Behavior



CISA
CYBER+INFRASTRUCTURE

What can you do today to defend yourselves?

August 21, 2019

CISA INSIGHTS
Ransomware Outbreak

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?

August 21, 2019

CISA INSIGHTS
Ransomware Outbreak

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.

CISA
CYBER+INFRASTRUCTURE

Ransomware Resources

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

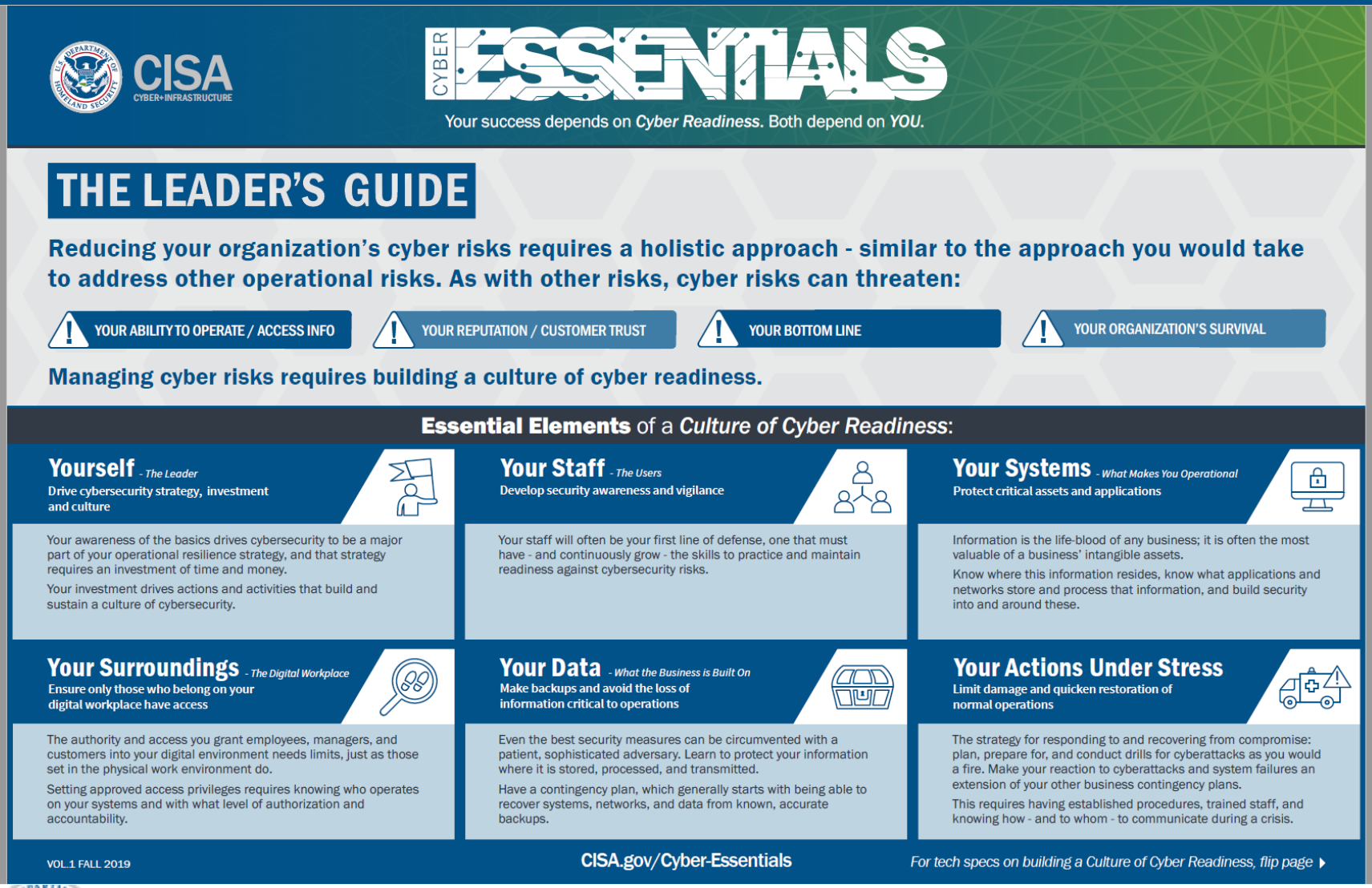
- Isolate the infected computer immediately
- Isolate or power-off affected devices
- Immediately secure backup data or systems
- Contact law enforcement
- Secure partial portions of the ransomed data that might exist
- Change all online account passwords and network passwords
- Delete Registry values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

CISA
CYBER+INFRASTRUCTURE

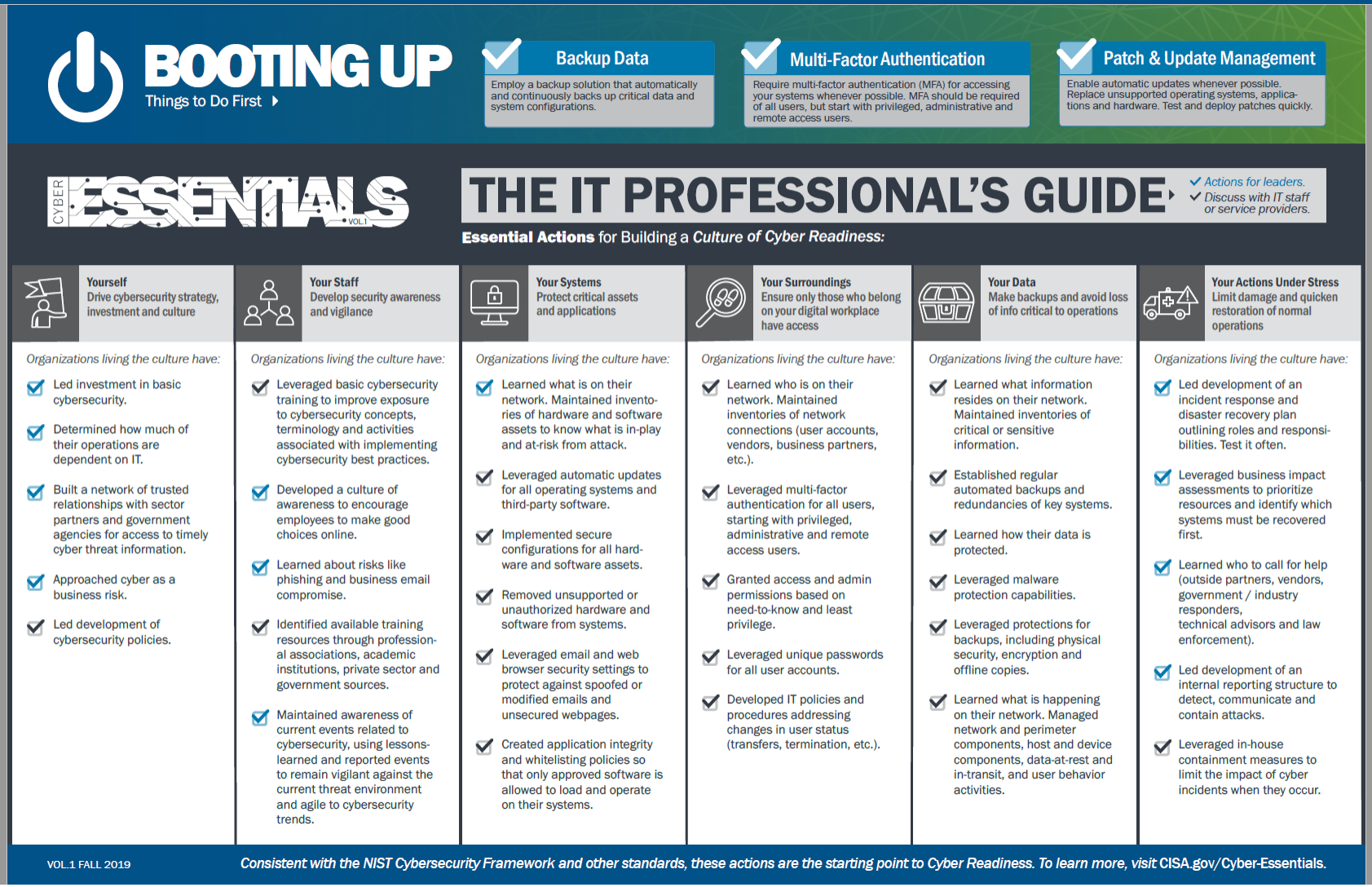
Ransomware Resources

- 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



Additional Resources



CISA
CYBER+INFRASTRUCTURE

Incident Reporting

CISA provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870;
  - cisaservicedesk@cisa.dhs.gov
  - WWW.CISA.GOV

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

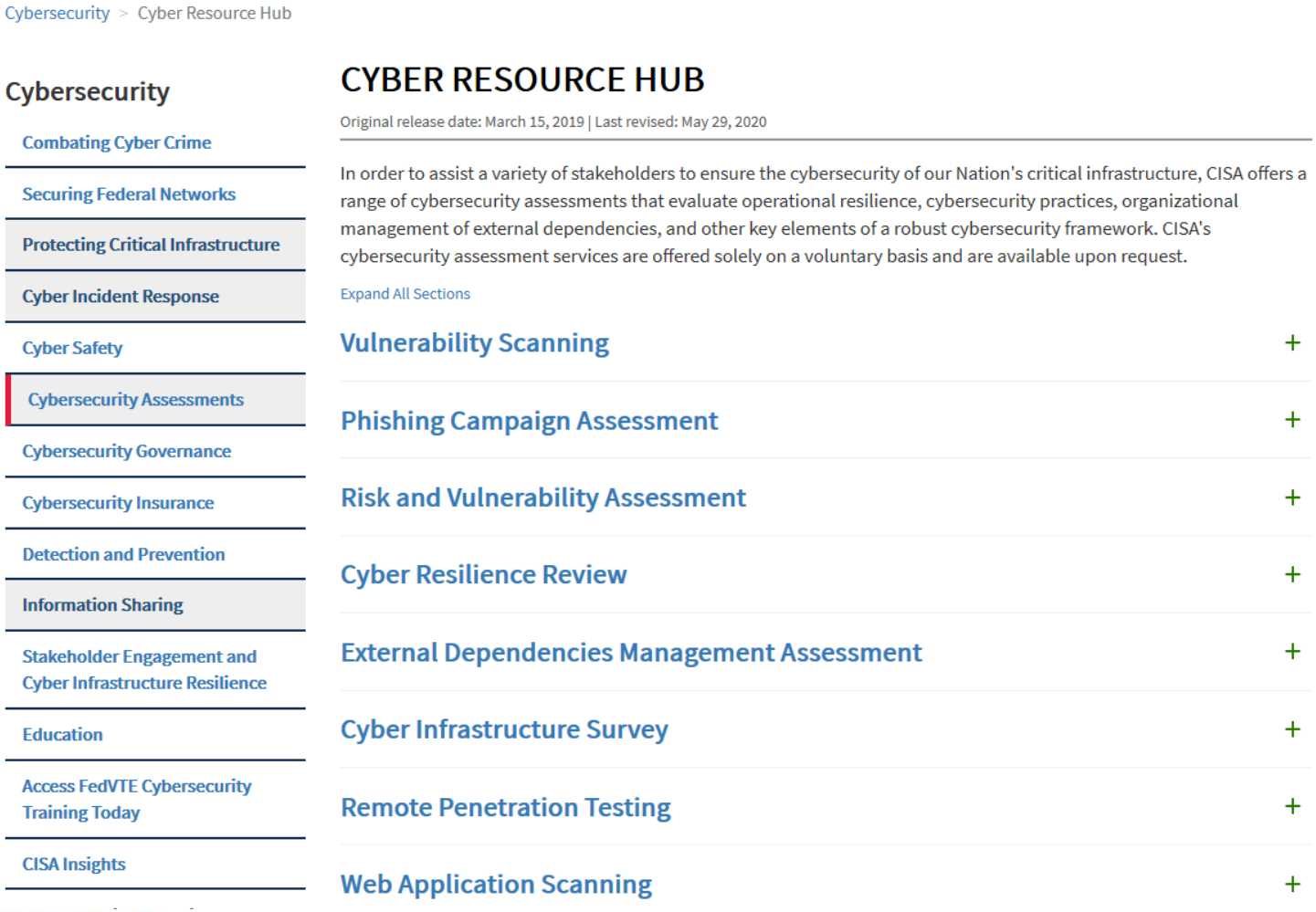
STRATEGIC
(C-Suite Level)

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

TECHNICAL
(Network-Administrator Level)

CISA
CYBER+INFRASTRUCTURE

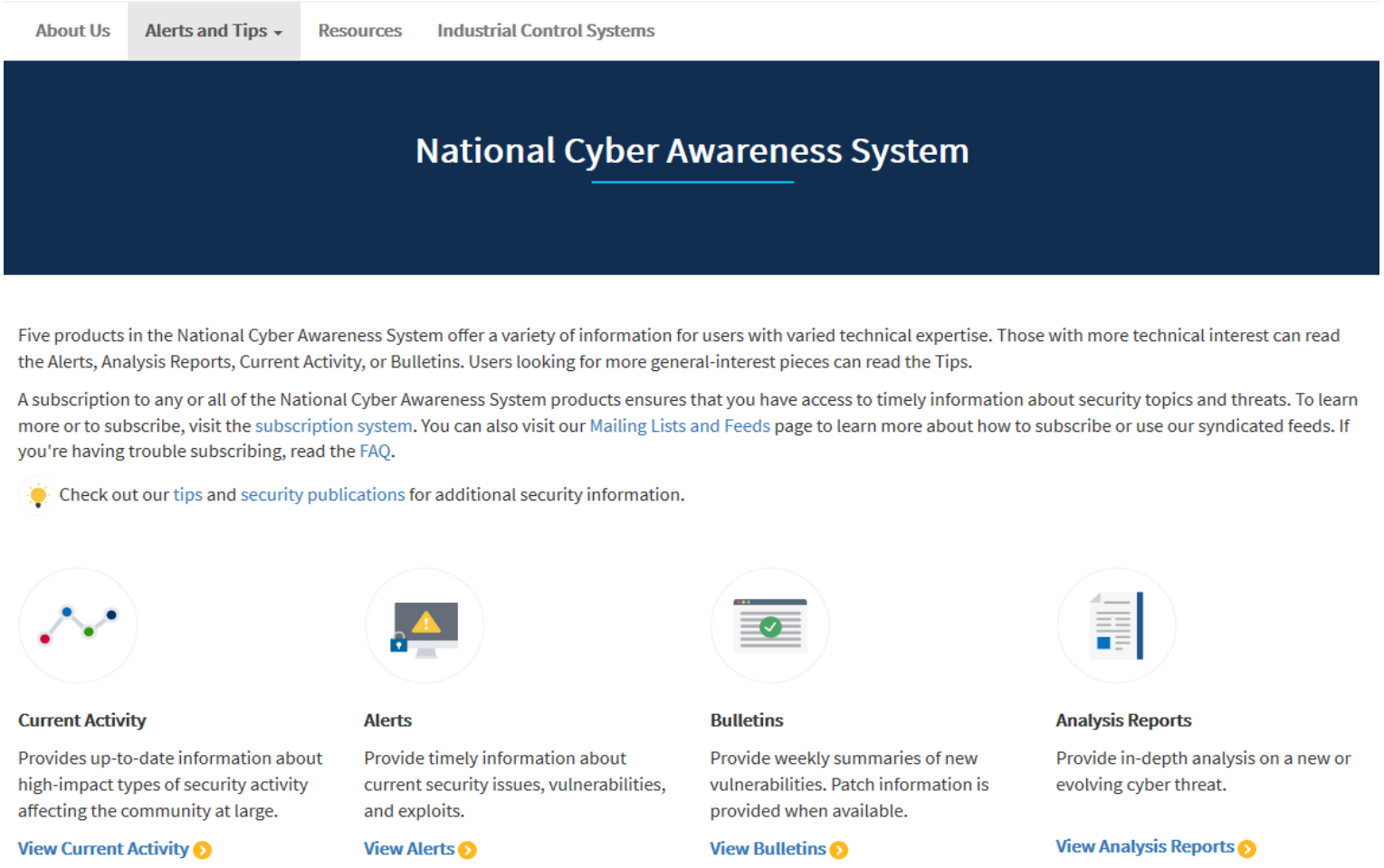
Cyber Resource Hub



CISA
CYBER+INFRASTRUCTURE

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

National Cyber Awareness System



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

CISA
CYBER+INFRASTRUCTURE