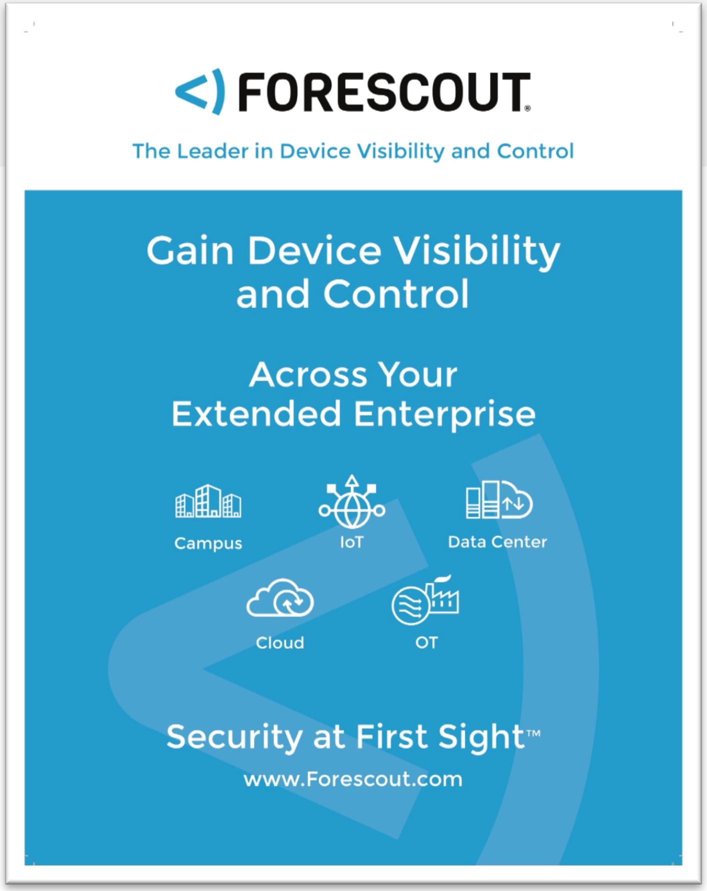
FORESCOUT

Lessons Learned: Ransomware in Atlanta

National Conference of State Legislatures
May 28, 2020

Jonathan Jesse, Senior Systems Engineer, Forescout
Yejin Jang, Government Affairs Director, Forescout

About Forescout + Speakers



FORESCOUT

The Leader in Device Visibility and Control

Gain Device Visibility and Control

Across Your Extended Enterprise

Security at First Sight™

www.Forescout.com

Jonathan Jesse

Senior Systems Engineer, Forescout

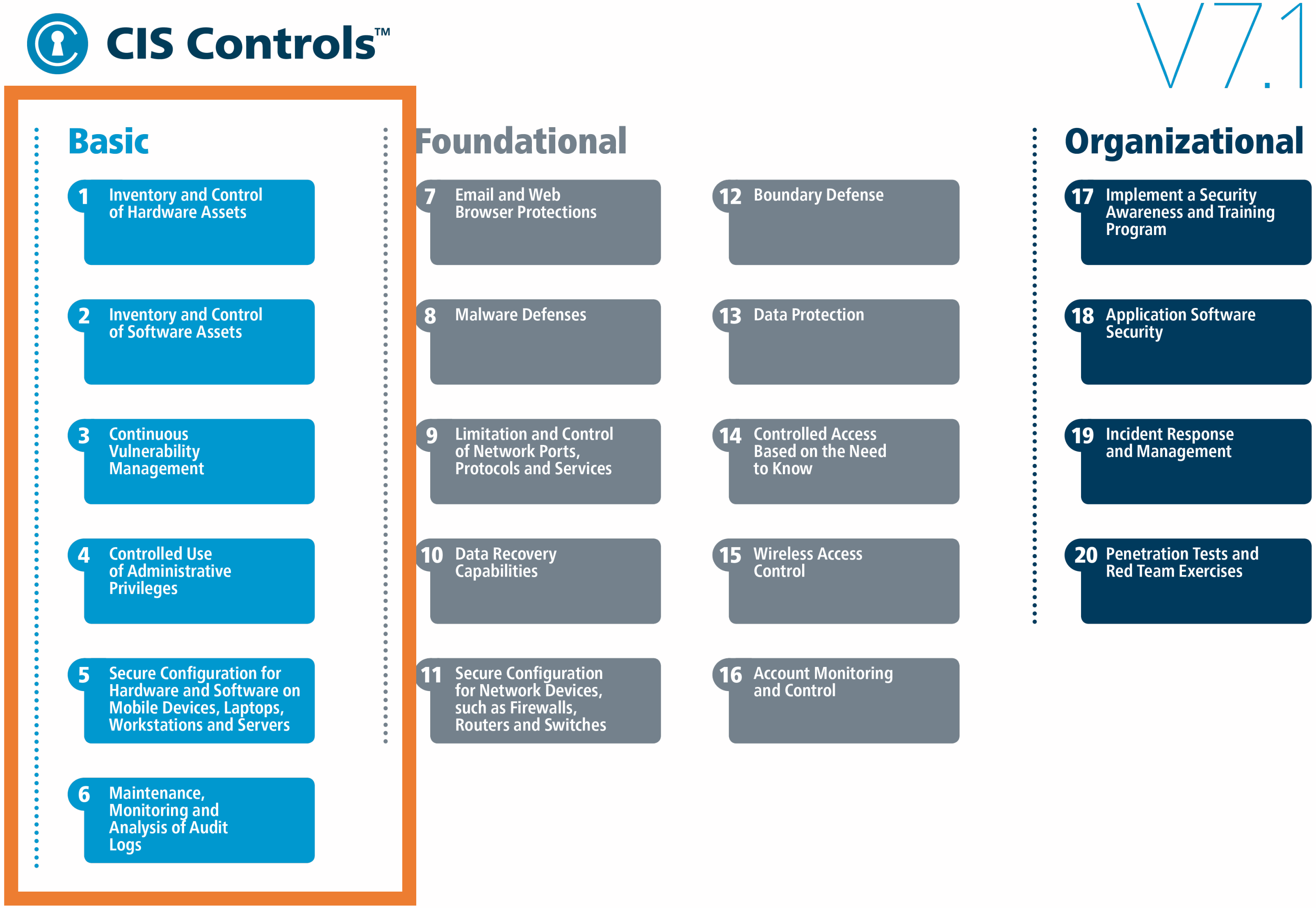
Yejin Jang

Government Affairs Director, Forescout

Agenda

- KEY CYBERSECURITY PRINCIPLES
- ATLANTA RANSOMWARE TIMELINE
- RANSOMWARE DETAILS
- LESSONS LEARNED
- MODEL LEGISLATION (TEXAS HB 4214)

Center for Internet Security (CIS) Top 20 Controls



CIS Controls™

V7.1

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

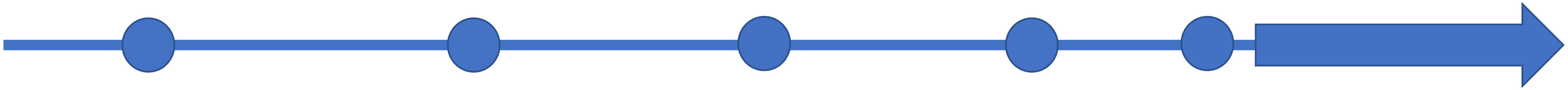
18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Source: https://www.cisecurity.org/controls/

Timeline + Ransomware Details



January 2018
Audit results released - 100 government servers running unsupported Windows software

March 2018
Atlanta announces ransomware attack

June 2018
424 applications not working (some critical)

Oct. 2018
Gary Brantley starts as CIO

Nov. 2018
DOJ indicts Iranian hackers

Stages of a SamSam Ransomware Outbreak

1) Vulnerability exists or remediating vulnerabilities not 100% complete/effective (SamSam uses JBOSS or RDP)

2) Exploitation/penetration occurs via stolen/compromised credentials (“brute force”)

3) Privileges elevated via Domain Controllers

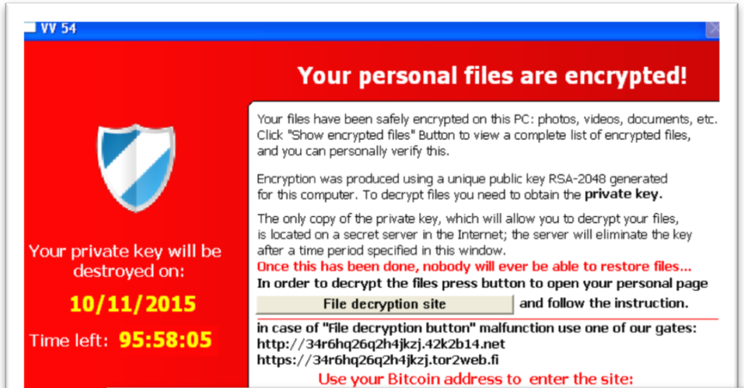
4) Identify vulnerable systems-actor tests waters identifying those systems he can command, what systems are “manageable” via credentials (write a empty text file to a directory)

5) Deploy the Payload - executable, script

6) Execute Payload

7) Encrypt systems (e.g.-file extension changed to “.sorry”, “.imsorry”)

8) Demand Ransom



Your personal files are encrypted!

Your private key will be destroyed on:

10/11/2015

Time left: **95:58:05**

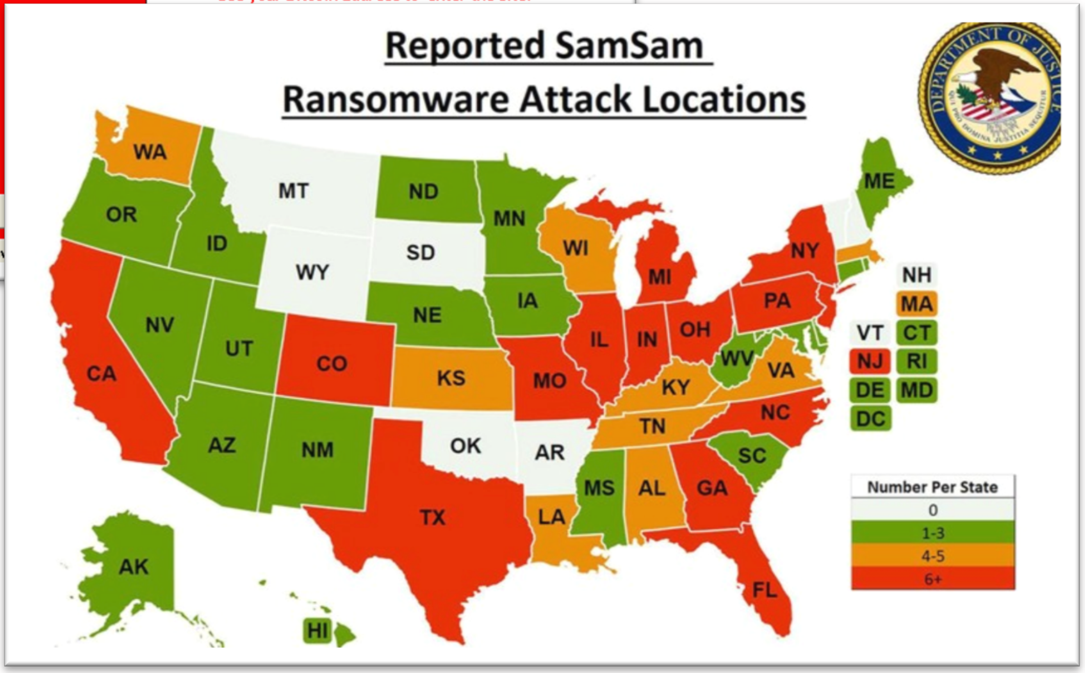
Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files press button to open your personal page
File decryption site **and follow the instruction.**

in case of "File decryption button" malfunction use one of our gates:
http://34r6hq26q2h4jkzj.42k2b14.net
https://34r6hq26q2h4jkzj.tor2web.fi

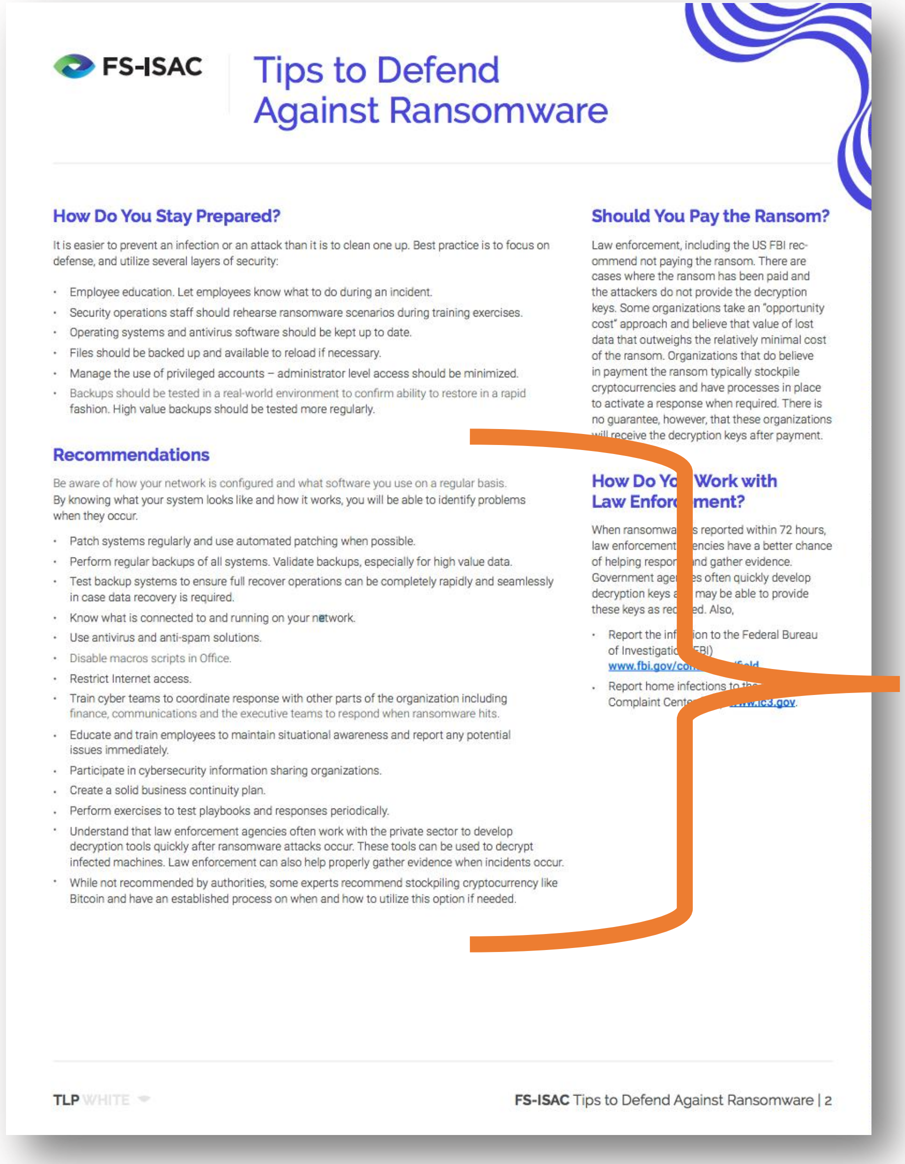
Use your Bitcoin address to enter the site:



Reported SamSam Ransomware Attack Locations

Source: https://www.justice.gov/opa/press-release/file/1114736/download

Recommendations



FS-ISAC

Tips to Defend Against Ransomware

How Do You Stay Prepared?

It is easier to prevent an infection or an attack than it is to clean one up. Best practice is to focus on defense, and utilize several layers of security:

- Employee education. Let employees know what to do during an incident.
- Security operations staff should rehearse ransomware scenarios during training exercises.
- Operating systems and antivirus software should be kept up to date.
- Files should be backed up and available to reload if necessary.
- Manage the use of privileged accounts – administrator level access should be minimized.
- Backups should be tested in a real-world environment to confirm ability to restore in a rapid fashion. High value backups should be tested more regularly.

Recommendations

Be aware of how your network is configured and what software you use on a regular basis. By knowing what your system looks like and how it works, you will be able to identify problems when they occur.

- Patch systems regularly and use automated patching when possible.
- Perform regular backups of all systems. Validate backups, especially for high value data.
- Test backup systems to ensure full recover operations can be completely rapidly and seamlessly in case data recovery is required.
- Know what is connected to and running on your network.
- Use antivirus and anti-spam solutions.
- Disable macros scripts in Office.
- Restrict Internet access.
- Train cyber teams to coordinate response with other parts of the organization including finance, communications and the executive teams to respond when ransomware hits.
- Educate and train employees to maintain situational awareness and report any potential issues immediately.
- Participate in cybersecurity information sharing organizations.
- Create a solid business continuity plan.
- Perform exercises to test playbooks and responses periodically.
- Understand that law enforcement agencies often work with the private sector to develop decryption tools quickly after ransomware attacks occur. These tools can be used to decrypt infected machines. Law enforcement can also help properly gather evidence when incidents occur.
- While not recommended by authorities, some experts recommend stockpiling cryptocurrency like Bitcoin and have an established process on when and how to utilize this option if needed.

Should You Pay the Ransom?

Law enforcement, including the US FBI recommend not paying the ransom. There are cases where the ransom has been paid and the attackers do not provide the decryption keys. Some organizations take an "opportunity cost" approach and believe that value of lost data that outweighs the relatively minimal cost of the ransom. Organizations that do believe in payment the ransom typically stockpile cryptocurrencies and have processes in place to activate a response when required. There is no guarantee, however, that these organizations will receive the decryption keys after payment.

How Do Yo Work with Law Enfor ment?

When ransomwa s reported within 72 hours, law enforcement encies have a better chance of helping respor nd gather evidence. Government ager es often quickly develop decryption keys a may be able to provide these keys as rec ed. Also,

- Report the inf ion to the Federal Bureau of Investigatic FBI) www.fbi.gov/co /field
- Report home infections to th Complaint Cent www.ic3.gov.

TLP WHITE

FS-ISAC Tips to Defend Against Ransomware | 2

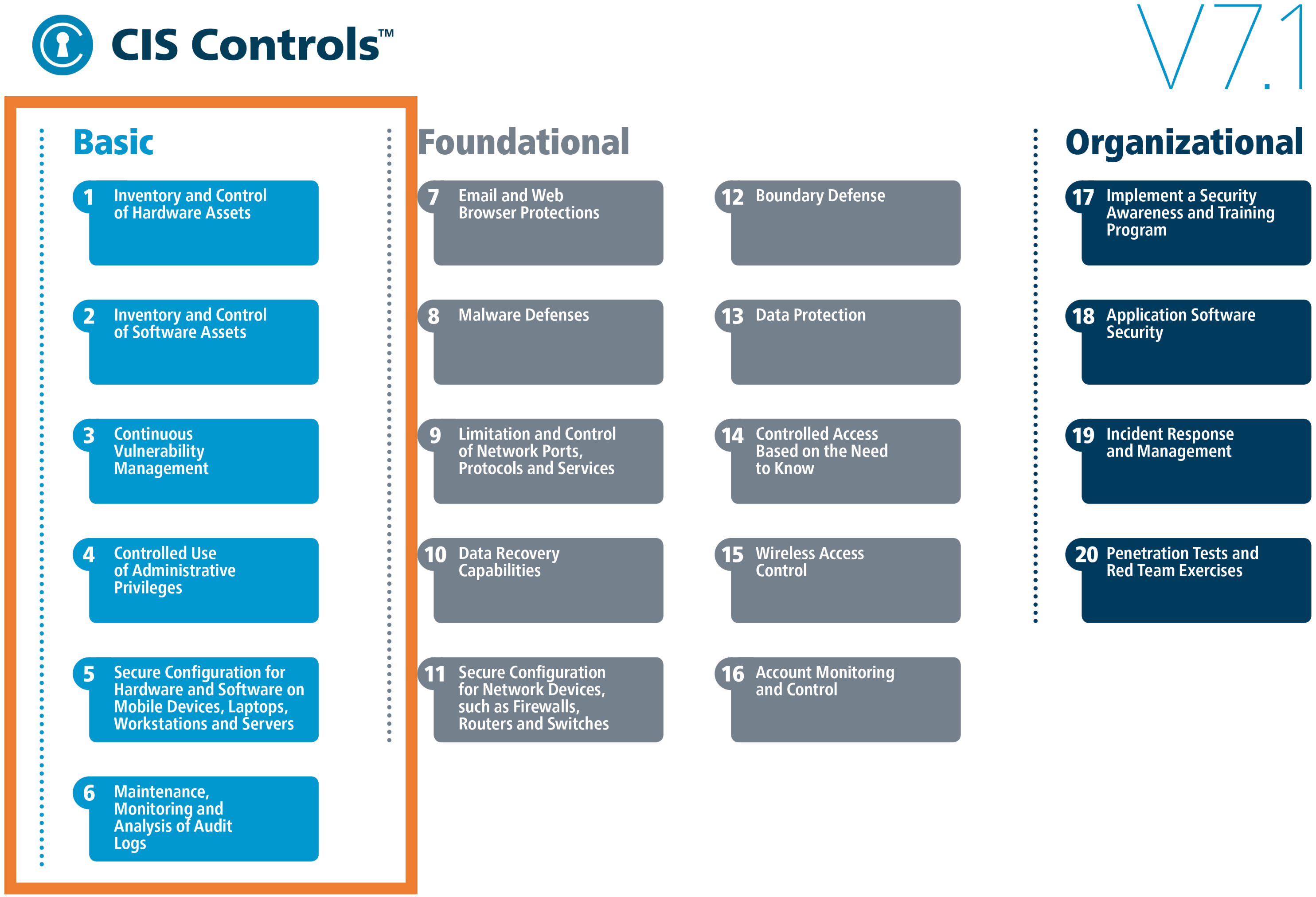
"Be aware of how your network is configured and what software you use on a regular basis. **By knowing what your system looks like and how it works, you will be able to identify problems when they occur."**

"Patch systems regularly and use automated patching when possible."

"Know what is connected to and running on your network."

Source: https://www.fsisac.com/hubfs/5442200/Resources/FSISAC_TipstoDefendAgainstRansomware.pdf

Lessons Learned



CIS Controls™ V7.1

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

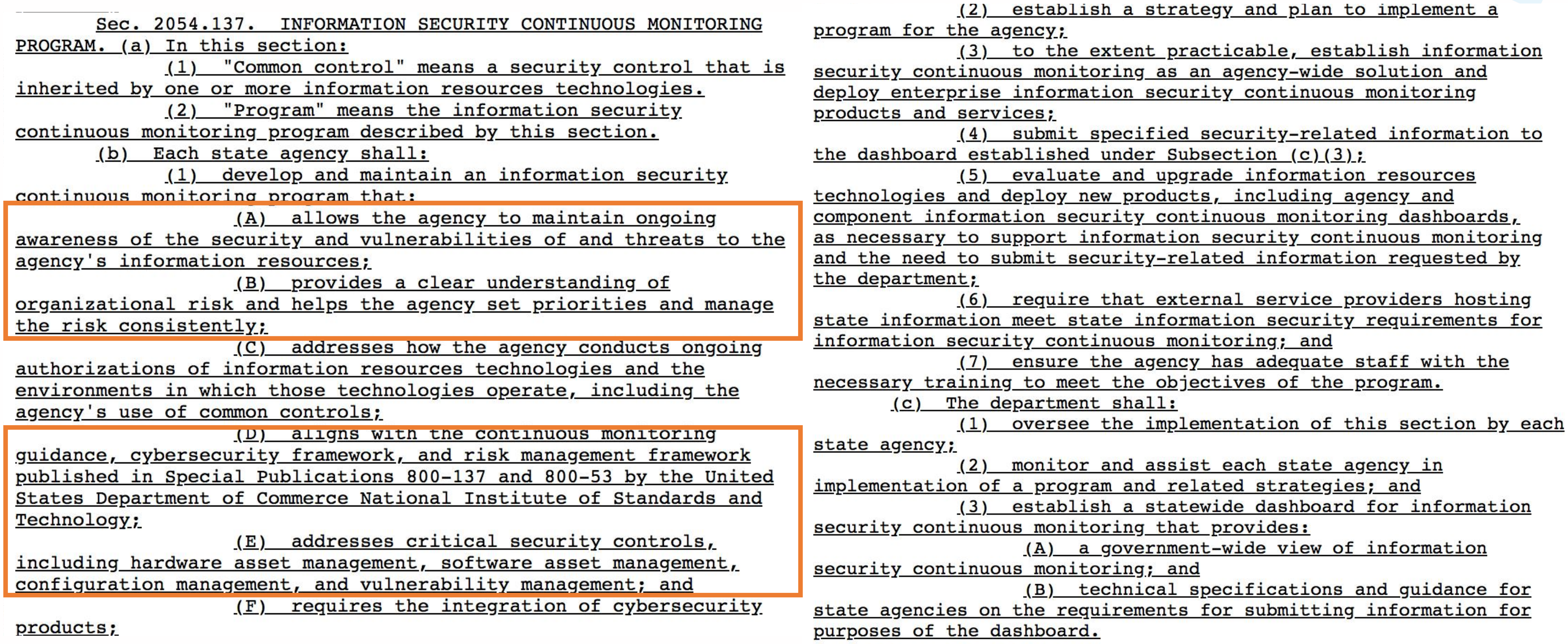
19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

- **Governance**
  - People
  - Processes
  - Tools
- **Disaster Recovery**
- **When it happens…**
  - Communication

Source: https://www.cisecurity.org/controls/

Texas HB 4214



Sec. 2054.137. INFORMATION SECURITY CONTINUOUS MONITORING PROGRAM. (a) In this section:

(1) "Common control" means a security control that is inherited by one or more information resources technologies.

(2) "Program" means the information security continuous monitoring program described by this section.

(b) Each state agency shall:

(1) develop and maintain an information security continuous monitoring program that:

(A) allows the agency to maintain ongoing awareness of the security and vulnerabilities of and threats to the agency's information resources;

(B) provides a clear understanding of organizational risk and helps the agency set priorities and manage the risk consistently;

(C) addresses how the agency conducts ongoing authorizations of information resources technologies and the environments in which those technologies operate, including the agency's use of common controls;

(D) aligns with the continuous monitoring guidance, cybersecurity framework, and risk management framework published in Special Publications 800-137 and 800-53 by the United States Department of Commerce National Institute of Standards and Technology;

(E) addresses critical security controls, including hardware asset management, software asset management, configuration management, and vulnerability management; and

(F) requires the integration of cybersecurity products;

(2) establish a strategy and plan to implement a program for the agency;

(3) to the extent practicable, establish information security continuous monitoring as an agency-wide solution and deploy enterprise information security continuous monitoring products and services;

(4) submit specified security-related information to the dashboard established under Subsection (c)(3);

(5) evaluate and upgrade information resources technologies and deploy new products, including agency and component information security continuous monitoring dashboards, as necessary to support information security continuous monitoring and the need to submit security-related information requested by the department;

(6) require that external service providers hosting state information meet state information security requirements for information security continuous monitoring; and

(7) ensure the agency has adequate staff with the necessary training to meet the objectives of the program.

(c) The department shall:

(1) oversee the implementation of this section by each state agency;

(2) monitor and assist each state agency in implementation of a program and related strategies; and

(3) establish a statewide dashboard for information security continuous monitoring that provides:

(A) a government-wide view of information security continuous monitoring; and

(B) technical specifications and guidance for state agencies on the requirements for submitting information for purposes of the dashboard.

Texas 86: HB 4214 (Rep Capriglione)

THANK YOU

Jonathan.Jesse@forescout.com

Yejin.Jang@forescout.com