Results. Guaranteed.

online

Objectives

Review Ransomware

BCP Overview

Review Template

❖ What is Ransomware?

- ✓ Ransomware is a type of malware (malicious software) distinct from other malware
- ✓ Ransomware defining characteristic is that it attempts to deny access to a user’s data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.
- ✓ After the user’s data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin)

- ✓ https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Response 1 Mitigate and Remediate

STEP 1: Disconnect everything

❑ Unplug the computer from the network via the Ethernet cable

❑ Contact SIRT team and BCP Team

❑ Turn off any wireless functionality: Wi-Fi, Bluetooth,

❑ Disconnect all external storage: memory sticks, attached phones/cameras, external hard drives, USB drives

❑ Do not turn the computer off. The message on the screen may be required to determine the ransomware type

❑ Call your Cyber Insurance Company

STEP 2: Determine the scope of the infection and check the following for Signs of Encryption from a known good, uninfected computer

- □ Find Credentials that were used to encrypt files
  - □ Need to lock down that user, in any other systems it’s logged on to
- □ Determine vector of infection (VPN, RDP etc), close hole
- □ Determine if all credentials needs to be changed
- □ Mapped or shared drives
- □ Mapped or shared folders from other computers
- □ Network storage devices of any kind
- □ External Hard Drives
- □ USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- □ Cloud-based storage: DropBox, Google Drive, OneDrive etc.

STEP 3: Determine the ransomware strain

(Advanced Skill – Contact Insurance First and Technical SMEs Before attempting or contacting)

- □ What strain or type of ransomware? For example: CryptoWall, Teslacrypt, etc.
  - □ https://id-ransomware.malwarehunterteam.com/
- □ Look for available decryptors
  - □ https://www.nomoreransom.org/
    - □ https://www.nomoreransom.org/en/decryption-tools.html

STEP 4: Determine Response

Now that you know the scope of your encrypted files and the ransomware strain you are dealing with, you can make a more informed decision about what to do next.

Response 1: Restore Your Files From Backup

- □ Locate your backups
  - □ Ensure all the files you need are there
  - □ Verify integrity of backups (i.e., media not reading or corrupted files)
  - □ Check for Shadow Copies if possible (may not be an option on newer ransomware)
  - □ Check for any previous versions of files that may be stored on cloud storage, e.g., DropBox, Google Drive, OneDrive
- □ A good practice is to back up the encrypted files in case a decryptor becomes available
- □ Rebuild the system from known good sources. Do not trust antivirus programs to completely remove all malware from a system. Install all patches to avoid reinfection from network-transmitted malware
- □ Restore your files from backups
- □ All credentials stored anywhere on the local network (including those saved inside Web browsers and password managers) could be compromised and need to be changed
- □ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete to avoid reinfection

online

Results. Guaranteed.

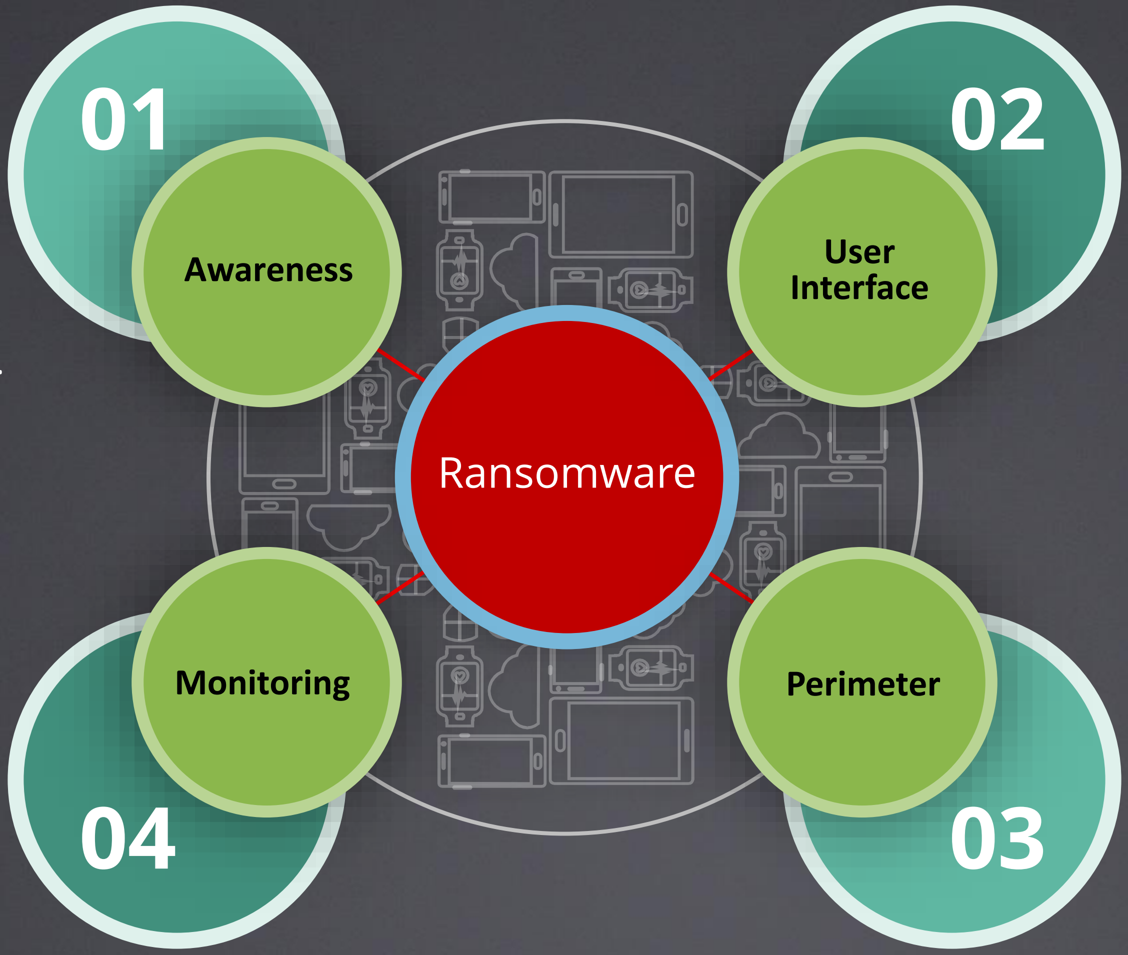
Security Measures

Awareness

- Security incident process
- Awareness emails
- +Targeted campaigns
- Monthly newsletters
- Labs and direct training
- Incentives
- Third Party Training https://phishinsight.trendmicro.com
- https://www.phishingbox.com

Monitoring

- Firewall perimeter alerts
- Enable IPS on firewalls
- Operations Center – central interface with key systems and alerts
- Back-up & Restore process
- 3rd party security monitoring
- Monitor outgoing traffic



User Interface

- Lock down desktop settings
- USB drives locked
- SPAM filters
- Only Application needed for business
- Stricter install policies
- File and computer inspections
- Limit EMR Access to working hours

Perimeter

- Reduce external connections
- VPN / VDI / MFA
- 3rd party connections
- SPAM filtering
- DDOS readiness
- Real-time EPP and IDS
- Work from Home Policy and Procedures

Technical Guidance

Monitoring Detection

- Implement IDS systems
- Monitor inbound and outbound data
- Virus protection
- Third party network testing
- Activity monitoring
- File access monitoring
- SOC Monitoring

Communication/ Network

- Email encryption and filtering (Mimecast, Barracuda)
- Fax directly to EMR system
- Network segmentation (Cloud)
- E3 Microsoft Security
- Third-Party EMR system
- Packet level filtering

Access Control

- MFA for all external connection that access ePHI and critical processes
- **Review third party accounts to make sure old accounts are not active**
- Internal account review
- Work from home policy and procedures
- Limit Access to EMR system

Emergency Management

- **BCP and IRP should have a specific plan for Ransomware**
- Contact Cyber Insurance company first to address forensics and chain-of-custody
- Have a chain-of-custody plan
- Have routine test of backups and restoring backups and critical operations

Business Continuity and Cybersecurity

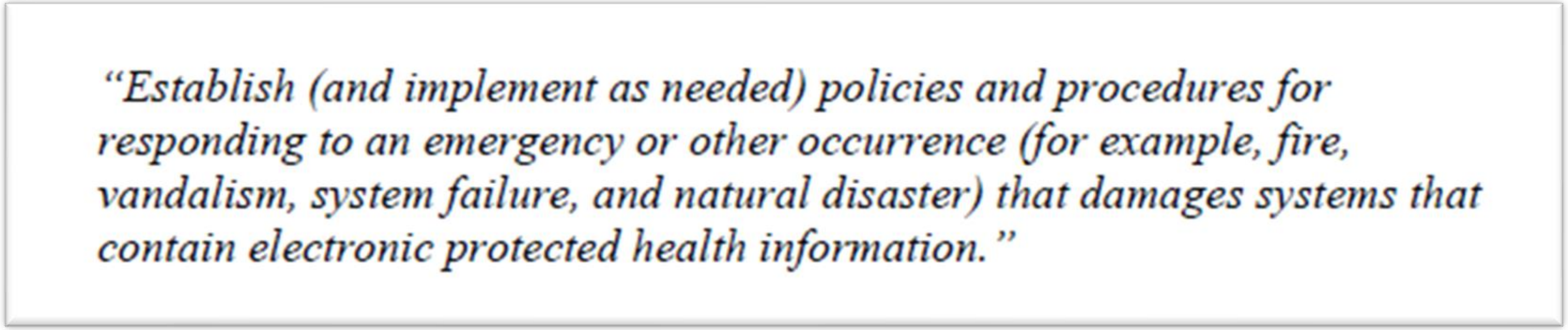
Why do you need a BCP Plan

- ❖ Ransomware/ Cyber Threats
- ❖ Business Objectives
- ❖ Patient Safety
- ❖ Financial Security
- ❖ HIPAA Compliance
- ❖ Just Good Business!

Why you Might Need A BCP

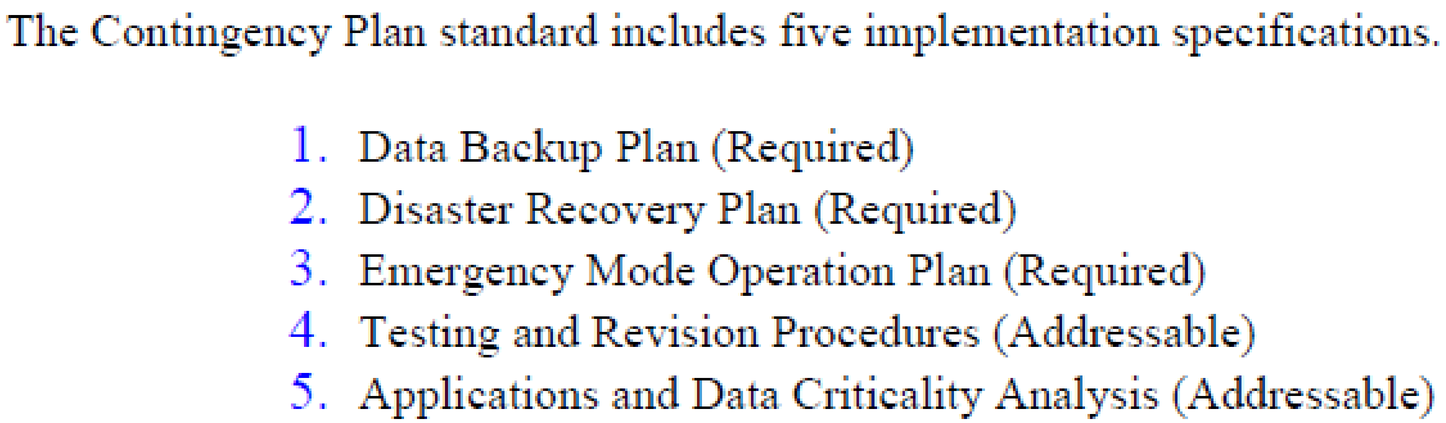
- Natural Disaster, Snowstorm
- Technical Outage, Power, Network
- Pandemic?
- Social and Political Conflict?
- Cyber Attack, Ransomware

Contingency Plan - § 164.308(a)(7)



> *"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."*

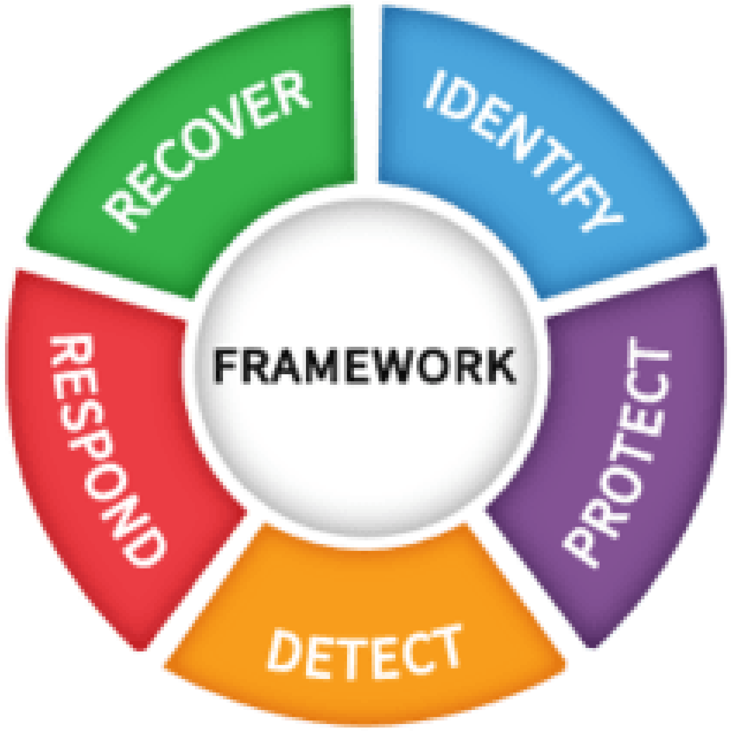
HIPAA and Emergency Response



The Contingency Plan standard includes five implementation specifications.

1. Data Backup Plan (Required)
2. Disaster Recovery Plan (Required)
3. Emergency Mode Operation Plan (Required)
4. Testing and Revision Procedures (Addressable)
5. Applications and Data Criticality Analysis (Addressable)

NIST Cybersecurity Framework



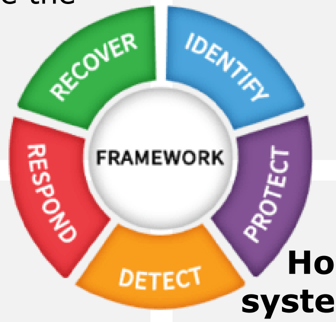
Business Continuity Plan

Respond

Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected events.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Identify

- What workflows are critical during an emergency?
- What systems and information are critical to supporting those workflows?



Recover

- When you return to "normal", how will you reconcile production and backup systems?
- Who will make determinations of when to switch systems?
- Lessons Learned.

Protect

How can you perform those workflows if those systems aren't available? How will information be available when and where needed?
- How will you maintain integrity of information as you go to paper-based or offline systems?
- **How will you maintain security controls during an emergency?**
- Consider: Access Control, Encryption, Monitoring, Backup/Recovery. Are there areas where you will bypass controls? For example: Emergency Authorization for access to systems? What compensating controls are in place?

online

Results. Guaranteed.

Business Continuity Template

Business Continuity Plan

- Components of the Business Continuity Plan
  - Business Units/Locations with primary and backup contact names and numbers
  - BCP Team Members and Responsibilities
  - List of critical assets (input from BIA)
  - Reference Documents such as facility recovery plans, system backup/recovery plans, State/local plans Departmental BCPs
  - Communications and Coordination Plans
  - Critical Vendor, Service Provider, and Law Enforcement contact information
  - Procedure to return to normal operations
  - **Be Prepared for IT and Ransomware Attacks (Overthink It)**

Evaluation Form

Results. Guaranteed.

online

Maintaining Cybersecurity When Disaster Strikes