

online

Ransomware: Prevention,
Response, and Preparedness

October 22, 2021

Objectives

-
- ❖ Provide information on the scope and problem of Ransomware
-
- ❖ Discuss Regulatory Requirements and Frameworks related to Ransomware Preparedness and Response
-
- ❖ Provide practical steps for preventing, containing, and responding to Ransomware attacks
-

Agenda



Overview of Ransomware



Legal and Frameworks



Prevention



Response and Preparedness



Q&A



Tabletop Exercise

Overview of Ransomware

Are Clinics a Target?

560 Healthcare Providers Fell Victim to Ransomware Attacks in 2020

In 2020, Emsisoft data shows 560 healthcare provider facilities fell victim to ransomware attacks, of an overall 2,354 US entities hit by the malware variant.



WOMEN@FORBES APR 14, 2017 @ 10:05 PM 6,666

The Little Black Book of Billionaire Secrets

Your Electronic Medical Records Could Be Worth \$1000 To Hackers



Mariya Yao, WOMEN@FORBES
CTO of Metamovers, Co-Author of "Applied Artificial Intelligence" FULL BIO
Opinions expressed by Forbes Contributors are their own.

<https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#571d3ece50cf>

41 Providers Reported Ransomware Attacks in First Half of 2020

While the rate of successful ransomware attacks remained flat during Q1 and Q2 of 2020, Emsisoft predicts a likely uptick due to the season and as the workforce returns to the office.



online

Are Clinics a Target?

[Global Edition](#) [Privacy & Security](#)

Hospital ransomware attack led to infant's death, lawsuit alleges

The 2019 incident, which disabled Springhill Medical Center's EHR and patient monitors for days, obscured access to critical information that could have allowed for a lifesaving C-section, the baby's mother says.


By [Mike Miliard](#) | October 01, 2021 | 01:31 PM


How Information is Used on the Dark Web

- Health records will surface as a 'fullz' the slang term on the Dark Web for a complete long-form document containing of all the intricacies of a person's health history, preferred pharmacy, financial data and PII data.
- What happens is the people who purchase those fullz then go to another vendor on the dark web for what's called **Dox**, the slang term for documentation, where they then proceed to have documents made.
 - Passports,
 - Drivers' licenses,
 - Social Security cards
- All these things that will help the counterfeit imitation of the victim. So, you have electronic health record that will typically go for \$20 apiece, and you'll spend a couple hundred dollars on 'doxs' to support that identity, and once it's an identity kit, you can sell it for \$1,500 to \$2,000."

Dark Web Add

matching: fullz

 Size: 30.9K [cc fullz \\$1000-\\$3000usd with safe cashout details dumps with pin](#)

 Home * Help * Login * Register New to Darknet? Want to learn more about criminality? { Start here } Disclaimer: Onionland and its admins are not liable for what is done with any information
<http://onionlandbakyt3j.onion/index.php?topic=16931.0>

matching: fullz

Dark Web Examples "Identity Kit"

USA Citizenship

[Products](#) [FAQs](#) [Register](#) [Login](#)

Become a citizen of the USA, real USA passport



We offer bulletproof USA passports + SSN + Drivers License and Birth Certificate and other papers making you an official citizen of the USA!
It will even work if you are not in the USA yet.

How we do it? Trade secret! But we can assure you that you won't have any problems with our papers. We are shipping documents from the USA, international shipping is no problem. You can use your own name or a new name!
Information on how to send us required info (scanned signature, biometric picture etc) will be given after purchase.

The total price is 3000 USD, 1000 USD paid when you order and the other 2000 USD when we show you photo and video proof of your passport.
The first 1000 USD are needed upfront to see you are serious about it. Once paid we will discuss details in our

shop internal message system.

Product	Price	Quantity
Your USA citizenship first payment 1000/3000	1000 USD = 0.01951 ₿	<input type="text" value="1"/> X Buy now
US bank account with online banking and card. Great for cashing out bitcoin. Accounts will last at least 8 years.	1000 USD = 0.01951 ₿	<input type="text" value="1"/> X Buy now

After buying an ID or passport send us a message with your age and gender so we can find a matching dataset, alternatively you can provide a dataset (name, age, gender, size etc). We will also need a biometric photo in high quality and signature scanned, we will give more instructions after your purchase.
Update 11.2017: All prices reduced for a limited time!

Passports



Product	Price	Quantity
Lithuanian Passport	1350 EUR = 0.03156 ₿	<input type="text" value="1"/> X Buy now
Netherlands Passport	1500 EUR = 0.03507 ₿	<input type="text" value="1"/> X Buy now
Denmark Passport	1500 EUR = 0.03507 ₿	<input type="text" value="1"/> X Buy now
Great Britain Passport	1800 EUR = 0.04209 ₿	<input type="text" value="1"/> X Buy now
Canada Passport	1250 EUR = 0.02923 ₿	<input type="text" value="1"/> X Buy now

Drivers Licenses



Product	Price	Quantity
Norway Drivers License	550 EUR = 0.01286 ₿	<input type="text" value="1"/> X Buy now
Denmark Drivers License	550 EUR = 0.01286 ₿	<input type="text" value="1"/> X Buy now
Netherlands Drivers License	550 EUR = 0.01286 ₿	<input type="text" value="1"/> X Buy now
UK Drivers License	500 EUR = 0.01169 ₿	<input type="text" value="1"/> X Buy now

The Changing Landscape (Current Webpages)

How to Order COVID-19 Vaccine and Medicine, Corona virus

How To Order COVID-19 Vaccine and Medicine from Wuhan Institute of Virology Lab, Corona Virus Vaccine and Medicine.

COVID-19 VACCINE COVID-19 MEDICINE WHO WE ARE HOW TO ORDER CONTACT US



HOW TO ORDER COVID-19 VACCINE AND MEDICINE FROM WUHAN INSTITUTE OF VIROLOGY LAB. CORONA VIRUS VACCINE AND MEDICINE.

CATEGORIES

COVID-19 Vaccine

COVID-19 Medicine

Who we are

How to Order

Contact Us

Life is priceless but we need funds to save more lives. As it is written on other pages we do not intend to sell covid vaccines and/or corona virus medicines so there is no price tag but there is a set minimum. Your donations will help to save more lives so please show your generosity. Any email with below set minimum BTC will not be replied and unfortunately there is some limitations so we can save more lives as quickly as possible.

- * Long emails will not be replied.
- * Investigation type questions will be denied and the address will be blocked.
- * Supply is very limited so all inquiries will be handled on first come first serve basis.
- * Beggars will be denied and blocked.
- * BTC only please.

We charge 0.0017 BTC per dose (vaccine or medicine), please calculate and send the necessary BTC amount to 1JCZ6RB5sXJnFVEZmjwe08jKRkrCv1H1ug and send all the necessary information below when sending an email to the address on the [Contact Us](#) page

Name and Last Name:
Gender:(Male / Female)
Age:
Email Address:
Physical Address:
Current Covid-19 Infection Status:(Positive / Negative)



SCAMMER REVENGE

Have you been scammed? With this service you can get revenge by hacking the scammer asking for a ransom to be sent to you.

120\$--600\$



PASSWORD RECOVERY

You will be able to recover your account password.

70\$--220\$



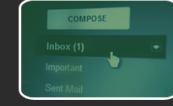
CUSTOM MALWARE/SOFTWARE

You'll have a group of hacker programmers ready to write



GRADES CHANGE

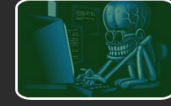
By using this service you will be able to change your school grade.



EMAILS HACKING

We have over 7.3 billion email records and corresponding passwords. If the email you are looking for is not among these data, you can always rely on our abilities.

190\$--270\$



WEBSITE/SERVER HACKING

XSS, CSRF, SQL inj, LDAP inj, CRLF inj --> are few vulnerabilities but they affect most websites. Not to mention the obsolete software installed on the servers.

170\$--600\$



2FA BYPASS

Tired of being blocked by 2FA? We can help you bypass it.



CUSTOM RANSOMWARE

Do you remember wannacry? They earned over \$ 100,000 from ransoms. The funniest thing is that they bought ransomware from us!

200\$--750\$

hackinstatgx13zk.onion/LeakedPass

Search Instagram Leaked Passwords **Vip Search** Purchase Terms FAQ **Combo Market** Hack Instagram Contact **News** Register

Login

Online Hash Crack Service
hashcrack25qkmjy.onion

Onion Bitcoin Wallet
onionbtcsbqctszc.onion

Minimum Wage

Search Instagram Users - Leaked Password Database

There are currently 430,949,291 accounts in Instagram Database
and about 10 billion accounts in our Leaked Database.

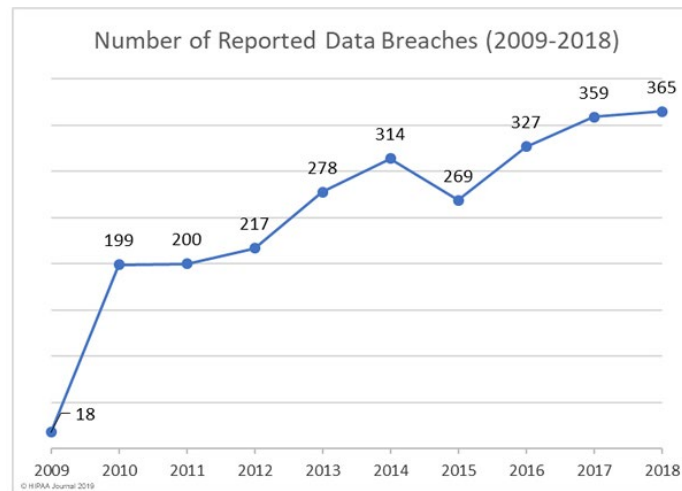


Maybe we are a Target?



41% of Healthcare Organizations have reported that they experienced a breach

https://www.beazley.com/news/2019/beazley_breach_insights_february_2019.html



2020 Major Breaches

- Name:** Trinity Health
Reported: 9/14/2020
Number of individuals affected: 3,320,726
- Name:** Inova Health
Reported: 9/09/2020
Number of individuals affected: 1,045,270
- Name:** Magellan Health
Reported: 6/12/2020
Number of individuals affected: 1,013,956
- Name:** Dental Care Alliance
Reported: 12/08/2020
Number of individuals affected: 1,004,304
- Name:** Luxottica of America
Reported: 10/27/2020
Number of individuals affected: 829,454
- Name:** Northern Light Health
Reported: 8/03/2020
Number of individuals affected: 657,392
- Name:** Health Share of Oregon
Reported: 2/05/2020
Number of individuals affected: 654,362
- Name:** Florida Orthopaedic Institute
Reported: 07/01/2020
Number of individuals affected: 640,000
- Name:** Elkhart Emergency Physicians
Reported: 05/28/2020
Number of individuals affected: 550,000

Threat Entry Points

- Phishing
- Connected Medical Devices (IoT)
- Social Engineering
- Misconfigured Servers
- Inadvertent Disclosures
- Unpatched Systems
- Vendors and Business Associates
- Facilities and other supporting systems



Frameworks and Legal Landscape

NIST Cybersecurity Framework



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.

- Perform a Business Impact Analysis
- What workflows are critical during an emergency?
- What systems and information are critical to supporting those workflows?

Identify



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.

- 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?

Protect

Topic	Questions
Identify	<ul style="list-style-type: none">• Are critical assets identified and their susceptibility to Ransomware assessed?
Protect	<ul style="list-style-type: none">• Are critical assets backed up? Are backups logically and physically separated from production systems?• Are critical assets on separate network segments?
Detect	<ul style="list-style-type: none">• Are systems in place to detect ransomware Indicators of Compromise (IOCs) so that it can be contained before it launches or spreads?
Respond	<ul style="list-style-type: none">• If critical assets are locked up, how will the organization respond?• How will the message be communicated externally?
Recover	<ul style="list-style-type: none">• Have you tested recovery plans for affected systems?

Reference & Title	Ransomware
§164.308(a): Security Management Process	Take steps to prevent, detect, contain and correct Ransomware
§164.308(a)(1)(ii)(A): Security Management Process -- Risk Analysis	Ransomware has been identified as a Top 5 Threat in healthcare
§164.308(a)(5)(ii)(B): Security Awareness, Training, and Tools -- Protection from Malicious Software	Train workforce on how to protect against Ransomware. This could include Phishing Campaigns.
§164.308(a)(6)(i): Security Incident Procedures	Implement Procedures for responding to Ransomware attacks
§164.308(a)(7)(ii)(A): Contingency Plan – Data Backup Plan	Backup data so that the organization can recover.
§164.308(a)(7)(ii)(D): Contingency Plan -- Testing and Revision Procedure	Test your plans to ensure you can actually recover. Note that modern Ransomware will attempt to lock up backups before taking the main system offline.

“Unless the covered entity or business associate can demonstrate that there is a “...low probability that the PHI has been compromised,” based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred.”

<https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
<https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx>
- Cybersecurity Reports and Tools
<https://www.phe.gov/Preparedness/planning/405d/Pages/reportandtools.aspx>



Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

online

Results. Guaranteed.

Prevention

- Practices to consider to address Ransomware
- Include:
 - Patching
 - Strong passwords with MFA
 - Anti-malware tools
 - Separate critical systems from threats
 - Asset Inventory
 - Tested backup and recover plan with offline backups

Threat: Ransomware Attack		
Vulnerabilities	Impact	Practices to Consider
Lack of system backup	Partial or complete clinical and service disruption Patient care and safety concerns Expenses for recovery The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	Ensure that users understand authorized patching procedures (7.S.A)
Lack of anti-phishing capabilities		Patch software according to authorized procedures (7.S.A)
Unpatched software		Be clear which computers may access and store sensitive or patient data (4.M.C)
Lack of anti-malware detection and remediation tools		Use strong/unique username and passwords with MFA (1.S.A, 3.S.A, 3.M.C)
Lack of testing and proven data back-up and restoration		Limit users who can log in from remote desktops (3.S.A, 3.M.B)
Lack of network security controls such as segmentation and access control		Limit the rate of allowed authentication attempts to thwart brute-force attacks (3.M.C)
		Deploy anti-malware detection and remediation tools (2.S.A, 2.M.A, 3.L.D)
		Separate critical or vulnerable systems from threats (6.S.A, 6.M.B, 6.L.A)
		Maintain a complete and updated inventory of assets (5.S.A, 5.M.A)
		Implement a proven and tested data backup and restoration test (4.M.D)
		Implement a backup strategy and secure the backups, so they are not accessible on the network they are backing up (4.M.D)
		Implement proven and tested incident response procedures (8.S.A, 8.M.B)
		Establish cyber threat information sharing with other health care organizations (8.S.B, 8.M.C)
		Develop a ransomware recovery playbook and test it regularly (8.M.B)
		Once ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures (HHS Ransomware Fact Sheet)

Table 3. Suggested Practices to Combat Ransomware Attacks

For additional information on activities to prepare for and respond to a ransomware attack, please see NIST Special Publication 800-184 – Guide to Cybersecurity Event Recovery at <https://csrc.nist.gov/publications/detail/sp/800-184/final>

- <https://www.cisa.gov/stopransomware>
- Ransomware prevention and response best practices
- **Services including FREE Vulnerability Scans and Penetration Tests for critical infrastructure, including healthcare**
- Outlines the role of law enforcement in responding to incidents

HOW DO I PROTECT MY NETWORKS?

A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
5. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
6. **Incident Response:** Do we have an incident response plan and have we exercised it?
7. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

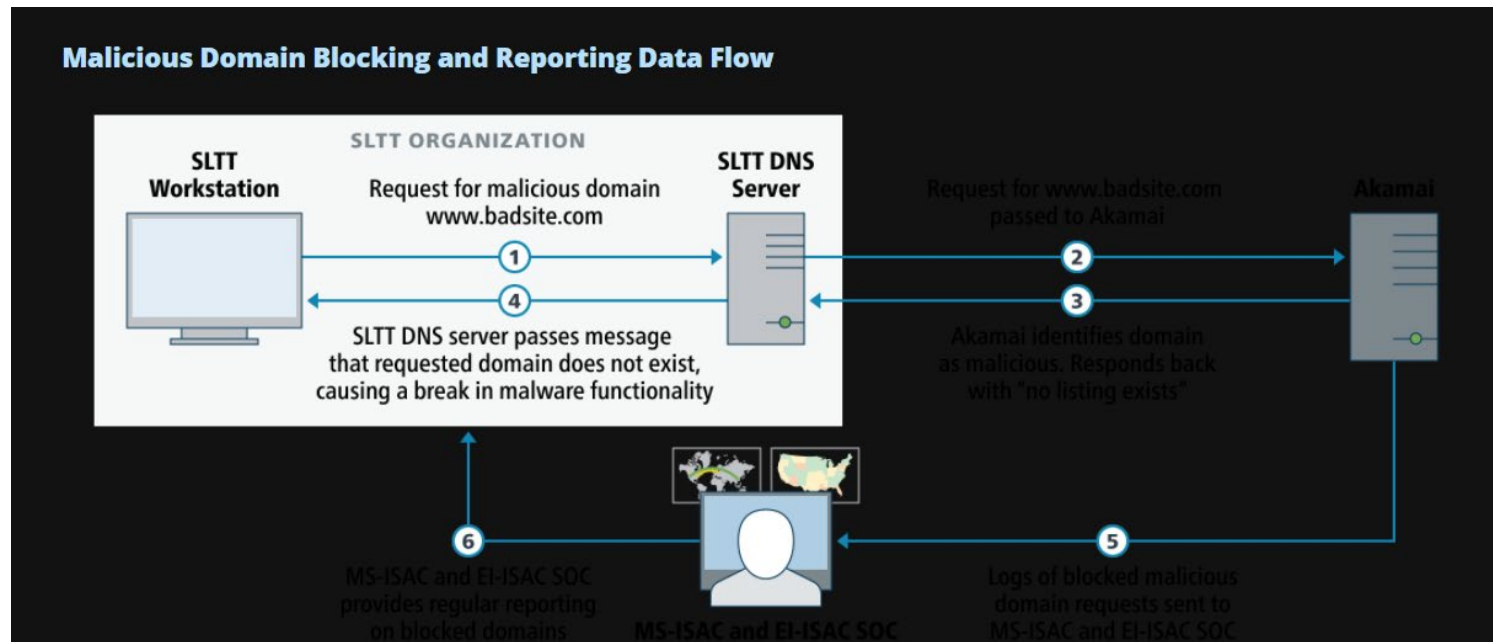
- <https://www.cisa.gov/stopransomware>
- Ransomware prevention and response best practices
- Services including FREE Vulnerability Scans and Penetration Tests for critical infrastructure, including healthcare
- Outlines the role of law enforcement in responding to incidents

HOW DO I PROTECT MY NETWORKS?

A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
5. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
6. **Incident Response:** Do we have an incident response plan and have we exercised it?
7. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

- <https://www.cisecurity.org/blog/ransomware-in-the-healthcare-sector/>
- **FREE Malicious Domain Blocking and Reporting for U.S. Hospitals**



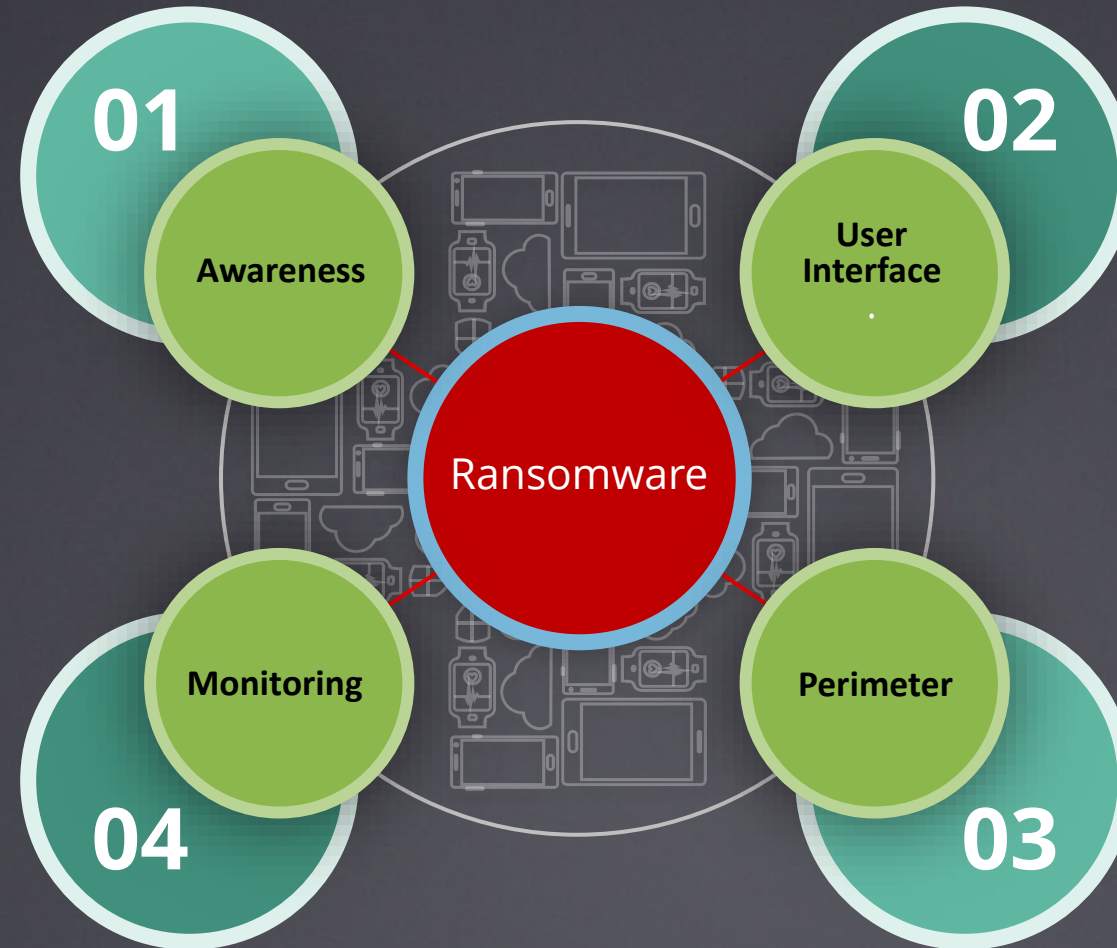
Security Measures

Awareness

- Security incident process
- Awareness emails
- Security web site
- Targeted campaigns
- Monthly newsletters
- Labs and direct training
- Incentives
- Third Party Training (KnowBe4)

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
- File and computer inspections

Perimeter

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

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


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

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

online

 Results. Guaranteed.



Response and Preparedness

Security Incident Procedures - §164.308(a)(6)

"Implement policies and procedures to address security incidents."

RESPONSE AND REPORTING (R) - § 164.308(a)(6)(ii)

"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

Definition of Security Incident:

"the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."



Maintenance

- Test Incident Response Plan through Tabletop Exercises
- Test likely scenarios (e.g. Ransomware, Phishing, Theft)
- Improve based on lessons learned
- Review documentation of security incidents to identify improvements
- Update/Review annually



Questions to ask yourself?

- How are we documenting security incidents?
- What is our communications plan? Internal/External?
- Who are the decision makers? For example, who has ultimate authority to shut down critical systems such as EMR in order to prevent further infection of malware?
- Do all employees know how to recognize a security incident, know their obligation to report, and know how to report?

Components of a Security Incident Response Plan

- Business Units/Locations with primary and backup contact names and numbers
- CIRT Team Members and Responsibilities (RACI Chart)
- Communications and Coordination Plans
- Security Incident Handling Procedures
- Security Incident Notification Plans
- Escalation Procedures
- Chain of Custody Procedures
- Critical Vendor, Service Provider, and Law Enforcement contact information
- Post Incident Activities



online

Results. Guaranteed.

Tabletop Exercise

Tabletop Exercise Goals

- Test the effectiveness of incident response and business continuity procedures
- Familiarize team members with steps to respond to and recover from an incident
- Identify areas of concern for the system's ability to detect and recover from an incident
- Elicit ideas to improve the plan





Tabletop Exercise Instructions

- The test has been designed to be realistic, however there may be parts of the exercise that are not realistic.
- Try to focus on the process and the dialogue and suggest improvements during the debriefing session afterward.
- Mistakes will likely be made, and plans will likely be missing key steps. Please note these as we go along for improving the plan and discuss during the debrief.
- As much as possible, role play and stay in the role during the exercise.
- Direct any questions to the test facilitator(s).

Tabletop Exercise Ground Rules

- There are no right or wrong answers. All ideas are welcome and will be captured and acted on as appropriate.
- Maintain a no-fault, stress-free environment. It's very important that today's discussion is driven by group decision making and problem-solving, so the environment in this room must remain open, positive and encouraging.
- Use the scenario to provide context and spark creative ideas. All ideas and thoughts should be based on the information provided by the scenario, but this should not limit your thinking.
- Do not limit the discussion to official positions or policies. Don't be afraid to go beyond your title/position as you think about the situations that are presented.

Incident Response Scenario – Ransomware Attack

-  A phishing email was sent to numerous members of the medical practice
-  One person clicked on the link and entered their credentials into the attacker's fake website
-  Shortly after, the victim's computer displayed a ransom message
-  The user reported the incident to the IT helpdesk

Incident Response Scenario – Ransomware Attack

- What is the impact to clinical care? Are there downtime procedures?
- How is the incident communicated internally? Externally?
- Can the systems be restored? What if the backups are wiped out?
- How is evidence maintained?
- How to determine whose information was breached?

Assessment

- Was the Incident Response Plan used?
- Who are the decision makers?
- How was the incident communicated internally and externally?
- Who was brought in to help respond?
- How did you determine if a breach occurred?
- Was information maintained for root cause analysis?
- What business considerations were used in making response decisions? Financial? Availability of Information?

Incident Response Scenario – Rogue Sys Admin

- System administrator was fired for not showing up to work for one week
- IT followed all access termination procedures
- The next day, user calls helpdesk to report that files have disappeared

Incident Response Scenario – Rogue Sys Admin

- Do you know that ALL accounts were properly terminated?
- Do you have an inventory of all systems and data?
- If the instance is wiped out, can it be recovered?
- Who do you call for help?

Assessment

- What was done differently this time?
- Was the Incident Response Plan used?
- Who are the decision makers?
- How was the incident communicated internally and externally?
- Who was brought in to help respond?
- How did you determine if a breach occurred?
- Was information maintained for root cause analysis?
- What business considerations were used in making response decisions?
Financial? Patient Care? Availability of Information?

Conclusion

- Consider what types of emergencies or incidents are likely to occur in your organization and the cybersecurity ramifications
- Have your response plans ready and tested
- Know roles and responsibilities for your organization (Hint: this isn't just an IT problem)
- Know when and how to reach out to experts

-
- NIST CSF – <https://www.nist.gov/cyberframework>
 - HIPAA Security Rule – <https://www.hhs.gov/hipaa/for-professionals/security/index.html>
 - HICP: Managing Threats and Protecting Patients
<https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx>
 - CISA Stop Ransomware - <https://www.cisa.gov/stopransomware>
 - CIS Ransomware in Healthcare -
<https://www.cisecurity.org/blog/ransomware-in-the-healthcare-sector/>

A blurred background image showing several people in a meeting or conference room. They appear to be looking at a screen or document. The image is dark and out of focus, serving as a backdrop for the text.

Thank You