From Digital to Physical Disaster: The Impact of Ransomware Attacks on Hospitals and Health Systems

Hacking Incidents Reported to OCR

2020 Total: 425 Breaches Impacting 26.7 Million Individuals

1/1/2021 - 8/30/2021
331 Breaches Impacting 32.4 Million Individuals

California: 31 Breaches Impacting 2.4 Million Individuals

Attack Patterns – Priority Risks

#1 Priority - High impact ransomware attacks especially those that result in a regional or statewide disruption of care delivery

2) Cyber risk exposure and impact through business associates:
   - Theft of large quantities of covered entity data in possession of business associates
   - Business associate as digital pathway into covered entity
   - Mission critical business associate becomes victim of ransomware attack

3) Theft of PHI and medical research related to COVID-19 treatment protocols and COVID-19 vaccine development from hospitals/health systems directly.
Nebraska Medicine was victim of cyber attack

UHS says all U.S. facilities affected by apparent ransomware attack

Cyberattack hobbles major hospital chain

“We are most concerned with ransomware attacks which have disrupted patient care operations and risk patient safety,” said an cybersecurity adviser to hospitals. “We believe any cyberattack on a hospital or health system is a threat to life and should be pursued as such by the government.”

Frank Bajak | Sep 23

Claims Journal - John Riggi, senior cybersecurity adviser to the American Hospital Association, called it a “suspected ransomware attack” after reporting on social media site Reddit by people

‘We got taken down’: UVM Medical Center says cyberattackers were likely after money

Cyberattack on UVM Health Network impedes chemotherapy appointments

The cyberattack has halted chemotherapy, mammogram and screening appointments, and led to 300 staff being furloughed or reassigned.
National Disruption of Healthcare

The Irish Government Refuses to Pay the Ransom

“A ransomware attack on a hospital crosses the line from an economic crime to a threat-to-life crime; these attacks should therefore be aggressively pursued and prosecuted as such.”

“...additional safe harbor protections from civil and regulatory liability be provided to hospital and health system victims of cyberattacks.”
• A ransomware attack on a hospital or health system crosses the line from an economic crime to a threat-to-life crime.

• This is a national security threat.

• The vast majority of these attacks originate from outside the United States.

• The AHA has urged the government to embark upon a coordinated whole of government and a whole of nation campaign.

“We’ve got to recognize these ransomware attacks for what they are. It’s a serious national security threat,” said Sen. Rob Portman, a Republican from Ohio. “Attacks against critical infrastructure are not just attacks on companies. They are attacks on our country itself.”
Reuters last week reported that the U.S. Justice Department is elevating the priority of ransomware investigations similar to those of terrorism attacks following a May 7 attack on the Colonial Pipeline and damage to other sectors. The department this week announced it had seized $2.3 million in bitcoin proceeds allegedly from the attack.

“The AHA has been leading a call to the government to pursue a coordinated campaign to disrupt these criminal organizations and seize their illegal proceeds, as was done so effectively during the global fight against terrorism,” said John Riggi, AHA senior advisor for cybersecurity and risk. “We have good reason to believe that our persistent advocacy and expert point of view on this issue helped influence this policy change.”

- **We need to do our part to defend against these threats with all available technical, human and financial resources.**
- **We continue to call on the government to embark on a coordinated campaign utilizing all diplomatic, financial, law enforcement, intelligence and cyber military capabilities to disrupt these criminal organizations, seize their illegal proceeds and increase consequences for those nations which harbor them - as we effectively did in the global fight against terrorism.**

Encouraging to see the Federal Bureau of Investigation (FBI) and the U.S. Department of Justice recently raise the investigative priority level of ransomware attacks to the same level as terrorist attacks. We are moving in the right direction.”

June 23, 2021
https://video.foxbusiness.com/v/6260730434001#sp=show-clips
..regardless of whether or not a victim chooses to pay, our goal is to identify, pursue, and impose consequences on criminal actors, not their victims."

The FBI strongly encourages victims to report ransomware incidents to the FBI.
Cybersecurity

Ransomware Gang REvil Vanishes From Web After Biden Warning

By William Turton
July 13, 2021, 10:01 AM EDT  Updated on July 13, 2021, 11:11 AM EDT

► Unclear if sites taken down voluntarily or by law enforcement
► Hacking group hit meat supplier JBS, Kaseya in recent weeks

The Russia-linked ransomware gang REvil has seemingly vanished from the dark web, where it maintains several pages documenting its activities including one called the “happv blog.”
Memorial Health System experiences cyber attack

Surgeries canceled, ambulances diverted, IT system down at Ohio health system after ransomware attack

Marietta, Ohio-based Memorial Health System is diverting some patients after a ransomware attack that forced it to shut down its IT systems, according to an Aug. 16 Marietta Times report.

Russian Ransomware Group REvil Back Online After 2-Month Hiatus

The operators behind the REvil ransomware-as-a-service (RaaS) staged a surprise return after a two-month hiatus following the widely publicized attack on technology services provider Kaseya on July 4.
**Ransomware Awareness for Holidays and Weekends**

**SUMMARY**

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends—when offices are normally closed—in the United States, as recently as the Fourth of July holiday in 2021. The FBI and CISA do not typically have any specific threat reporting indicating a cyberattack will occur over the upcoming Labor Day holiday. However, the FBI and CISA are sharing the below information to provide awareness to be especially diligent in your network defense practices in the run up to holidays and weekends, based on recent actor tactics, techniques, and procedures (TTPs) and cybertargets during holidays and weekends during the past few months. The FBI and CISA encourage all entities to exercise their current cyberdefense posture and implement the recommended best practices and mitigations to manage the risk posed by all cyber threats, including ransomware.

**THREAT OVERVIEW**

Recent Holiday Targeting

Cyber actors have continued to conduct increasingly impactful attacks against U.S. entities on or around holiday weekends over the last several months. The FBI and CISA do not currently have specific information regarding cyber threats coinciding with upcoming holidays and weekends. Cyber criminals, however, may view holidays and weekends—especially holiday weekends—as attractive timeframes in which to target potential victims, including small and large businesses. In some cases, this tactic provides a head start for malicious actors conducting network exploitation and follow-on propagation of...

**Immediate Actions You Can Take Now to Protect Against Ransomware**

- Make an offline backup of your data.
- Do not click on suspicious links.
- If you use RDP, secure and monitor it.
- Use strong passwords.
- Use multi-factor authentication.

**RECOMMENDED MITIGATIONS**

- Your IT and CISO should tightly secure network infrastructure and access for ransomware that may target the following:
  - E-mail and cloud storage platforms, including email accounts, file storage, and data
  - Web applications and services, including webmail accounts and services
  - File sharing services, including cloud storage, file sharing, and secure messaging
  - Mobile devices, including smartphones and tablets
  - IoT devices, including smart home devices and industrial control systems

- Use a tool such as F-soar to detect and respond to ransomware.
- Use a tool such as F-soar to detect and respond to ransomware.
- Use a tool such as F-soar to detect and respond to ransomware.
- Use a tool such as F-soar to detect and respond to ransomware.

**Ransomware Trends 2020 - 2021**

- Attacks are highly targeted against specific healthcare entities
- Phishing emails is still the primary “attack vector” – because it’s simple and it work, followed by remote access, unpatched vulnerabilities and compromised credentials
- Increasing in sophistication and severity. Ryuk, Conti and DopplePaymer, Mamba, Nefilim, REvil
- Network and data backups may be targeted first
- Ransomware may now execute within hours or minutes upon initial compromise leaving very little reaction time to identify and contain
- Ransom demands are increasing and scaled based upon size of organization targeted, multi-million dollar requests common, reports of ransom demands exceeding $60,000,000 in 2020
- High volume/disruptive telephone calls to executives and staff demanding ransom payment
- Ransomware attack combined with other cyber crimes - data extortion. Criminals threaten to sell /publish stolen patient data
Ransomware Impact 2020 -2021

- Disruption to patient care and business operations – *Patient safety issue*
- Telemetry systems inoperable – nurse must be present for critical patients
- EMR rendered inaccessible – treatment and drug allergies / interactions unknown – delay in rendering care
- Lab results and imagery unavailable
- Surgeries and cancer treatments cancelled or delayed
- *ED’s shutdown - Ambulances placed on full divert - delay of emergency treatment – Rural Impact – Regional Impact – Level 1 Trauma Center – Golden Hour, stroke patients, bad weather, could eliminate medivac option and increase diversion transport time*
- *Ransomware “blast radius” – dependent providers and third parties, also disrupted*
- Recovery time from ransomware attacks, even if able to restore from unaffected backups, minimum 3-4 weeks - residual impacts lasting up to 6 months
- Increased insurance premiums
- Increase in credit risk leading to increase in cost of financing
- Lost revenue implications, burn rate, and of course:
  - Reputational harm - loss of patient, community and investor confidence

Combating Ransomware

A Comprehensive Framework for Action: *Key Recommendations from the Ransomware Task Force*

- **21 DAYS**
  - Average downtime due to ransomware attacks
    - (Coveware)
- **287 DAYS**
  - Average days it takes a business to fully recover from an attack
    - (Emsisoft)
- **$350 MILLION**
  - Victims paid in ransom in 2020 – a 31% increase over the prior year
    - (Chernaya)
- **$312,493**
  - The average payment in 2020 – a 171% increase compared to 2019
    - (Palo Alto Networks)

In 2020, nearly **2,400** U.S.-based governments, healthcare facilities, and schools were victims of ransomware
Contributing Factors 2020 -2021

- Email – Phishing Attack. Need for increased employee awareness and training
- Email – Insufficient email technical security controls. Need for increased email advanced threat protection, behavior and signature based, quarantine of attachments, safe links
- Lack of multifactor authorization (MFA) for remote access of networks, VPN, and email. Institute MFA for all categories of remote access – Then internally for all system administrative privileges
- "Flat" networks. Need for network segmentation
- Lack of real time 24/7 log, event, incident and alerts monitoring. Need full time internal or external Managed Detection and Response (MDR) service

Contributing Factors 2020 -2021 (cont.)

- Insufficient or delayed leadership notification, response and/or emergency containment actions. Need updated, organization wide, routinely tested cyber incident response plan, with clear lines of designated and delegated emergency action authorities.
  - Inability to restore from backups. Need to ensure backups are offline, network segmented, multiple copies on prem and in cloud, highly secure, no remote access, MFA, 3-2-1 rule.
  - Unprepared for a multi-week or multi-month IT disruption. Need contingency plans for continuity of patient services, imaging, lab results, documentation on paper, revenue cycle disruption, 3rd party dependencies.
- Insufficient cyber insurance coverage hindering response and recovery efforts. Conduct review of cyber insurance coverage for limitations, exclusions, ransomware coverage, forensics firms capabilities, bitcoin.
Good News, Helpful Strategies and Resources

Below you will find the U.S. Government’s recommended best practices — we’ve selected a small number of highly impactful steps to help you focus and make rapid progress on driving down risk.

What We urge You To Do Now

Implement the five best practices from the President’s Executive Order: President Biden’s Improving the Nation’s Cybersecurity Executive Order is being implemented with speed and urgency across the Federal Government. We’ve outlined five key steps to protect against ransomware and denial of service attacks. These steps are critical because of the threat’s persistence and the unique vulnerability of hospitals and other critical infrastructure organizations.

Backup your data. System images, and configurations, regularly test them, and keep the backups offline. Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups. Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems.

Update and patch systems promptly. This includes maintaining the security of operating systems, applications, and firmware, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to drive your patch management program.

Test your incident response plan. There’s nothing that shows the gaps in plans more than testing them. Run through some core questions and use those to build an incident response plan. Are you able to sustain business operations without access to certain systems? For how long? Would you turn off your manufacturing operations if business systems such as billing were offline?

Check Your Security Team’s Work. Use a 3rd party pen tester to test the security of your systems and your ability to defend against an sophisticated attack. Many ransomware criminals are aggressive and sophisticated and will find the equivalent of unlocked doors.

Segment your network. There’s been a recent shift in ransomware attacks — from stealing data to disrupting operations. It’s critically important that your corporate business functions and manufacturing/production operations are separated and that you carefully filter and limit internet access to operational networks. Identify links between these networks and develop workarounds or manual controls to ensure ICS networks can be isolated and continue operating if
Recommended Mitigations

- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
- Use two-factor authentication with strong passwords, including for remote access services.
- Monitor cyber threat reporting regarding the publication of compromise credentials and change passwords/ settings if applicable.
- Keep computers, devices, and applications patched and up-to-date.
- Install and regularly update anti-virus or anti-malware software on all hosts.

Review the following additional resources.

- The joint advisory from Australia, Canada, New Zealand, the United States on Technical Approaches to Uncovering and Remedying Activity provides additional guidance when hunting or investigating common mistakes to avoid in incident handling.
- The Cybersecurity and Infrastructure Security Agency-Multi-State & Analysis Center Joint Ransomware Guide covers additional best practices to prevent, protect, and respond to a ransomware attack.
- StopRansomware.gov is the U.S. Government’s official one-stop forum for resources to tackle ransomware more effectively.

Information Requested

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom also does not guarantee that a victim’s files will be recovered. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. Regardless of whether you or your organization decide to pay the ransom, the FBI urges you to report ransomware incidents to your local field office. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

The FBI may seek the following information that you determine you can legally share, including:

- Recovered executable files
- Live memory (RAM) capture
- Images of infected systems
- Malware samples
- IP addresses identified as malicious or suspicious
- Email addresses of the attackers
- A copy of the ransom note
- Ransom amount
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom
- Post-incident forensic reports

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI’s 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI’s National Press Office at (202) 324-3901.
Cybersecurity bill with AHA-supported provisions signed into law Jan. 05 2021

President Trump yesterday signed into law a bill (H.R. 7898) PL 116-321 containing provisions that require the Secretary of Health and Human Services to consider certain recognized cybersecurity best practices when making determinations against HIPAA-covered entities and business associates victimized by a cyberattack. For example, the bill recognizes cybersecurity practices established under the National Institute of Standards and Technology Act and approaches established under Section 405(d) of the Cybersecurity Act of 2015 by the Healthcare and Public Health Sector Coordinating Council (HSCC) Working Group, whose members include the AHA. The HSCC expressed strong support for the provisions. The legislation cleared the Senate by unanimous consent on Dec. 19.

• Recognized Cybersecurity Practices in Place Previous 12 months
• Reduced Fines
• Early, Favorable Termination of Audits
• Mitigation of other penalties
• No Increased Penalties for Not Having Recognized Cybersecurity Practices in Place

“This law will have long lasting positive impact for the entire health care sector in securing patient data and protecting patients from cyber risks,” said John Riggi, AHA senior advisor for cybersecurity and risk. “The law provides the right balance of incentivizing voluntary, enhanced cybersecurity protocols in exchange for regulatory relief and recognition that breached organizations are victims, not the perpetrators.”

Risk Tolerance and Cyber Insurance

• How much cyber risk are we willing to accept?
• How much risk are we willing to transfer?
• Do we have cyber insurance?
• What are the limitations and requirements?
• Vendor and subcontractor requirements?
• Scales with VRM risk prioritization
• Is our cyber insurance coverage adequate and current to cover all costs associated with a:
  o Multi-day network outage
  o Breach mitigation and recovery
  o Lost revenue
  o Reputational harm
  o Legal and regulatory exposure
  o Victim and patient services – credit monitoring
• Forensics firms panel – integration with IRP
• Interaction and integration with other insurance policies
• Ransomware coverage – bitcoin
• “Act of war” exemption for cyber?
“VMware Carbon Black found there were 239.4 million attempted attacks on the firm’s healthcare customers in 2020, a nearly 10,000 percent increase from 2019, according to Moody’s.”

Strategic Vendor Risk Management Program Considerations

- Does your organization have a vendor risk management program (VRM)? What is the governance structure and does that structure still make sense?
- Is there a formal process to incorporate cybersecurity in the VRM program?
- Is there process to conduct periodic in-depth technical, legal, policy and procedural review of the VRM program and the BAA?
- Does the BAA include cybersecurity and cyber insurance requirements for the vendor and any subs of the vendor? Are the coverages and limits sufficient?
- Annual cyber risk assessments for vendors?
- Compliance requirements with applicable regulatory standards - HIPAA, PCI, PII, taxpayer funded medical research and IP?

Strategic Vendor Risk Management Program Considerations (cont.)

• Identify, risk classify and risk prioritize vendors and their subcontractors based upon:
• Aggregation of data – regulated data and unregulated data such as pop health genetic studies, clinical trials, COVID-19 research
• Access to sensitive data, networks, systems and physical locations
• Criticality/Impact to continuity of operations - Clinical, facilities, utilities, business (e.g. telecom, medical transcription, billing and coding, PPE supplies, etc)
• Foreign operations and foreign subcontractors
• Implement risk based controls and cyber insurance requirements
• Need to balance financial opportunities and greater supply-chain flexibility with potentially higher cyber risks associated with certain vendors

Cyber Incident Response Plan

• Backup status and security, 3-2-1, restoration point and time, offline?
• Do we have a unified cyber-incident response plan & is it up to date?
• Multi-day impact and multi-incident plan?
• Does it include specific individuals from all clinical, business, admin and facilities functions - with defined roles, responsibilities and off hours contact information and plan access?
• Activation and decision escalation protocol and matrices?
• Leadership role – designation and delegation of critical authorities?
• Is the plan regularly tested, gaps and best practices identified and updated to include current threat scenarios such as ransomware?
• Legal, regulatory, financial and reputational risks?
• Internal and external communications strategy?
• Out of band communications?
• Paper copies and downtime procedures?
• Continuity of operations – emergency management?
• Cyber insurance requirements – forensics firm?
• FBI, government and forensics firm integration?
Thank You

John Riggi
Senior Advisor for Cybersecurity and Risk
American Hospital Association
jriggi@aha.org
(O) +1 202-626-2272