# Executive Summary of Reference Material

*Friday, September 9th, 2022 from 9:30 am – 10:45 am PT*

The following information is provided to inform recipients of current global cyber threats posing risk to U.S. healthcare. The attached also provides a snapshot of relevant cyber legislative and policy issues.

Included please find the following documents:

On 8/24/2022, AHA released a cybersecurity podcast: **"Preparing for Cyberattacks with Northwell Health"** where John Riggi, moderated a discussion with Kathy Hughes, Vice President & Chief Information Security Officer and Brian O'Neill, Vice President for Crisis Management, about how hospitals and health systems can create a stronger cybersecurity posture to protect their expanded networks, their data, and most importantly, their patients and the communities they serve.

The FBI and Cybersecurity and Infrastructure Security Agency **urged** organizations on 8/12/2022 to take steps to protect against Zeppelin ransomware attacks, which use remote desktop protocol and firewall vulnerabilities and phishing campaigns to access victim networks and deploy ransomware.

"The Zeppelin 'Ransomware as a Service' is especially targeting health care and medical organizations," said John Riggi, AHA national advisor for cybersecurity and risk. "The alert contains very detailed and actionable indicators of compromise which should be immediately loaded in organizations network defense systems. Along with encrypting files, this gang is engaging in the 'double layered' data extortion method. It appears this gang is stealing and threatening to publicly release sensitive information such as patient information, payroll, human resources and non-disclosure-protected information. Thus, even if a victim organization can independently restore encrypted files from backup, they face the dilemma of potential public release of stolen information in the possession of the criminals. The AHA, along with the federal government, strongly discourages the payment of ransom. This alert along with the comprehensive #stopransomware site provide extensive guidance on how to protect your systems from ransomware and avoid the ethical and legal dilemma of 'pay, not pay.'

**Federal agencies** in July 2022 recommended U.S. health care organizations take certain actions to protect against the Maui ransomware threat.

"The Maui ransomware identification and funds seizure is a great example of how important it is for hospital and health system victims of cyberattacks to engage in timely and active cooperation with the FBI," said John Riggi, AHA's national advisor for cybersecurity and risk. "Not only did it assist the individual victims, but it also provided critical pieces of the intelligence 'puzzle' for the FBI. This allowed the FBI to inflict some consequences on the Maui bad actors and prevent additional attacks against health care by disseminating actionable intelligence to the field on the threat. Make no mistake, the Maui ransomware not only represents a threat to health care, but it also represents a national security threat. The North Korean regime, a designated state sponsor of terrorism, has a history of engaging in global criminal activity to fund its own illicit activities, including its nuclear weapons program. The American Hospital Association works very closely with the FBI on the local and national level to exchange cyber threat information, and we encourage all hospitals and health systems to develop working relationships with their local FBI and CISA offices — before becoming a victim of a cyberattack."

On 7/19/2022 the **Justice Department announced** the recovery of about $500,000 in ransom that a Kansas hospital and Colorado medical provider paid to state-sponsored North Korean hackers.

"Thanks to rapid reporting and cooperation from a victim, the FBI and Justice Department prosecutors have disrupted the activities of a North Korean state-sponsored group deploying ransomware known as 'Maui,'" said Deputy Attorney General Lisa O. Monaco at the International Conference on Cyber Security on 7/19/2022. "Not only did this allow us to recover their ransom payment as well as a ransom paid by previously unknown victims, but we were also able to identify a previously unidentified ransomware strain."

Dissemination and coordination of cyber threat intelligence from FBI, CISA and DOJ resulting in the AHA issuing a **Cybersecurity Advisory** on 7/6/2022. The AHA is closely monitoring the potential for increased ransomware attacks on health care and public sectors due to the North Korean 'Maui' ransomware. The bureau

said the threat stems from the North Korean state-sponsored "Maui" ransomware platform, which has been in use by cyber actors since at least May 2021. The FBI, jointly with the Cybersecurity and Infrastructure Security Agency and the Department of the Treasury, released resources, tactics, techniques and procedures, along with indicators of compromised systems, with the recommendation that organizations apply mitigation strategies and not pay ransom demands.

**The Senate Health, Education, Labor and Pensions Committee** held a hearing on how to strengthen cybersecurity in the health care and education sectors, from training and recruiting more cyber security experts to helping organizations share information. In her opening statement, Chairman Patty Murray, D-Wash., noted that 70% of hospitals surveyed in 2020 reported facing a significant cybersecurity incident.

John Riggi, AHA's national advisor for cybersecurity and risk, said, "The AHA applauds the committee's attention to the impact of cyberattacks on hospitals and appreciates the testimony of our colleague and partner Denise Anderson from the H-ISAC. The AHA has for years strongly advocated, including before the Senate, that ransomware attacks on hospitals disrupt and delay patient care delivery and risk patient safety. The AHA also works in close partnership with the H-ISAC to disseminate the latest technical threat intelligence, which can be found here."

**The National Security Agency, Cybersecurity and Infrastructure Security Agency and FBI** issued an alert on 6/10/2022 urging U.S. organizations to apply available patches, replace end-of-life infrastructure and implement a centralized patch management program to protect their networks from common cyber vulnerabilities that Chinese state-sponsored actors continue to exploit.

John Riggi, AHA's national advisor for cybersecurity and risk, said, "This joint agency advisory is an excellent summary of the government's declassified information on how the Chinese government conducts cyber espionage campaigns and which information technology vulnerabilities it most commonly exploits to penetrate computer networks. Note that the tactics include disguising and routing malicious traffic through non-Chinese infrastructure so as to avoid suspicion, and that the Chinese government continues to exploit home routers, which is of significant concern in this era of the remote work environment. Remote access to sensitive patient data and medical research by off-site staff and third parties should be strictly limited and closely monitored. According to previous U.S. government alerts, the Chinese intelligence services continue their aggressive pursuit of U.S. genetic data and medical research, including that related to precision medicine and infectious diseases. Patching of the identified vulnerabilities related to Chinese espionage campaigns should be implemented as soon as possible."

A **FBI TLP White Joint Cybersecurity Advisory: Weak Security Controls and Practices Routinely Exploited for Initial Access** alert was issued on 5/17/2022. The Joint Cybersecurity Advisory was coauthored by the cybersecurity authorities of the United States, Canada, New Zealand, the Netherlands, and the United Kingdom. Cyber actors routinely exploit poor security configurations (either misconfigured or left unsecured), weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a victim's system. This joint Cybersecurity Advisory identifies commonly exploited controls and practices and includes best practices to mitigate the issues.

Best Practices to Protect Your Systems:

- Control access.
- Harden credentials.
- Establish centralized log management.
- Use antivirus solutions.
- Employ detection tools.
- Operate services exposed on internet-accessible hosts with secure configurations.
- Keep software updated.

**PATCH Act Seeks to Shore Up Security for Medical Devices, Io T Networks 4/1/2022.** The PATCH Act closely mirrors what the AHA has been advocating the FDA implement since 2018. The new Protecting and Transforming Cyber Health Care Act would implement a series of new requirements for medical device and network security.

The bipartisan bill was introduced in the Senate this week by Sens. Tammy Baldwin, D-Wisconsin, and Dr. Bill Cassidy, R- Louisiana. There is already companion legislation in the House of Representatives sponsored by Reps. Dr. Michael C. Burgess, R-Texas, and Angie Craig, D-Minnesota. The aim is to "help ensure that the U.S. healthcare system's cyber infrastructure remains safe and secure" even as ransomware and other cyberattacks have increased in scope and severity in recent years.

The PATCH Act would:

- Impose a series of cybersecurity requirements for manufacturers applying for premarket approval through the Food and Drug Administration
- Enable manufacturers to design, develop and maintain processes and procedures to update and patch the device and related systems throughout device lifecycles
- Establish a Software Bill of Materials for devices that will be provided to users
- Require development of plans to monitor, identify and address postmarket cybersecurity vulnerabilities
- Request a Coordinated Vulnerability Disclosure to demonstrate safety and effectiveness of a device

**AHA-supported Cybersecurity Bill Clears Committee on 3/30/2022.** Developed from direct input from John Riggi, national advisor for cybersecurity and risk, in conversations with Senate staff suggesting that requirements be put on government agencies to assist instead of requirements solely being placed on the healthcare sector. The Senate Committee on Homeland Security and Governmental Affairs voted to advance as amended the **Healthcare Cybersecurity Act (S.3904)**, an AHA-supported legislation that would improve collaboration and coordination between the Cybersecurity and Infrastructure Security Agency and Department of Health and Human Services. The bill also would authorize cybersecurity training and an analysis of cybersecurity risks for the health care and public health sector, with a focus on impacts to rural hospitals, medical devices and cybersecurity workforce shortages.

**At a House Judiciary Committee hearing on 3/29/2022,** FBI Cyber Division Assistant Director Bryan Vorndran said disruptive cyber threats have targeted hospitals during the COVID-19 pandemic and credited the agency's strong relationship with the AHA for helping to disseminate cyber threat intelligence to the field. **PL 116-321 (HR 7898) Signed into law on 1/5/2021.** In sum the law directs HHS to provide regulatory relief for HIPAA covered entities which become victim of cyber-attack, if they have had recognized cybersecurity practices in place for the previous 12 months. The recognized cybersecurity practices are as defined by the National Institute for Standards and Technology (NIST) and the Healthcare Industry Cybersecurity Practices developed under section 405(d) of the Cybersecurity Information Sharing Act of 2015. If a cyber-attack victim can demonstrate the practices have been in place, HHS is directed to:

- Reduced fines
- Provide early, favorable termination of audits
- Mitigate other penalties otherwise provided
- No increase of penalties for not having recognized cybersecurity practices in place

The AHA was a significant contributor to the development of the **ASPR TRACIE Healthcare System Cybersecurity Readiness & Response Considerations** resource which is designed to help healthcare providers prepare for and respond to ransomware attacks. The information contained within the document is specifically related to the effects of a disruptive cyber-attack on the healthcare operational environment, specifically the ability to effectively care for patients and maintain business practices and readiness during such an event. AHA and National Advisor Riggi assisted in the development of this guide.

The **CISA Insights report "Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm"** a groundbreaking qualitative and quantitative analysis, which models and measures hospital strain associated with excess deaths, as well as the effect of ransomware and the impact such a strain can have on a hospital and region, further contributing to excess deaths. This report tends to corroborate what to many is intuitive - ransomware attacks on hospitals may disrupt care delivery, risk patient safety and are threat to life crimes. AHA provided input and guidance to CISA on this issue and helped promote the report and its findings.

University of Vermont Medical Center was a victim of a cyberattack with wide-ranging consequences. A **UVM ASCO article "Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect"** details the immediate challenges faced by UVM including the impact to cancer care during the cyberattack and the timeline of the complete shutdown until restoration.

On **4/6/2022 AHA released a special cybersecurity podcast:** Lessons Learned from a Ransomware Attack at UVM Health where John Riggi, moderated a discussion with UVM Health, Dr. Stephen Leffler, President and Chief Operating Officer and Dr. Douglas Gentile, Chief Medical officer, about what they learned from the major ransomware attack at UVM Health in Fall 2020.

The following is a **NPR article "Hackers disrupt payroll for thousands of employers – including hospitals."** A ransomware attack that happened mid-December 2021 affected the Kronos Private Cloud solutions, disrupting scheduling, timekeeping and payroll at many hospitals and health systems across the US. This is attack also highlights the need to have in place robust downtime procedures, redundancy and business continuity plans to sustain a loss of, on premises or cloud-based, mission-critical services or technology, for up to four to six weeks. The AHA's prominent public advocacy through the media and government channels resulted in Kronos establishing a separate group to focus on restoration of services to hospitals, health systems and all organizations involved in the maintenance of public health and safety.

For more information on these or other cybersecurity and risk matters visit www.aha.org/cybersecurity and feel free to contact John Riggi, AHA National Advisor for Cybersecurity and Risk, with questions at jriggi@aha.org.