SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE RAPIDLY EVOLVING AND CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog April 2024

THE CHANGE HEALTHCARE RANSOMWARE ATTACK: WHAT THIS MEANS FOR MEDICAL DEVICE MANUFACTURERS

ATTACK AND CONTINUING FALLOUT

The messy fallout from the February ransomware attack on Change Healthcare continues to develop and provides an opportunity to examine the current state of healthcare cybersecurity from patient, business, regulatory and cyber criminal viewpoints. First the facts: On February 21st Change Healthcare isolated their systems following identification of a cybersecurity incident. Hospitals, healthcare systems and pharmacies reported ongoing disruptions to Change Healthcare services On February 26th a ransomware group known as "BlackCat"(Also known as ALPHV) claimed responsibility for the attack. In early March APLHV/BlackCat received a payment of over $20 million in Bitcoin, which UnitedHealh Group (the parent company of Change Healthcare) refused to confirm was a ransomware payment. On April 7th RansomHub, a dark web site that sells stolen data and facilitates ransomware attacks, claimed that it had "over 4 TB of highly selective data" from the United Healthcare breach and set an April 20th deadline for further payment from Change Healthcare or else the data would be sold to the highest bidder. In the time since the attack, which "reportedly affected billing and care authorization portals", healthcare entities have dealt with disrupted services and significant financial losses. The Massachusetts Health and Hospital Association estimated in mid-March that the associated costs from the cyberattack for the Massachusetts healthcare system were approximately $24 million a day, and cybersecurity firm First Health Advisory estimated in early March that healthcare providers are losing more than $100 million a day. UnitedHealth continues attempts to restore services and provide workarounds and has advanced at least $2 billion dollars to providers.

Any ransomware attack in the healthcare sector will have two primary concerns for patients: Disruption to the ability to provide medical care and the breach of personal information including PHI. RansomHub has made it clear that they are in possession of patient data, telling UnitedHealth Group "You have one chance in protecting your clients' data". As of April 2nd there are 24 class-action lawsuits stemming from the cyberattack. 13 of the lawsuits were from consumers regarding the data breach, while the remaining 11 were from healthcare providers who are having disruptions regarding receiving payment. Change Healthcare is attempting to consolidate the lawsuits.

SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE RAPIDLY EVOLVING AND CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog April 2024
THE CHANGE HEALTHCARE RANSOMWARE ATTACK: WHAT THIS MEANS FOR MEDICAL DEVICE MANUFACTURERS

TO PAY OR NOT TO PAY?

Ransomware payments have long been a source of contention between private industry and federal entities (explored in depth in February's blog). The extortion attempts by ALPHV/BlackCat and subsequently RansomHub have painted a convoluted picture of the cybercriminal landscape and seem to lend credence to those calling for a ban on ransomware payments, often federal entities and including industry leaders such as the Ransomware Task Force which has released a "Roadmap to Potential Prohibition of Ransomware Payments". Among the primary arguments of those advocating for a ban of ransomware payments by victims is that there is "no honor among thieves". There are no guarantees that cybercriminals will uphold their end of the bargain upon receiving payment, and may attempt to "double extort" victims who they now know are likely to pay. Those resistant to a ransomware payment ban believe that ransomware actors need to rely on their reputations and that a verifiable history restoration of services following payment serves to entice victims to pay and pay quickly. It is not clear how RansomHub came to be in possession of the Change Healthcare data: Cyberscoop reports that theories include an ALPHV/BlackCat associate taking the information to RansomHub following a dispute with ALPHV/BlackCat regarding the division of the initial ransom payment, ALPHV/BlackCat attempting a double extortion under a different name following what is thought to have been a fraudulent "exit scam" in early March in which they made it appear as if their website had been seized by law enforcement. It is also possible that RansomHub doesn't even have the data and is bluffing in an attempt to piggyback on the original successful extortion attempt. If RansomHub does indeed have the data it raises question about how many other entities have access to the data and could attempt further extortion attempts, or could release the data even if RansomHub is paid and true to their word.

HOW DOES THIS AFFECT THE REGULATORY LANDSCAPE? CONSIDERATIONS FOR MDMs

The severity of the attack on Change Healthcare has attracted the attention of the legislative branch. In late March Sen. Mark Warner (D-Va) proposed a bill that would provide financial assistance to healthcare providers affected by similar attacks provided they (and their vendors) meet certain cybersecurity standards. Senator Ron Wyden (D-Ore) has publicly stated that he is also in support of minimum cybersecurity standards for the healthcare sector.

SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE RAPIDLY EVOLVING AND CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog April 2024
THE CHANGE HEALTHCARE RANSOMWARE ATTACK: WHAT THIS MEANS FOR MEDICAL DEVICE MANUFACTURERS

The HHS has recently been advocating for a mix of voluntary incentive-based cybersecurity goals for healthcare entities and the authority to "…(create) new enforceable cybersecurity standards". The proposal of cybersecurity regulations has been met with pushback from healthcare groups encapsulated in a letter from Richard Pollack, President and Chief Officer of the American Hospital Association.

It should come as no surprise to the medical device manufacturers following this blog that this is a unique and unpredictable time in healthcare cybersecurity legislation and that changes come quickly. In the time since Section 524B, which gave FDA statutory authority to reject premarket submissions based solely on cybersecurity grounds, has come into effect the entire process of design, development and premarket submission of medical devices has changed dramatically. As last month's blog discusses regulatory expectations will continue to evolve rapidly. Medical device manufacturers should monitor how the Change Healthcare breach develops for two reasons. The first is that ransomware is a clear and present danger and continues to proliferate. Ransomware concerns were a driving factor in the recent regulatory developments in medical device cybersecurity and ransomware is specifically identified in FDA Final Guidance Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (2023). Threat modeling and cybersecurity risk assessments conducted by medical device manufacturers must consider and mitigate ransomware-associated risks. Can the device be used as the entry point for a ransomware attack on a larger network? How is the device protected from a ransomware attack on a larger network? What responsive controls are in place to respond to a device affected by a ransomware attack (logging, backups/resiliency, updates/patching, etc.)? The second reason why medical device manufacturers should monitor the developing Change Healthcare situation is that there may be direct regulatory ramifications for medical device manufacturers. Sen. Warner's proposed minimum cybersecurity standards legislation for healthcare entities identifies that healthcare providers AND their vendors would be mandated to meet the minimum cybersecurity standards. While the bill has not passed it is indicative of a line of thinking that could eventually be codified into law one way or another, as the PATCH Act was never passed by Congress but served as the basis for Section 524B of the FD&C Act. Medical device manufacturers who were familiar with the PATCH Act when it was before Congress were better prepared to adapt to the new cybersecurity regulatory landscape when it became law. The medical device cybersecurity regulatory landscape could be on the precipice of another evolution and familiarization with Federal and Legislative trends and sentiment regarding the sector will allow for medical device manufacturers to anticipate which way the wind is blowing.

END OF APRIL 2024 BLOG

