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 February 2024
THE STATE OF RANSOMWARE ATTACKS IN THE HEALTHCARE SECTOR

REGULATION AND TRENDS

The proliferation of ransomware attacks has been the catalyst for significant developments in critical infrastructure cybersecurity legislation and regulation over the past several years. This blog series has explored critical infrastructure ransomware attacks and trends and the associated governmental and industry responses since October of 2020 with an emphasis on the healthcare industry. A number of factors, including the increasingly interconnected and networked modern world, the professionalization and ease of use of ransomware, and the limitations of slow and reactive federal legislative developments created a critical infrastructure cybersecurity threat landscape that gained national attention with the ransomware attacks on the JBS meatpacking plant and the Colonial Pipeline in 2021. Legislation introduced in 2022 evolved into Section 524B of the Consolidated Appropriations Act of 2023, amending the FD&C Act to require medical device manufacturers to include specific cybersecurity documentation in their premarket submissions and granting the FDA significant statutory authority regarding the approval of those devices on the basis of cybersecurity. In September of 2023 the FDA finalized the guidance *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*, providing updated recommendations for medical device manufacturers regarding a secure product development framework (SPDF) the security of the total product lifecycle (TPLC) of a device, to ensure that cybersecurity considerations were "built-in" instead of "bolted-on". This final guidance specifically identifies ransomware attacks as a primary consideration in many of the recommendations it provides.

The effects of these significant regulatory changes will not be known for some time. The first wave of premarket submissions to the FDA adhering to the new cybersecurity criteria will take time to populate the landscape. In the meantime, the ransomware threat on the healthcare industry presents a muddled picture. A report by Proofpoint/Ponemon indicated that of 653 IT and IT security practitioners in healthcare surveyed, only 48% are worried about ransomware attacks, making it no longer the perceived top threat, and ransomware negotiation firm Coveware reported that ransomware payments (across all industries) dropped to a record low in the final quarter of 2023. It may seem these trends are indicative of positive developments regarding ransomware attacks in the cybersecurity sector, but a closer look reveals troubling developments. Sophos reports despite a reported drop in the rate of ransomware attacks in the healthcare sector in 2023, almost 60% of respondents reported that they suffered ransomware attacks. Although a decline in the amount of ransomware attacks on the healthcare sector is welcome news, the report states that ransom payments and recovery costs for healthcare entities who suffer ransomware attacks rose significantly in 2023 when compared to 2022, and that recovery time is down from 2022.

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 February 2024
THE STATE OF RANSOMWARE ATTACKS IN THE HEALTHCARE SECTOR

THE STAKES ARE HIGHER THAN DOLLARS AND CENTS AND EXTORTION TACTICS ARE EVOLVING

The ransomware attack landscape regarding healthcare must be examined beyond the metrics of cost, data breaches and/or downtime. There is an increasing awareness and quantification of the effect these attacks can have on patient safety, either acutely or as a "ripple effect". While ransomware attack numbers on healthcare may be down overall, what can be classified as a single attack may affect large numbers of patients. CommonSpirit Health, which operates more than 700 care sites and 142 hospitals in the US, was the victim of a ransomware attack was struck by a ransomware attack in 2022 which affected "dozens of hospitals across 13 states, and hundreds of thousands of patients". Capital Health and Ardent Health Services were both victims of ransomware attacks at the end of 2023, with Ardent being forced to divert patients from emergency rooms in three states (mirroring a 2020 ransomware incident in Germany cited in the FDA's *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*).

Ransomware extortion tactics are becoming increasingly abhorrent, presumably in an effort to pressure healthcare entities to pay (or to pay more). In 2023 patients of the Lehigh Valley Health Network had "…medical photos…depicting patients' naked breasts in various angles and positions" leaked onto the internet in response to a refusal to pay the ransom demand. In November of 2023 the Fred Hutchinson Cancer Center was impacted by a security breach in which they were able to obtain patient information of up to an estimated 1 million people. When the cancer center refused to pay the ransomware demands, current and former patients were contacted directly by the hackers and directly extorted. When the cancer center urged patients not to send money to the hackers, the hackers issued threats of "swatting" ("the action or practice of making a prank call to emergency services in an attempt to bring about the dispatch of a large number of armed police officers to a particular address").

A BAN ON RANSOMWARE PAYMENTS?

The FBI has been vocal in their stance that they do not support "paying a ransom to the adversary" in cyber incidents. The idea of a federal ban on ransomware payments has been discussed for years, and has picked up steam with the news that the White House has once again been considering the move following a 2022 decision not to implement one. A U.S.-led alliance of 50 countries endorsed a joint policy statement asserting that "relevant institutions under our national government authority should not pay ransomware

extortion demands". Banning ransomware payments for private entities has been a thorny issue. Proponents suggest that a ban on ransomware payments will disincentivize threat actors and stimulate private-public sector coordination in combating the problem, as well as citing the fact that there is no guarantee that threat actors will actually do what they say they will once they are paid. Sceptics of a ban on ransomware payments state that they are unsure of any disincentivizing of threat attackers, believing that ransomware will always be a pervasive problem and that threat actors will only escalate extortion tactics to circumvent the ban. Under a ban on ransomware payments healthcare entities may not want to engage in private-public sector coordination for fear of penalties for disclosing payment, or double-extortion tactics by threat actors demanding more money once the initial payment is made under the threat of reporting the payment to authorities.

The enhanced statutory authority of the FDA regarding cybersecurity in premarket medical device submissions is a substantial and significant step towards mitigating the threat of ransomware in the healthcare sector. However, as a recent GAO report indicates, the FDA does not have any statutory authority over the cybersecurity of legacy medical devices still in use nor HDO operations, both of which are critical components in addressing cybersecurity threats to the healthcare sector (the FDA does offer voluntary resources to address these components), although the HHS is proposing improvements for the latter component. 2024 will be a pivotal year in healthcare cybersecurity and stakeholders should pay close attention to the threat landscape to anticipate developments in regulation and best practices.

END OF FEBRUARY 2024 BLOG

