American Hospital Association and Health-ISAC Joint Threat Bulletin

Originally published on July 1 at TLP:GREEN
Updated August 1 at TLP:WHITE. This report may be shared without restriction.

Executive Summary

The recent ransomware attacks on OneBlood, Synnovis, and Octapharma by Russian cybercrime ransomware gangs resulted in a massive disruption to patient care. The outcomes of these attacks highlight the need to incorporate mission-critical and life-critical third-party suppliers into enterprise risk management and emergency management plans to maintain resiliency and redundancy in the modern digitally connected healthcare ecosystem.

Now that three critical third-party supply chain attacks have significantly impacted healthcare delivery in the past three months, it should serve as a wake-up call across the industry to address supply chain security and resilience. Organizations should prioritize applying risk management assessment principles to their critical suppliers and partners. Consider supply-chain outages, and availability, determine impact to business operations and care delivery, and identify alternative suppliers or use multiple suppliers to create redundancy. The idea is to eliminate the single points of failure in healthcare supply chains and minimize disruptions to healthcare delivery in the event of ransomware attacks on critical suppliers.

Analysis

Health-ISAC and the American Hospital Association (AHA) are delivering this threat bulletin to inform readers of the potential for cascading impacts from cyberattacks on healthcare suppliers.

Background – Recent Blood Supplier Ransomware Incidents

On July 30, 2024, Florida-based blood supplier, OneBlood, experienced a software outage that is impacting their ability to ship blood products to hospitals in the region. The outage, caused by a ransomware attack, has forced the organization to resort to manual labeling of blood samples. There are so many blood samples in the OneBlood inventory that taking the time to manually process them is causing major shipping delays. The resulting blood shortage is so severe that the Florida Hospital Association (FHA) has recommended that affected hospitals begin to activate critical blood shortage protocols.

On June 3, 2024, the pathology provider Synnovis was attacked by the QiLin ransomware gang resulting in multiple London hospitals being unable to provide healthcare services. The disruption

caused numerous hospitals to reschedule appointments and postpone operations. According to the United Kingdom's National Health Service (NHS), the attack delayed more than 800 planned operations, and 700 outpatient appointments needed to be rescheduled. The attack caused thousands of O-negative and O-positive blood donations to be destroyed because of a lack of connectivity to electronic health records (EHR), making it too difficult to rapidly identify a patient's blood type.

On April 15, 2024, the BlackSuit ransomware gang attacked blood plasma provider Octapharma through a vulnerable VMWare system, resulting in the closure of over 190 plasma donation centers in 35 U.S. states. According to the BlackSuit cybercriminals, the group was able to steal sensitive donor information as well as donor-protected health information (PHI) during the attack. It is speculated that BlackSuit is a rebrand of the ransomware gang Royal. The attack also closed facilities that manufactured plasma, delaying the transfer of life-saving plasma to hospitals across the U.S. and EU. The U.S. Octapharma centers accounted for nearly 75% of the supply of plasma used in Octapharma therapies. Because of this, the shutdown of the U.S.-based supply of plasma likely caused a major disruption to patient care in both the U.S. and the EU.

Impacts of Critical Supply Chain Outages on Patient Care

These ransomware incidents demonstrate how catastrophic failures can occur in healthcare delivery when mission-critical and life-critical suppliers are attacked. For healthcare delivery organizations (HDOs), hospitals and health systems, these attacks had massive impacts to patient care because the entities that were attacked provided mission-critical services to a multitude of healthcare providers, including hospitals, ambulances and medical clinics. The physical supply chain disruptions caused by these attacks highlight the potential for cascading impacts to patient care as a result of disrupting niche, critical healthcare suppliers.

The attacks against Octapharma, Synnovis and OneBlood appear to be unrelated and have been conducted by separate Russian-speaking ransomware groups. However, the unique nature and proximity of these ransomware attacks - targeting aspects of the medical blood supply chain within a relatively short time frame, is concerning. These incidents provide ample reason and impetus for HDOs, hospitals and health systems to review contingency plans for possible disruption to the blood supply chain and other mission and life-critical medical supplies. At the time of this writing, there has been no observed connection between the groups; however, there has been an observed increase in ransomware groups targeting third-party infrastructure that these attacks would be consistent with. As the healthcare sector begins to become more interconnected with third-party medical suppliers and software providers, these incidents are beginning to have larger impacts on patient care.

Hypothetically, if attacks were to occur on different suppliers at the same time, for example, a blood donation organization and a medical gas supplier, the impacts to patient care would likely compound to create a larger impact than if the suppliers were attacked individually at different times. The aggregate effect could be exponentially greater and could result in an unanticipated cascading effect to patient care. While this has not been observed yet, a potential coordinated ransomware attack against multiple healthcare mission-critical and life-critical suppliers could result in significant disruption to patient care globally.

The potential community-felt impacts that could arise from disruptive cyberattacks against

critical healthcare suppliers represent a systemic risk in the modern healthcare ecosystem. As critical infrastructure becomes more interconnected and interdependent and more efficient, third-party suppliers also represent more critical functions because one or more hospitals may directly rely on the same supplier for critical materials, such as plasma or medical gas. If this supplier were to become unavailable for a time due to a ransomware attack, the collateral damage and cascading effects could be wide-reaching and disrupt numerous patient operations as seen in the attacks against Octapharma, Synnovis and OneBlood.

Another current example of healthcare systemic risk and disruption to healthcare delivery can be found in the ransomware attack against UnitedHealth Group's Change Healthcare. The attack against Change was the most significant and consequential cyberattack against U.S. healthcare in history. When critical services abruptly went dark as a result of the ALPHV/BlackCat ransomware attack against Change Healthcare, every hospital in the U.S. was impacted directly or indirectly for months, especially in regard to revenue cycle disruptions.

Recommendations

Health-ISAC and the AHA recommend that special consideration be given to critical supply chain entities. These elements can be identified through three criteria:

- being essential to the healthcare mission,
- having catastrophic consequences if they fail, and
- the lack of suitable alternatives.

For many HDOs, blood suppliers fit into this category. Additionally, key services and business relationships could fall into this category. One example of how software represents as much systemic risk as niche products was experienced in the aftermath of the attack on Change Healthcare. The services Change Healthcare provided the sector represented a unique point of failure —and due to the lack of alternatives to their payment processing product, the outage caused severe operational and financial impacts to pharmacies and hospitals across the US.

The identification of these single point of failures, especially the healthcare sector-specific ones are essential for an effective supply chain risk management plan amid patient-impact driven ransomware attacks. To learn more about how to structure a healthcare-specific supply chain risk management plan, please view the Health Industry Cybersecurity Supply Chain Risk Management Guide here: https://healthsectorcouncil.org/hic-scrim-v2/

Mitigations

The AHA and Health-ISAC encourage organizations to consider supply-chain outages and availability as part of their overall risk management assessment process. HDOs, hospitals and health systems are recommended to consider alternative suppliers and/or incorporate multiple suppliers of these critical supplies into their supply-chain strategy to create redundancy in the event that one mission-critical supplier becomes inoperable as a result of a cyberattack. The risk management business decisions should eliminate (or reduce) the single points of failure in healthcare supply chains and minimize patient impact in the event of ransomware attacks on crucial medical suppliers.

The following specific recommendations are provided to assist healthcare organizations prepare for the impact of mission and life-critical third parties and supply chains:

● Develop and implement a multi-disciplinary Third-Party Risk Management (TPRM) governance committee and program in which each represented function identifies, on an ongoing basis those third parties and supply chain which are life-critical, mission-critical and business-critical for each function. Assess strategic and technical risk for each.

● Develop continuity procedures for each to sustain a loss of those critical services and supplies for 30 days or longer. developed with the objective to sustain business operations and to continue safe and quality care.

● Thoroughly document, test and update continuity plans and downtime procedures for each, at least annually.

● Risk prioritize and stratify identified entities on an enterprise level and include other criteria such as:

- Storage or access to sensitive data
- Network access – privileged access
- Foreign operations and subcontractor risk
- Technical cybersecurity posture currently and ongoing monitoring
- Consider aggregate risk from the third parties for multiple services provided
- Develop customized risk-based cybersecurity requirements for each
- Develop customized risk-based cyber insurance requirements for each
- Breach notification and responsibility requirements
- ll risk-based requirements should be contractual and included in business associate agreements and third-party contracts

Sources

https://www.hipaajournal.com/octapharma-ransomware-attack/

https://therecord.media/plasma-donation-company-cyberattack-blacksuit
https://www.nytimes.com/2024/06/13/world/europe/nhs-london-hospital-cyberattack.html

https://www.independent.co.uk/news/health/nhs-hospital-cyberattack-london-blood-tests-b2556383.html

https://www.techtarget.com/searchdatacenter/definition/Single-point-of-failure-SPOF

https://www.aha.org/advancing-health-podcast/2024-03-27-cyberthreats-and-assessing-third-party-risk-providence-part-one

https://www.aha.org/advancing-health-podcast/2024-03-29-part-two-cyberthreats-and-assessing-third-party-risk-providence

https://trustees.aha.org/cybersecurity-awareness-board-responsibility

https://apnews.com/article/blood-center-cyberattack-ransomware-florida-d82905237830b55fbbad30acee116893

https://www.oneblood.org/pages/ransomware-details.html