withum

CASE STUDY

CYBER AND INFORMATION SECURITY SERVICES

HOSPITAL AND HEALTHCARE NETWORK AVOIDS DEBILITATING CYBERATTACK AT THE HEIGHT OF A GLOBAL PANDEMIC.

Learn how Withum's Cyber and Information Security Services Team delivered an end-to-end cyber threat solution saving millions of dollars and potentially hundreds of lives after stepping into a vCISO role.

EXECUTIVE SUMMARY

During the height of the global pandemic brought on by the aggressive spread of COVID-19, Withum's Cyber and Information Security Services Team was able to identify, protect and defend a large hospital and healthcare system from an international cyberattack. Initially, brought on as a vCISO (Virtual Chief Information Security Officer), the Team quickly discovered vulnerabilities within the organization's infrastructure, which resulted in a full-scope advisory project to mitigate any future risk and design a robust cyber and information security framework. As the average cost of a typical cyber breach hovers near $8.9M, the potential loss for the healthcare system during this time would have been astronomical, both financially and reputationally, through potential class-action lawsuits for loss of life.

THE CLIENT

A leading NJ-based hospital and healthcare network needed a vCISO to fill a position on their information technology team in response to a current employee taking a maternity leave of absence. During this time, the organization was in the beginning stages of the due diligence process as part of a potential merger with a similarly sized healthcare system. Recognizing the importance of this role during a pivotal time in the organization's growth strategy, the hospital agreed to engage Withum for advisory vCISO services to fill the temporary staffing gap.

CASE BRIEF

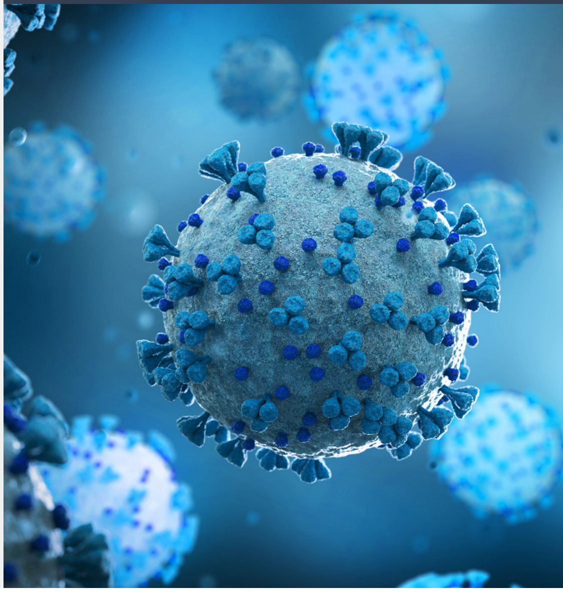
CLIENT: A U.S. hospital and healthcare network based in the Northeast

STRENGTH: Leader in clinical excellence and patient safety

CHALLENGE: Maintain information security during a global pandemic

OPPORTUNITY: Gain an external perspective on security infrastructure via a third party

OUTCOME: Mitigated international cyber intrusion and created robust cyber and information security framework



The organization's leadership was familiar with Withum from the current services the firm was already providing. Therefore, the healthcare system's leadership was confident that Withum's Cyber and Information Security Team would provide the level of service and expertise required.

THE CHALLENGE

It's typical for internal IT Teams to be hesitant to integrate an independent third party into a business's IT operations and processes. In a Chief Information Security Officer (CISO) role, on-premises or virtual, the individual is responsible for continuously assessing and addressing the architecture, goals and strategy of the organization. This role includes evaluating the current environment to ensure proper processes, procedures and controls are in place to protect the integrity of the organization as well as the PII (Personally identifiable information) it maintains. Challenges this hospital and healthcare network faced before engaging Withum included:

- There was no dedicated CISO in place. The IT Team had someone acting in this role; however, this individual was also responsible for other duties within the organization. This limited the organization's ability to be fully immersed in each aspect of its IT infrastructure.
- The Compliance and IT Departments lacked a sound understanding of what each team does. These two departments should provide a checks-and-balances system to ensure that things are done accurately. However, Compliance lacked the full knowledge of what IT could deliver, and IT provided what it understood Compliance to be requesting.
- The hospital lacked a virtual incident response team trained in cyber forensics and high-tech investigations support.
- The C-Suite and Board did not have an independent and clear understanding of their current cybersecurity posture, as well as the current cyber threats facing their organization.

Withum's Cyber and Information Security Services Team was engaged to take on the vCISO role to act at the level that the organization required while also serving as the liaison between the IT and Compliance Departments. Stepping into this role just before the coronavirus global pandemic, Withum's Team was able to assess the security infrastructure, identify control gaps and shift the perspective of what is truly necessary to protect an organization of this size that stores so much patient PII (Personally Identifiable Information).

During the engagement, Withum's Team completed a series of standard tests, which resulted in the detection of a phishing attack launched during the height of the pandemic, when hospital resources were limited, tension was high, and patient care was of the highest priority. Based on the results of the penetration testing, threat emulation and cyber forensics, an incident response was imperative to protect the livelihood of the hospital system and the patients it served.

New challenges identified once Withum's Cyber and Information Security Services Team was engaged included:

- Trace and isolate the incident identified as a threat from an international foreign actor.
- Compartmentalize the onset of the intrusion during COVID-19.
- Enhance the security of the healthcare system.
- Prevent massive data loss, reputational demise and loss of life.
- Create a robust, secure infrastructure to automatically detect, identify, respond and recover from future threats or intrusions.

THE APPROACH AND SOLUTION

Withum addressed each red flag within the organization's IT and IT security framework due to the extensive background and experience of the Cyber and Information Security Services Team. To best tackle the needs of the healthcare system, Withum's Team divided the project into four phases:

PHASE I — IDENTIFICATION OF CYBER THREAT

At the onset of the discovery of the intrusion, the Team performed a forensic investigation. Withum's cyber forensic specialists analyzed the phishing email and additional forensic artifacts collected. Based on forensic evidence analyzed, the origin of the phishing email and suspect activity was traced back to a well-known sophisticated nation-state cyber threat actor in the Middle East. The email entered the hospital's system through a trusted source, a third-party vendor the organization uses to fulfill nursing staffing needs. This identified vulnerabilities within not only with the healthcare system but with the staffing company as well.

PHASE II — RESPONSE TO CYBER THREAT

After identifying the point of intrusion and the extent of the impact within the organization, Withum's Cyber and Information Security Services Team isolated the incident and compartmentalized the onset of intrusion. Withum's Team identified the hospital's legal counsel and law enforcement agencies as appropriate to ensure proper reporting, responses and actions took place.

PHASE III — MITIGATION OF CYBER THREAT

To properly understand the extent of vulnerability within the healthcare network, Withum performed an in-depth penetration test. The penetration test, a systemized hacking by professionals in a secure manner, revealed severe areas of weakness within the organization's infrastructure. Withum's Team was able to take complete control of the IT environment, undetected, within a few hours. This report of system vulnerability created a baseline for creating a solution that promised a secure IT infrastructure.

PHASE IV — SOLUTION TO CYBER THREAT

Withum deployed two AIR$_4$Droid^{TM} computer devices to deliver real-time protection to the healthcare system in the future. Withum's AIR$_4$Droid^{TM} devices provide intelligent identification, scanning, probing and mapping of an organization's network(s) devices and vulnerabilities.

The organization now receives real-time active and passive cybersecurity monitoring, alerts, auditing, incident response, cyber forensics and reporting to a secure, personalized account. Withum's Cyber and Information Security Team provides full support and monitoring of the AIR$_4$Droid™ devices through its 24/7/365 Security Operations Center.

THE RESULTS, ROI

Withum's Cyber and Information Security Services Team delivered an end-to-end solution for the hospital and healthcare network.

Withum's Cyber and Information Security Services Team was able to:

- Deliver on acting as a trusted vCISO in an advisory role.
- Detect, identify and mitigate a foreign network intrusion.
- Save upwards of $8.9M in damages, reputational risk and potential loss of patient life.
- Develop strong relationships and rapport with the healthcare system's board and general counsel as well as local law enforcement.
- Identify other vulnerable areas within the organization's IoT (Internet of Things) and define plans to secure their interactions with such systems and devices to protect PII and remain HIPPA compliant.
- Demonstrate that a member of the organization's IT Team played a significant role in the project, which earned him a promotion.

Withum's Cyber and Information Security Services Team also identified areas of vulnerability and improvement for the third-party nursing staffing company, which resulted in strengthened IT processes and procedures for sharing information between companies.

Withum's cybersecurity specialists were able to create more value for the hospital and healthcare network as it moved forward in the merger process with a neighboring health system. Its IT infrastructure now creates greater confidence in the security of future patients' PII.

During one of the most stressful and demanding times on hospital systems in history, Withum's Cyber and Information Security Services Team was able to act quickly and effectively to eliminate a damaging cyber threat. Through a collaborative approach with the organization in-house IT Team, there was minimal disruption to operations giving the hospital the required time and attention to focus on patient care and saving lives.