ACCORIAN

CASE STUDY

A leading **NJ large medical practice company** called Accorain's team of experts to help them after a Ransomware attack.

Situation

Our client's systems were ransomware attacked through one of their open ports and applications. This then replicated internally to their desktops and the AWS environment. The client was able to shut down the machines before everything had been replicated. The applications were hosted on AWS infrastructure including their EMR. Due to COVID, a large number of their staff were working from remote and so they had opened up more applications and ports to external users than usual.

Solution/Approach

Accorian's Incident Response team was called to help after the ransomware attack:

- Recovery
- Negotiation with threat actor
- Forensics
- Compliance

Recovery:

We worked with the MSP to understand all threats & vulnerabilities in their current infrastructure in order to securely bring up the environment. We approached Recovery in 3 distinct steps:

- Malware analysis - Understand the type of malware, how it replicated and indicators of compromise (IoC)
- Understood the current vulnerabilities in the environment and drafted a hardening strategy
- Started bringing back a secure environment with the MSP. This involved patching, segmentation, vulnerability scanning & penetration testing

Negotiation with Threat Actor

Understood the threat actor's demands, negotiated, and got the bitcoin wallet ready. Ultimately, we helped our client recover from a back-up and our client didn't have to pay, but we were ready if needed.

Forensics

As exfiltration of PHI data was of utmost importance & concern, we worked with the client and their MSP to analyze data flows & all the systems with PHI data. In conjunction, we started to understand what systems were accessed and the possible root cause along with system zero. Additionally, we ran daily status meetings with the client, MSP, and the law firm.

Compliance

Worked with the law firm to provide the necessary documentation for all statutory reporting to HHS.

In total, the ransomware attack caused our client to be down for 3 days and a spend of over $250,000 even without a significant breach or data exfiltration. If data had been taken out of the environment the cost would have been significantly higher.

Running a periodic vulnerability assessment in the form of an external penetration test, segmentation testing, patching and phishing exercise would have likely avoided the loss of revenue and cost. But, most importantly – an inability to service their patients during the downtime.