From Reactive to Proactive Security: Ransomware Attack Prompts a Culture Shift at a Healthcare Nonprofit

Case Study

- **Industry:** Nonprofit
- **Country:** United States
- **Size:** Mid-size

Challenges

- Business disruption following a ransomware attack.
- Company culture prioritized convenience over security.
- Limited organizational support to learn and follow security best practices.

Solutions

- The Arete Digital Forensics and Incident Response (DFIR) and Cyber Strategy and Defense (CSD) teams helped mitigate the attack, conducting a forensic investigation to uncover root cause and assisting with system restoration.
- The Arete CSD team conducted internal, external, and vulnerability assessments to uncover vulnerabilities and security gaps.
- Ongoing CIO-as-a-Service guidance to improve cyber resiliency and cultivate a more security-minded culture.

Benefits

- Restored business operations within days.
- Enhanced security awareness and training across the company.
- Developing a road map to harden infrastructure and strengthen cyber posture.

When a nonprofit healthcare organization suffered a ransomware attack, the incident did more than bring business to a temporary standstill — systems were down for nearly five days — it also shined a spotlight on the dangers of a convenience-first culture.

For more than 70 years, this nonprofit has been supporting people with intellectual and developmental disabilities through day and community habilitation and resident, respite, and family support services. Unfortunately, ransomware groups tend to target hospitals and healthcare organizations — generally, because they are willing to pay ransoms. In this case, however, the nonprofit engaged Arete, whose experience managing thousands of ransomware cases gave it the confidence to not pay the ransom.

> “No business can afford to be down for long, but we trusted Arete to direct us what to do when — and they saved the day.”

“No business can afford to be down for long, but we trusted Arete to direct us what to do when — and they saved the day,” said the nonprofit’s VP of IT. “Not only did we not pay the ransom, but we also didn’t even consider negotiating. Instead, with help from the Arete DFIR and Restoration teams, we knew we could restore from backups and, as necessary, rebuild systems.

“While there were certain systems we wanted to turn back on sooner, because we’d experienced a breach, Arete advised waiting a beat to allow the forensics team to gather evidence and complete their investigation. In fact, they guided us every step of the way in terms of what to turn on, what not to turn on, what to allow employees to access, how to segment our network, etc. Without their counsel, we likely would have relaunched several systems too early; in the long run, the small delay saved us time and effort.”

Closing gaps and improving compliance

“If systems had gone down in the past, our previous boss’s mantra was, ‘Use pen and paper,’” said the VP of IT. “Needless to say, our culture was in need of a change.”

With the ransomware threat contained and mitigation underway, the nonprofit turned to Arete to conduct three assessments (internal, external, and vulnerability), find any other gaps or vulnerabilities, finetune systems and policies, and raise overall security awareness.

“We’ve always been a HIPAA-compliant healthcare nonprofit — or at least, that’s what we thought,” said the nonprofit’s CEO. “To the best of our abilities, we work to maintain compliance, but after the ransomware incident, we realized we could do better. “The Arete team has been incredible to work with. Their line of questioning can be rigorous, but it’s

always purposeful. They offer logical reasons for everything they ask, which has put our staff at ease during a stressful time. They've helped us understand the many nuances of compliance and where we can make improvements."

The VP of IT shared this sentiment, "I have the utmost respect for the Arete CSD team. We meet weekly, and they've been our guiding force — helpful, resourceful, easy to work with — as we put together a road map to address issues identified during the assessments. Their extensive incident response experience and expertise give us all the confidence to act on their recommendations and direction. And that includes our entire employee base."

"The Arete team has been incredible to work with. Their line of questioning can be rigorous, but it's always purposeful. They offer logical reasons for everything they ask, which has put our staff at ease during a stressful time. They've helped us understand the many nuances of compliance and where we can make improvements."

Making security a priority

Historically, the nonprofit's culture hasn't been to invest in security — it's been a more reactive than proactive environment. "Our employees are focused on people, not security. If a task doesn't deal directly with a human aspect of the business, it's not considered as important," said the VP of IT. "What's more, many are resistant to change and have an antiquated view of IT. They see my team as the folks under desks, plugging in cords or unjamming printers. So, it's not always been easy to get them to see that security is part of the business."

Since the ransomware attack, however, the VP of IT has started to see a shift. "The attack was a wake-up call. And thanks to continuing education from the Arete CSD team, people are starting to see that security, while not a human service, can still serve the client; that outdated and unsupported legacy systems carry risk; that two-factor authentication is worth the small inconvenience; that resetting passwords on a regular basis should be a habit."

In short, Arete helped bring more than the business back online following the incident. The CSD team has helped the CEO and VP of IT bring a sense of security accountability to more departments across the entire organization.