Deloitte.

Together makes progress

A life sciences company turns a ransomware attack into a road map for IT modernization

The challenge

A life sciences company had been hit with a ransomware attack. In a panic, the company's IT management erased core network components.

Essential processes ground to a halt just as the company was preparing a large shipment of medical products. With leadership deciding not to pay the ransom, the focus shifted to getting the business back up and running.

A business-first approach

Deloitte's first step was a meeting with the CEO to understand the critical business functions that had to continue, while the technology remained unavailable. Manufacturing, shipping, and financials were the most urgent matters, the CEO said.

With that guidance, we consulted the appropriate business leaders to align business continuity strategies, tapping Deloitte's global network so that leaders outside of the United States had a local resource to work with. Meanwhile, Deloitte's assurance professionals set up quality checks to help management determine the materiality of the incident and test the integrity of the financial data for the company's external auditor.

Revamping security

At the technology level, we identified gaps in the company's security hygiene—that is, the measures in place to minimize risks and prevent breaches—and determined what needed to happen to achieve containment as quickly as possible.

Among other things, the threat actor had taken control of the company's on-premises endpoint detection

and response (EDR) system. So the Deloitte team replaced the old EDR with CrowdStrike's Falcon platform, which proactively hunts and isolates sophisticated threats. We also engaged Deloitte's Cyber Threat Intelligence team to map the client's public IP space and identify any connections to known threat actor activity.

With the investigation and business recovery efforts underway, the Deloitte team stood up the client's systems one at a time in an isolated recovery environment. That way, we could determine what the level of security was on each of those systems and whether ransomware had infiltrated the backups. Only after confirming a clean and functional recovery did we put the system back into production.

Results

Amid three months of active incident response, recovery, and defense hardening, the company completed their year-end close on time. They were also able to let their board of directors know the company had established a cohesive cybersecurity program, including round-the-clock endpoint monitoring using CrowdStrike and interim cyber leader via Deloitte.

By treating the ransomware attack as a business issue, not just a technology one, the company was able to continue with business, while Deloitte carried out a focused recovery in parallel with a digital forensics and incident response. This journey provided the CEO and CFO critical insight into the state of their operations. This led to a decision to modernize the company's entire IT infrastructure, from assembly line to shipping and back-end systems. Rather than simply recover, these leaders have opted to create a hardened, agile, and secure space in which the company can become even more innovative and achieve their goals for rapid growth.

About Deloitte's Cyber Operate

Deloitte's Cyber Operate-managed security services bring cloud-based threat hunting, detection, response, and remediation capabilities to your cybersecurity environment. Specialists pursue threats before they become attacks and respond to help reduce business impact in the event an attack occurs. Example services include:

- Cyber threat intelligence
- Incident readiness and response
- Zero-trust identity prevention, detection, and response
- Enterprise prevention, detection, and response
- Attack surface management and vulnerability management
- Multicloud security

Contact us today to see how Deloitte ***Operate*** can deliver for you.

Contact us:

Paul J. Kim
Managing Director
Deloitte & Touche LLP
pjkim@deloitte.com