Case Study

Law Firm Client Gets Support for Mission-Critical Malware Remediation

The client

The client is a successful law firm that has provided legal services for individuals, families, and businesses in dozens of practice areas for more than 50 years. As a top-ranked U.S. law firm and provider of financial services, the client employs more than 200 employees and exceeds annual revenues of $50 million.

The challenge: Quickly regaining operability and control over data without paying ransom

When a phishing attack introduced ransomware into the client's network, the result was a total infection of the client's infrastructure — approximately 700 devices impacted. Nearly every digital asset was encrypted, freezing operations and triggering immediate remediation efforts.

Insight had previously supported the client in an unrelated service area; when the client's prior contracted service providers attempted containment and remediation to no effect, the firm's managing partners reached out to Insight leadership for emergency cybersecurity support.

Industry:

Legal services

CDCT provided:

- Emergency threat identification, containment, and remediation
- Negotiation support and data restoration
- Reactive and preventive network and security solutions
- Coordinated services with Insight's Connected Workforce solution area

CDCT services:

- Incident Response services
- Security Services
- Consulting Services
- Network Professional Services

The solution: An all-hands-on-deck approach to mitigation, remediation, and prevention

As soon as the client contacted Insight, our Incident Response team took action, working through the night to develop foundational security and define a path forward. Within the first 24 hours, 16 team members from Insight Cloud + Data Center Transformation (CDCT) Consulting Services, Security Services, and Network Professional Services, and Insight Connected Workforce across the country had accomplished significant remediation, including:

- Assessing data backups for potential restoration
- Addressing issues with the client's Office 365® tenant
- Restoring functionality to desktops and servers
- Enabling multifactor authentication, firewalls, and other security protocols

Within 32 hours, the client had some business functionality restored, with full functionality restored to their environment over the course of a week. Insight teams were able to successfully restore backup data, eliminating the need for the client to purchase the bad actor's decryption tool. Expert negotiation efforts also saved the client from paying the requested $1.8 million ransom.

The benefits: Fast, effective emergency remediation and the foundation for a long-term partnership

Our work with the client not only helped them to avoid the potentially devastating financial and professional results of an unmitigated data breach but also quickly got their operations back on track and with stronger preventive security measures in place. Once regular operations resumed, we began actively working with the client on further remediation efforts to help provide controls for protecting their environment in the event of another potential ransomware event.

The collaboration, professionalism, and ability to execute delivered by the Insight team impressed on the client the benefits of having a capable and committed technology partner. As a result of Insight's emergency response work, the client made an additional security service investment and has since determined to consolidate IT partners and route as much IT business as possible through Insight to continue taking advantage of the support and expertise we offer.

Benefits:

Fast and effective data and device restoration

Prevention of financial losses upwards of $1.8 million

Cross-team and client collaboration

Stronger security posture against future attacks

Continued support with an ongoing partner relationship

©2020, Insight Direct USA, Inc. All rights reserved. All other trademarks are the property of their respective owners.
CS-SA-1.0.05.20