



Client Story

Victory Over Ransomware: Law Firm Keeps \$1.8 Million With Swift Response

Despite a data breach that compromised 700 devices, this organization took firm control of its data within 24 hours, avoiding a hefty ransom and establishing stronger security measures that will continue to pay dividends.

An unexpected event

Law firms are no strangers to highly sensitive and confidential data — from trust accounts that hold significant sums of money to information on clients and high-stakes court cases.

When a phishing attack introduced ransomware into this law firm's network, it resulted in total infection of the infrastructure, impacting approximately 700 devices. Nearly every digital asset was encrypted. The firm was forced to freeze operations and trigger immediate remediation efforts.

A previously contracted service provider attempted containment and remediation with no success, so the firm's managing partners reached out to Insight; we had previously supported the firm in an unrelated service area, and we were ready to take action.

With 50+ years of experience, this top-ranked U.S. law firm employs more than 200 employees, exceeds annual revenues of \$50 million, and serves individuals, families and businesses in dozens of practice areas.

Industry:

Legal services

The challenge:

Quickly regain operability and control over data after a phishing attack without paying a ransom.

The solution:

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

Insight provided:

- Emergency incident response — threat identification, containment and remediation
- Negotiation support and data restoration
- Reactive and preventive network and security solutions

Insight services:

- Security Services
- Consulting Services
- Professional Services

Course correcting

As soon as the firm contacted Insight, our Incident Response team took action and began working through the night to develop foundational security and define a path forward. Within the first 24 hours, 16 Insight team members from across the country had accomplished significant remediation, including:

- Careful assessment of 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

In less than two days, the firm had some business functionality restored, and within one week, full functionality was restored to its environment. Thanks to expert negotiation efforts and successfully restored backup data, the firm no longer had to purchase the bad actor's decryption tool — or pay the substantial \$1.8 million ransom.

The firm no longer had to purchase the bad actor's decryption tool — or pay the substantial \$1.8 million ransom.

Stronger today — and tomorrow

Our work with the law firm not only helped it avoid the potentially devastating financial and professional results of an unmitigated data breach — it also quickly got the firm's operations back on track and with stronger preventative security measures in place. Once regular operations resumed, we began actively working with the firm on further remediation efforts. Together, we've established controls for protecting the firm's environment in the event of another potential ransomware incident.

After a ransomware attack, successful remediation hinges on visibility, collaboration and the ability to execute quickly and strategically.

As a result of Insight's emergency response work, the firm made an additional security service investment and has since decided to consolidate IT partners and route as much IT business as possible through Insight to continue taking advantage of our support and strategic expertise.

Even as bad actors continue to refine their attack methods, the firm is well poised to face cyberthreats head on.

Benefits & outcomes:

\$1.8 million

kept for the business —
not lost to cybercrime

Fast and effective
data and device
restoration for
700 affected devices



**Stronger security
posture against
future attacks**

Cross-team
and client
collaboration



**Continued
support and
optimization
with strategic
security expertise**

©2022, Insight Direct USA, Inc. All rights reserved. All other trademarks are the property of their respective owners.
CS-SA-1.0.11.22

solutions.insight.com | insight.com