



CASE STUDY

Upholding Trust with Professional Services Firm in the Face of Ransomware Attack

In the professional services industry, trust is crucial. A recent ransomware attack targeted a leading firm's critical data. Resilience swiftly intervened, reducing the ransom demand by 67% and securing a rapid resolution within a week.

INDUSTRY

Professional Services

FEATURES USED

The Risk Operations Center

CONTEXT

Trust is paramount in the professional services industry, spanning client relationships, data security, and operational systems. However, this trust is vulnerable, as demonstrated by a significant ransomware attack on a leading firm, jeopardizing its financial stability, client trust, and reputation.

CHALLENGE

The firm faced a critical ransomware attack targeting essential data stored on shared network drives, posing an immediate threat to its operations, financial health, and brand reputation. With trust hanging in the balance, rapid and effective response was imperative.

SOLUTION

Resilience's Risk Operations Center (ROC) blends human expertise and automation for proactive threat response. Within an hour of the ransomware attack, the ROC activated Resilience's 24/7 Claims and Incident Management team, engaged Incident Response partners, and identified the ransomware variant to guide targeted strategies. Swift identification of the ransomware variant enabled targeted response and negotiation strategies, while collaboration with key stakeholders ensured transparent communication and informed decision-making. By monitoring threats across Resilience's portfolio and intelligence sources, the ROC delivers proactive recommendations, equipping security teams with actionable insights at scale.

RESULTS

- Strategic negotiation efforts, backed by expert guidance, reduced the ransom demand by approximately 67%, significantly alleviating potential financial losses.
- Resilience facilitated a speedy resolution within a week, demonstrating efficiency in managing large claims and coordinating with other insurers.
- The successful outcome highlighted the value of a collaborative, human-centric approach to crisis management through the Risk Operations Center.
- Trust in the professional services firm was preserved through effective and strategic action.



Discover the strategy that drove our success

CONTACT US
ReachUs@cyberresilience.com

Please refer to your insurance quote for specific details governing your coverage. Insurance coverage presented herein is for informational purposes only. The terms and conditions of your specific insurance quote will govern. Certain conditions and limitations may apply. The purchase of insurance coverage is in no way tied to the purchase of security services. Nothing in these materials should be construed as an express or implied endorsement or recommendation of Resilience by any government or government agency. In the United States, insurance products are distributed by Ocrea Risk Services, LLC (NPN 19169260) d/b/a Resilience Cyber Insurance Solutions. Resilience products are underwritten by Homeland Insurance Company of New York or Homeland Insurance Company of Delaware, each subsidiaries of Intact Insurance Group USA LLC with their principal place of business at 605 Highway 169 N, Plymouth, Minnesota 55441. Arceo Labs, Inc. d/b/a Resilience provides security services through its expert security team.