Ransomware risk mitigation

QOMPLX builds security solutions for global professional services firm

1.
A global professional services firm feared a ransomware attack; its incident response capabilities were lacking.

2.
QOMPLX designed and implemented a digital forensics and incident response (DFIR) program to find and fix gaps in the client's security program and support its aggressive, acquisition-based, growth strategy.

Challenge

In 2020, ransomware demands grew to the high seven-figure ranges. At the end of 2020 and into 2021, some ransom demands reached into the tens of millions of dollars.

These are unprecedented times in cybersecurity. Global speciality insurer Hiscox reported in its 2021 Cyber Readiness Report: 43% of the companies suffered a cyberattack in 2020 — up 38% in the 12 months before — and one in six of those attacks was a ransom attack.

When one of the world's top professional services firms saw the rising risks from ransomware and looked at their incident response capabilities, they knew they couldn't afford a similar fate. The need was particularly acute because the security postures of the firm's acquisition targets varied widely, some with elevated risks. QOMPLX was the solution.

INDUSTRY:	Professional Services
HEADQUARTERS:	Global
EMPLOYEES:	5,000+
OFFICES:	>100
SELECT SERVICES:	■ Banking & Finance ■ Corporate Services ■ Energy
ANNUAL REVENUE:	USD Billions

Solution

QOMPLX designed and implemented a four-part digital forensics and incident response (DFIR) program to find and fix gaps in the firm's security stack and support the firm's aggressive, acquisition-based, growth strategy.

- Scan targets, assess internal and external risks, instrument and enumerate gaps in the client's environment.
- Profile and prioritize critical risks, frame decisions for management, and implement a process for finding and fixing security issues.
- Use Privilege Assurance to identify over-permissioned accounts, minimize access and trusts.
- Use Identity Assurance to protect authentication and detect likely attacks on the firm's Domain Controllers and member servers, on the assets of acquired companies.

Impact

Since first launching the comprehensive DFIR program for its client, QOMPLX has monitored the security posture of its client and the client's acquisitions 24×7.

With QOMPLX's Digital Forensics and Incident Response service, the client can confidently avoid the worst risks from a ransomware attack, make risk-based decisions, and aggressively grow.

> QOMPLX's Digital Forensics and Incident Response (DFIR) service rapidly cut the client's ransomware-related risk exposure and freed the firm to focus on growth

Why QOMPLX®

QOMPLX harnesses data to provide unified visibility into cyber risks and trust in identity. QOMPLX solutions reduce cyber risk and attack surfaces by mapping exposures and performing real-time detection of attacks. This approach increases network observability by closing the largest remaining gaps in cybersecurity: identity verification, cross-tool data fusion, and data interoperability. QOMPLX defends some of the world's most renowned brands by re-establishing trust for client organizations, assuring authentication, and enabling confident security decisions.

For more information, visit **qomplx.com** and follow us **@QOMPLX**.