Claim Case Study: Ransomware Attack

An engineering firm's mission-critical systems were restored within 3 days of a ransomware attack and normal business operations resumed within 10 days.

At-Bay provided a swift resolution to its client by delivering remediation and recovery after a ransomware attack.

The Target

Industry	Engineering
Revenue	$75M - $125M
Size	800 - 1,000 employees
Location	Offices across the U.S. and Canada
Attack Type	Open RDP port entry

The Attack

One Sunday morning, an engineering firm discovered it had been targeted by an attack, which exploited an open Remote Desktop Protocol (RDP) port to access the firm's internal systems and hold its project files, contracts, and sensitive client information for ransom. The firm immediately shut down all systems to prevent further damage.

Example of an At-Bay Claim Response Timeline[1]

Team Contact & Assembly	
Sun | 8:00 - 9:45 a.m.	The firm's insurance broker contacted At-Bay and a breach coach on behalf of the engineering firm. The gravity of the situation was readily apparent, and At-Bay immediately began assembling a response team.
Sun | 9:00 - 10:30 a.m.	Even though early on a Sunday morning, the team quickly came together — the breach coach, forensics firm, cryptocurrency payment facilitator, and ransom negotiator — and began assessing the situation right away: • The team initiated a scoping call with select vendors, including the response firm most experienced with the ransomware variant and the type of data at risk, to get a handle on what they were up against. • A Statement of Work (SOW) was created, outlining the recommended work that needed to be done.
Sun | 11:30 a.m.	The SOW was approved, forensic work began, and intelligence-gathering on the attacker was initiated.

Negotiation & Resolution	
Sun | 1:00 p.m.	At-Bay approved contact with the attacker — identified as Lockbit ransomware group — and the response firm began gathering intelligence from the group to validate against data and information being collected in the firm's forensic investigation.
Mon | 3:00 p.m.	After negotiating a **50% reduction**, the ransom was paid.
Tue | 9:00 a.m.	The response firm received a decryption tool from the attacker and, after determining that the decryptor contained no malicious capabilities, began bringing the firm's systems back online. • At-Bay's Security team continued to run external scans of the business throughout the investigation. They found an open port and contacted the incident adjuster. The adjuster followed up with the business, who reviewed and advised that the port was connected to a third-party service provider. The business reached out to the provider to close the port, reducing their risk of another attack.
Wed | 10:00 a.m.	The engineering firm's most critical systems were up and running, and the company resumed partial operations.

The Result

10 days

Time from discovery of the attack until the firm was back to business as usual.

50% reduction

The amount by which the At-Bay team was able to negotiate down the ransom payment.

Throughout the incident, At-Bay kept in close and frequent contact with the client. The speed at which recovery took place enabled the firm to avoid a much larger business interruption loss.

At-Bay Insurance: Confidence to Thrive in the Digital World

At-Bay is the world's first InsurSec provider designed from the ground up to help businesses tackle cyber risk head on. By combining industry-leading insurance with world-class cyber security technology, At-Bay offers end-to-end prevention and protection for the digital age. At-Bay helps its 30,000+ customers close their security technology and skills gap — all through their cyber insurance policy — making them up to 5X less likely than the industry average to be hit with a ransomware attack.[2]

Learn how At-Bay can help protect your business | at-bay.com/cyber

[1] Note: Response timelines differ. In all scenarios, At-Bay is committed to providing prompt, efficient, and equitable claims handling. This content is provided for information purposes only and is not intended to define any Policy commitment. No warranty is given or liability accepted regarding this information.

[2] Frequency based on Primary and Excess Cyber and Tech Errors & Omissions losses reported and exposure earned through 9/30/2022, evaluated as of 10/1/2022, and 2020-2021 industry analysis.

This communication contains product summaries intended for use solely by properly licensed insurance professionals. Any cost, premium, or coverage stated are not guaranteed. Actual cost, premium, and coverage are subject to the unique considerations of each individual risk. ©10/2023 At-Bay. All Rights Reserved.