

# Incident Response in Action

## Introduction

A mid-sized tech company faced a major ransomware attack that crippled their operations overnight. With critical data encrypted and customer information at risk, the company urgently needed to recover its systems and prevent future attacks. This case study outlines how we responded quickly with a thorough Incident Response plan to restore the business, contain the attack, and improve their overall cybersecurity.

## Background

The client, a growing technology company specializing in software development, had experienced rapid expansion over the past two years. Their services cater to a diverse range of industries, including healthcare, manufacturing, and retail. However, this growth also increased their exposure to cyber threats, particularly as their IT infrastructure became more complex and their workforce expanded.

Despite having basic cybersecurity measures in place, the company did not have a dedicated Incident Response team or a comprehensive strategy to manage advanced threats. This gap left them vulnerable when they became the target of a sophisticated ransomware attack.



We Serve, We Prove, We Repeat

# Data

Incident Response Stats	Details
Ransom Demand	\$750,000 ransom was demanded by the attackers.
	\$0 was paid, thanks to backup recovery.
Data Recovery	95% of critical business data was successfully recovered from clean backups.
	Only 5% of non-critical data was lost.
Downtime & Financial Loss	The attack affected 80% of the company's systems.
	Each hour of downtime cost approximately \$50,000.
	Business operations were restored within 72 hours, minimizing revenue loss.
Containment	75% of systems were infected when the attack was first discovered.
	20% of the network was protected by isolating infected machines.
Threat Response Time	Infected systems were isolated within 2 hours of detecting the attack.
	Malware eradication was completed within 24 hours.
	Full data recovery and system restoration took 48 hours.
Security Improvement	60% reduction in vulnerabilities due to enhanced security measures, including patching, detection, and employee training.
Employee Training	100% of the workforce was trained in cybersecurity awareness post-incident, reducing the risk of future phishing attacks.
Financial Impact Avoided	By not paying the ransom and restoring from backups, the company saved \$750,000.

Removing the Risk  
from Universe!

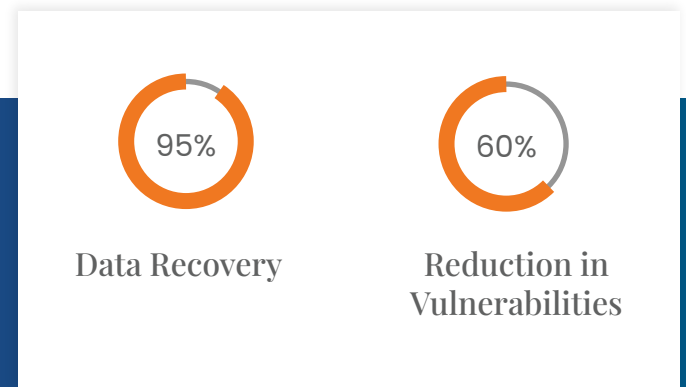
# The Cyber Attack

The attack began with a phishing email that appeared to be from a trusted vendor. One employee unknowingly clicked on a malicious link, which downloaded ransomware onto their machine. Over the next several hours, the ransomware propagated through the network, encrypting key files and servers. By the time the IT department discovered the attack, it had already spread to over 75% of their infrastructure.

The attackers demanded a ransom of \$750,000 in Bitcoin in exchange for the decryption keys. They also threatened to leak sensitive customer data if the ransom was not paid within 72 hours. The company was faced with critical decisions: pay the ransom or find another way to recover their systems.

## Client Challenges:

The client faced several immediate and long-term challenges due to the attack:



1

### Widespread Network Infection

The ransomware had infected 80% of their systems, including critical development environments and customer databases.

2

### Data Encryption

Sensitive customer data, internal documents, and critical code repositories were encrypted, leaving the company unable to operate.

3

### Threat of Data Leak

The attackers threatened to publicly release sensitive customer information if the ransom was not paid, risking severe reputational damage and potential legal consequences.

4

### Lack of Preparedness

The client lacked an Incident Response plan or team, meaning there were no predefined steps to contain or mitigate the attack.

5

### Operational Downtime

Every hour of downtime was costing the company an estimated \$50,000 in lost revenue, delayed projects, and damaged client relationships.

The company needed an immediate response to contain the threat, recover their data, and get their operations back online as quickly as possible.

# Our Incident Response Plan

Our team was called in to manage the crisis. Within hours, we initiated a comprehensive Incident Response Plan, involving both containment of the ongoing attack and long-term solutions to prevent future incidents.

## 1 Immediate Containment and Damage Assessment

The first step was to halt the spread of the ransomware and limit further damage. We took the following actions:

### ◆ Network Segmentation

We immediately isolated the infected machines from the rest of the network. This prevented the ransomware from propagating to the remaining 20% of the systems that had not yet been compromised.

### ◆ Shutdown of Infected Systems

To prevent further data encryption, we shut down all infected systems, leaving only essential, unaffected systems operational.

### ◆ Forensic Analysis

We initiated a detailed forensic investigation to understand the scope of the attack. This involved reviewing logs, monitoring unusual network traffic, and identifying the ransomware's entry point and propagation methods.

## 2 Threat Eradication

Once the attack was contained, we focused on eradicating the ransomware from the network

### ◆ Malware Removal

Using advanced threat detection tools, we identified and removed all instances of the ransomware from infected machines. This process was completed within 24 hours.

### ◆ Patch Management

We identified the vulnerability that allowed the ransomware to spread, which was an outdated software patch. We applied the necessary updates and security patches across all systems to prevent further exploitation.

## 3 Data Recovery Without Paying the Ransom

The client's backups were fortunately unaffected by the attack, but they were not well-organized or up-to-date. We initiated a recovery plan using available clean backups:

### ◆ Data Restoration

Over the course of 48 hours, we restored 95% of the company's critical data from backups. Although some non-essential data was lost, the majority of the business-critical information was fully recovered.

### ◆ No Ransom Payment

By leveraging secure backup systems, the client was able to recover their data without paying the ransom, saving them the \$750,000 demanded by the attackers.

## 4 Communication and Crisis Management

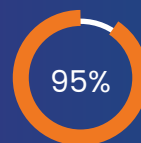
While the technical response was underway, it was equally important to manage the communication surrounding the incident. We assisted the client in:

### ◆ Internal Communication

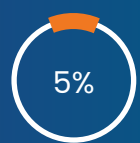
We worked with the client's leadership to inform employees about the incident, ensuring transparency and providing instructions on safe IT practices to prevent further infections.

### ◆ Customer Communication

We crafted public communications to notify customers about the breach, providing assurances that their data had been recovered and explaining the steps taken to mitigate the impact.



Recovered Critical data



Lost Non-Critical data

# 5

## Post-incident review and Long-term Strategy

After the immediate crisis was managed, we focused on strengthening the client's cybersecurity framework to prevent future attacks

### Incident Review

We conducted a full review of the attack, including its origin, methods, and impact. This allowed us to identify key vulnerabilities and areas for improvement.

### Security Upgrades

We implemented a multi-layered defense strategy, including endpoint detection, advanced threat monitoring, and regular security audits. We also deployed an automated phishing detection system to prevent future attacks from succeeding.

### Employee Training

Given the origin of the attack (phishing), we conducted comprehensive security awareness training for all employees, with a focus on recognizing and avoiding phishing attempts.



Cybersecurity Services  
Company that Extenuates Risks!

## Outcome

Our Incident Response team's rapid action and thorough mitigation efforts led to several positive outcomes for the client:



### Business Continuity Restored

Critical business operations were restored within 72 hours of the attack, minimizing downtime and financial loss.



### Data Recovery

95% of the client's critical data was successfully restored from backups, allowing them to resume operations with minimal disruption



### No Ransom Paid

By avoiding the ransom payment, the client saved \$750,000, while also avoiding the ethical dilemma of funding cybercriminals.



### Reinforced Security Posture

After the incident, the client's overall security framework was significantly enhanced. With advanced threat detection, regular security audits, and improved employee training, they saw a 60% reduction in vulnerabilities within six months.



### No Data Leak

Despite the attackers' threats, no customer data was leaked, thanks to the swift response and comprehensive containment measures.



The speed and professionalism of the Incident Response team were remarkable. They not only helped us recover from the attack but also ensured we are better protected against future threats. Their guidance throughout the crisis saved us from financial and reputational disaster

— Chief Technology Officer, Technology Firm



From Strategy to Success,  
Partners in every step!



This case study highlights the importance of a swift, coordinated response to cyber attacks. Through proactive containment, data recovery, and long-term security enhancements

We helped the client recover from a potentially catastrophic ransomware attack without paying a ransom or compromising their customers' data.

If your organization is dealing with a cyber threat or needs stronger Incident Response capabilities, reach out to us. We'll secure your operations and ensure a fast, effective recovery, minimizing damage and keeping your business running smoothly in the face of any attack.



✉ info@satrix.com

🌐 www.satrix.com

☎ +91 796 819 6800 | +971 52 930 4713 | +1 (325) 515-4107

📍 Registered office

28, Damubhai colony, Anjali cross roads,  
Bhattha, Ahmedabad - 380007

📍 Corporate office

B, 10<sup>th</sup> Floor - Krish Cubical, Sindhu Bhavan Marg,  
Thaltej, Ahmedabad - 380059