Ransomware Hits Your Business. Here Is Exactly What Happens Next

When a business is attacked by ransomware, a chain of serious incidents occurs immediately, affecting even complex financial operations.

The First 30 Minutes

It usually starts with a phone call from someone on your team who cannot open their files. Every document, every spreadsheet, every database has been encrypted. There is a text file on the desktop with instructions for paying a ransom in cryptocurrency. The amount is typically between $50,000 and $500,000 for a small to mid-sized business, with a deadline that creates artificial urgency.

Your instinct is to call your IT person. If you have break-fix support, they are unavailable, on another job, or need time to assess the situation remotely. If you have managed IT, the alert was before triggered the phone call came in. This difference in response time, minutes versus hours, often determines whether the damage stays contained or spreads to every system on your network.

Hour 1 Through 4: Containment and Assessment

The first priority is stopping the spread. Every infected machine needs to be isolated from the network immediately. This means pulling Ethernet cables, disconnecting Wi-Fi, and shutting down VPN connections. The instinct to turn machines off is understood but often wrong. Powering down can destroy forensic evidence

that Investigators need to determine how the attacker got in and whether data was exfiltrated before encryption.

During these hours, your IT team is trying to answer three critical questions. First, how did the attacker get in? Usually it is a phishing email, a compromised remote desktop connection, or an unpatched vulnerability. Second, how far did the encryption spread? If backups were accessible from the compromised network, they may be encrypted too. Third, was data stolen before it was encrypted? Modern ransomware groups almost always exfiltrate data first, giving them a second lever: pay us or we publish your files.

Day 1: The Hard Decisions

By the end of the first day, you are facing a decision tree with no good branches. If your backups are intact and tested, you can begin restoration. This typically takes two to five days for a small business and up to two weeks for larger organizations. During that time, operations are severely limited or completely halted.

If your backups are compromised or nonexistent, you are looking at either paying the ransom or rebuilding from scratch. The FBI advises against paying, and for good reason. Roughly 20 percent of businesses that pay never receive a working decryption key. Of those that do, 80 percent are attacked again within a year because the underlying vulnerability was never fixed.

Meanwhile, you have legal obligations. If you handle customer data, patient records, or financial information, breach notification requirements kick in. You need a lawyer who specializes in data privacy. You need a forensic investigation firm. You may need a crisis communications team. These are not optional expenses. They are legal requirements, and they add up fast.

Week 1: The Real Costs Emerge

The ransom payment, if you make one, is usually the smallest cost of a ransomware attack. Here is what the actual bill looks like for a typical 50-person business:

Incident response and forensics run between $30,000 and $150,000. Legal counsel for breach notification and regulatory compliance adds $20,000 to $75,000. Business interruption losses during the recovery period average $8,000 to $12,000 per day. System rebuilding and hardening costs range from $50,000 to $200,000. Cyber ?? insurance deductibles are typically $10,000 to $50,000, even when you have coverage. And the long-term costs, lost customers, damaged reputation, increased insurance premiums, continue for months or years.

IBM puts the average total cost of a ransomware attack at $4.88 million. Even at the low end for small businesses, you are looking at $100,000 to $300,000 in direct costs.

How to Avoid Being the Case Study

Every ransomware victim says the same thing afterwards: we thought we were covered. They had antivirus. They had a firewall. They had backups, or thought they did. What they did not have was a layered security posture with 24/7 monitoring, tested disaster recovery, employee training, and an incident response plan. A **backup and disaster recovery services** are the difference between a bad week and a business-ending event. If your backups are not tested and monitored, ransomware groups will find that gap.

The businesses that survive ransomware without catastrophic loss are the ones that prepare. They have endpoint detection that catches encryption threats before beginning. They have backups stored offline and tested quarterly.

They have employees who can spot phishing emails. And they have an IT partner who treats security as a continuous process, not a product you buy once. If your current setup does not include all of that, it is time to **explore cloud security and network monitoring services** .