MARSH

Surviving a Ransomware Attack: A Case Study

A project manager for ABC Inc., a manufacturer with $1 billion in annual revenue and operations in 30 countries steps off the elevator at company headquarters. She's returning to her office after a lunch break and is eager to get back to work on a major order for a large client that is due next week. But something's wrong.

When she sits down at her desk, she sees that her computer does not seem to be functioning. Instead of the usual desktop image on her monitor, she instead sees a lock and a disturbing message:

> *Your files are encrypted. If you do not submit payment to us — $5 million in bitcoin — within three days, your files will be lost forever.*

Worried, she calls ABC's IT manager on the other side of the floor, but the IT manager and his staff are too busy to answer. Other employees around the world are reporting that procurement and shipping software is inaccessible. At the company's factories in China, India, and elsewhere, assembly lines have come to a halt. And that same message is being seen on computers at every company office.

The company is a victim of ransomware — an attack that is growing increasingly more frequent, severe, and sophisticated.

A ransomware attack can disrupt a business for weeks, cost millions of dollars in downtime and restoration costs, and damage reputations. Millions more is often needed to pay the actual ransom. Personal information may also be exposed, resulting in significant costs for breach notification and credit monitoring. But with the right advisor and with effective planning and preparation, a business can weather the storm and take action to protect its operations, systems, revenue, and reputation.

Marsh can be that advisor to your organization, delivering recommendations before, during, and after an incident. Here's how a ransomware attack can play out, and how we can help you manage its impacts on your organization.

To Pay or Not to Pay

As critical data is held hostage and systems are rendered inoperable, ABC finds itself in an untenable situation. Operations are completely halted; the technology that powers ABC's manufacturing line is down. Employees cannot perform critical tasks — they cannot order components that go into their products, nor can they ship finished goods to customers.

With contractual obligations not being met and assembly lines idling, the company is losing money — every hour, every minute, every second. And with the threat actor's deadline looming, ABC's risk management and leadership teams face a critical decision: Should we pay the ransom?

Several factors should go into this decision. These include the criticality of affected data and systems, availability and integrity of data backups, cost of the ransom versus the estimated cost of restoration, the likelihood of successful restoration (whether the ransom is paid or not), and regulatory implications.

Organizations should develop guidance regarding ransomware decision-making and build this into their incident response plans. Generally, choosing to pay or not requires careful consideration and input from key stakeholders, including in-house and outside legal counsel and vendors.

As ABC considers its options, it can rely on Marsh for help.

1 Scenario 1: Paying the Ransom

ABC makes the decision to pay the ransom after determining that restoring its systems, files, and data is not possible — or at all timely. ABC quickly engages a law firm with specific expertise in ransomware to serve as the incident response coordinator.

Computer forensic teams actively investigate the incident and try to determine its scope while working to limit the spread of the malware. Crisis management and public relations teams are engaged to manage reputational harm.

ABC, meanwhile, is also busy getting the necessary internal authorizations and working with third parties to prepare for a cryptocurrency payment. Legal and regulatory checks must be performed, such as a review of whether payment is possible under rules established by the **Office of Foreign Asset Control**, which prohibits payment to certain sanctioned foreign parties.

A ransomware response vendor, meanwhile, begins negotiating with attackers on ABC's behalf for a reduction in payment demands and a later deadline. The vendor's specialists have seen this strain of ransomware before and understand how the threat actor group operates.

After initial communication with the threat actor group's "PR department," the vendor engages the threat actor group's "finance department" and succeeds in extending the payment deadline and cutting the required payment to $2 million in bitcoin. The ransomware response firm also tests the decryption keys to make sure they work.

ABC is ready to make payment. The company works with its legal advisors and ransomware response vendor to make a bitcoin payment to the cyber-attackers four days after the ransomware message first appeared. In exchange, its IT team receives a decryption key to restore access to the network.

The work, however, is far from over. It may take weeks to deploy the decryption keys across ABC's network and restore all impacted systems to full functionality. Additional forensics may be necessary to confirm there are no remnants of the malware, that backdoors are identified and eliminated, and that systems have been scrubbed clean.

Backups will need to be reconfigured and tested and data may need to be restored. To prevent incident reoccurrence, new hardware or software may also be needed as a part of reengineering IT systems and boundaries. The overall focus of reengineering is to improve the overall security environment and support improved cybersecurity monitoring.

ABC's cyber insurance coverage, secured with the help of its brokers at Marsh, can prove useful. ABC's cyber policy will reimburse the ransomware payment and cover the costs of the vendors that helped with the negotiation. Incident response, including attorney fees, PR expenses, and data restoration costs will also be covered, as is lost income during ABC's downtime and extra expenses that might have been incurred to keep operating.

In addition to securing your cyber policy, Marsh can help you navigate the carrier's vendor and ransomware reimbursement consent requirements. And we can help you prepare a business interruption claim to ensure that you maximize your cyber insurance coverage.

As ABC returns to some semblance of normalcy, the assembly line once again begins to hum.

2 Scenario 2: Not Paying the Ransom

In ABC's executive offices, the ransomware demand sparks heated debate. While some argue in favor of paying quickly to minimize the damage and resume operations as quickly as possible, company leadership ultimately concludes that the company will be able to make a near full recovery using its offline backups.

After engaging a ransomware response vendor, ABC also learns that the attackers hardly ever deliver a working decryptor key. For these reasons, ABC decides not to pay the ransom.

Instead, ABC works with its advisors — including consultants from Marsh, experienced cyber legal counsel, forensic analysts, and others — to determine the extent of attackers' presence within their networks and what data and systems may be compromised. Efforts are taken to contain the malware and to isolate and remediate impacted systems. Once the network is scrubbed clean, ABC then takes steps to restore backups and rebuild critical datasets.

ABC's cyber insurance coverage can again prove useful, responding in many of the same ways as if the company had paid the ransom. Its policy provides coverage for incident response, data restoration, business interruption, and extra expenses.

One week after the ransomware message first appeared, ABC successfully starts restoring access to its core systems and backup data, though the process is still a long one. As ABC rebuilds its IT infrastructure, some legacy systems need to be replaced. While operations can resume as active monitoring for indicators of compromise (IoCs) continues, ABC is only operating at 50% capacity. Once the network is scrubbed clean and purged of malware, the company gradually increases its capacity to get back up and running again.

Three weeks out, factory operations resume at 100% capacity and affected employees fully return to work. ABC can once again focus on its core mission of delivering high-quality manufactured goods to its customers.

Managing Claims

With cyber insurance responding in either scenario, the next phase for ABC is to seek recovery.

With help from Marsh, which regularly communicated with insurers as the company responded to the ransomware attack, ABC's risk management team gets to work capturing loss estimates tied to its downtime following the attack and cataloguing extra expenses incurred while responding. Documenting and capturing decisions regarding activities and resources during the incident as they are made is critical to ABC's successful claim development — and Marsh supports the process to help maximize insurance recovery

Once this information is in hand, ABC provides its cyber insurer with a detailed submission. Ultimately, the company is able to recoup the reasonable and necessary costs from the incident — subject to self-insured retentions — under the terms of its well-crafted cyber insurance policy.

Post-Incident Steps

The ransomware attack is over; ABC has weathered the storm. But there's still one final step in the process.

As part of its cyber incident response plan, ABC's final action is to conduct an after-action review. The purpose of this exercise is to understand and document what went well and what didn't — and how to address any gaps or weaknesses. That's a critical step to take in order to ensure ABC learns from the incident and is better prepared for the possibility of a future attack, which may be similar to the last one — or completely different.

With the help of a forensics provider, ABC learns that the ransomware entered its networks through a phishing campaign and was able to spread across its network with ease, scooping up administrative credentials along the way and even credentials for the company's industrial control systems. Armed with these findings, ABC develops an action plan to harden its cybersecurity with additional phishing tests, new multifactor authentication initiatives, and improved network segmentation based on system and data criticality. ABC also re-evaluates its cyber insurance limits as risk transfer has proven to be both critical and complementary to ABC's risk mitigation efforts.

As part of this exercise, the both Marsh and ABC review ABC's cyber incident response plan. Like a number of its peers, ABC's plan — while robust in many ways — did not specifically address a ransomware attack. But developing a plan specific to ransomware is critical to making timely decisions.

Working with Marsh and external partners, ABC is able to update its internal guidance around ransomware attacks, perform an IoC assessment, identify and document vulnerabilities or gaps, and review its backup strategy – and critically, align all key stakeholders around ABC's strategies to manage the organization's cyber risk. The bottom line: ABC is more confident, more aligned, better prepared, and better protected in the event of another ransomware attack in the future.

How Else Can Marsh Help You Manage Ransomware Threats?

Beyond providing support following an attack, Marsh can also help your organization address potential ransomware threats on an ongoing basis. We can offer:

- **Ransomware Insights:** An intelligence briefing detailing the ransomware environment, your potential vulnerabilities, top attack vectors, best practices for you to follow, and potential cost estimates.
- **Insurance Program Design:** Advice and guidance on key policy terms and conditions and program structures, insight into underwriters' priorities and objectives, and aggressive marketing on your behalf.
- **Ransomware Readiness Assessment:** A review of your current operations, with feedback and analysis based on best practices sourced from assessments of more than 1,400 businesses.
- **Cyber Financial Stress Test:** An estimate of the potential total cost of a ransomware or other cyber incident on your organization, which can inform critical decisions about cyber insurance and risk management strategies and investments.
- **Cyber Incident Response Plan:** Assistance in building or revising an existing plan to help you respond to a cyber event, with specific considerations for ransomware.
- **Cybersecurity Program Review:** A review of an organization's cybersecurity policies, plans, procedures, and training that culminates in a maturity assessment and actionable recommendations for improvement.

ABOUT MARSH

A global leader in insurance broking and innovative risk management solutions, Marsh's 30,000 colleagues advise individual and commercial clients of all sizes in over 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue over US$14 billion and nearly 65,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms. In addition to Marsh, MMC is the parent company of Guy Carpenter, Mercer, and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to *BRINK*.

CONTACT US

Contact your Marsh McLennan Agency representative to learn more.