(508) 339-5163
www.spadetechnology.com
info@spadetechnology.com

# Solutions & Success

## The Inside Story

## Spade Technology Helped This New England Construction Firm Minimize Damage From A Devastating Ransomware Attack

Ransomware would have caused a lot more damage to this New England construction firm if they hadn't gotten in touch with our team for expert assistance. Are you confident your current IT support could effectively respond to a ransomware attack?

What would you do if you found out you were infected with ransomware right now? If you don't have a plan to go on, then you're risking a lot right now, and every minute going forward.

You've probably heard a lot about ransomware and other cybercrime threats. It's easy to hype up the doom and gloom about cybercrime – fear is often a great motivator. At a certain point, it's probably turned into background noise, right? You hear so much about these types of threats that you may begin to become numb to it.

Here's a reminder of just how real cybercrime is: in May, a New England construction firm found out they had been infected with ransomware. They had to choose between a $47,000 ransom, or losing three months of work for their 20 employees.

Put yourself in their shoes — what would you do?

# This New England Construction Firm's IT Support Provider Was Scared

When this firm's CEO and his team discovered they had been infected with ransomware, he called his IT support to find out what to do.

"We had an IT guy we had used for years that was really inexpensive," says this firm's CEO. "I felt like the guy I had didn't know what to do. He seemed more scared of it than I was."

As they slowly realized the extent of the ransomware infection, it became clear that his IT support provider hadn't been properly protecting their systems, nor would he be capable of doing much to limit the damage and cost of dealing with the attack.

## That's When This Construction Firm Called Spade Technology

Recognizing the need for more capable IT support, this firm's CEO called Myles Keough, CEO of Spade Technology.

This firm's CEO had considered working with Spade Technology years ago, but, at the time, considered their rates to be too expensive. He opted for the IT support provider they had at the time ransomware attack instead, who charged a fraction of the rates Spade did.

"Like I tell my customers, 'You get what you pay for'," says this firm's CEO. "Unfortunately, I didn't know what I didn't know. We weren't safe. I called Myles because we had the ransomware attack."

## Spade Technology Discovered Just How Damaging This Ransomware Attack Was

As is often with cybercrime attacks like this, companies don't know how vulnerable they are until it's too late.

"The problem with technology is most people don't know what they just don't know," says this firm's CEO.

After giving this firm's CEO some immediate advice as to how to proceed, Spade's team came onsite to assess the damage and see what could be done.

This New England construction firm was using two servers, one old and one new. Most of their data had been migrated to the newer server, which is the one that had been encrypted by ransomware. Many of their work PCs had been infected as well.

While at the outset of the infection, only the data partition was encrypted, the other IT support provider had instructed this firm's CEO to reboot the server, which led to further encryption of the Operating System as well. That meant Spade's team couldn't even boot the server to determine the extent of the damage.

In order to get a better idea of the state of the server, the Spade team installed a new OS to view the encrypted files on the data partition. This was also a difficult process, due to the fact that the other IT support provider had accidentally let the support contract for that server expire and did not keep up-to-date with the firmware on that server.

Furthermore, even though his other IT support provider had told this firm's CEO that their backups were working, in reality, their last viable backup was over 90 days old. That meant that, at best, this construction firm in New England would lose more than three months of work for their staff of 20 employees if they didn't pay the ransom.

## This Construction Firm Tried Everything To Avoid Paying The Ransom

With the new OS installed on the server, Spade's team could finally determine which files were encrypted, as well as read the ransom note left by the hackers. They were requesting a bitcoin payment equal to approximately $47,000 in exchange for the decryption key.

Initially, this firm's CEO attempted to lower the ransom, claiming that they didn't have the necessary funds to cover the full amount. In response, the hackers did something truly unprecedented: they responded with a screenshot of this firm's CEO's business and personal bank accounts, showing they knew this New England construction firm could afford the ransom (as well as the degree to which they had breached their private data). Raising the stakes, the hackers then threatened to release the CEO's personal information if he didn't pay.

Next, this firm's CEO engaged two different companies that promised to be able to decrypt the files. Even if that were true (based on the level of encryption, Spade's team considered it to be unlikely) these companies charged a fee three times greater than the hacker's proposed ransom.

With his options exhausted, this firm's CEO decided to move forward with paying the ransom. If he didn't, he was risking hundreds of thousands of dollars worth of lost work, not to mention the ongoing wasted payroll wages he was paying as his staff waited to get back to work.

# Spade Technology Helped This New England Construction Firm Reduce The Ransom By $17,000

"Myles showed up, was calm, clear on what needed to happen, and knew what to do," says this firm's CEO. "Once he really saw how serious it was, he stepped up their efforts, and everything kind of calmed down."

Now resigned to paying the ransom (by far the least expensive of the options available to this New England construction firm) this firm's CEO had Myles and the Spade Technology team get to work. In order to minimize costs, eliminate associated risks, and ensure the decryption key was valid, Spade did the following:

- Spade logged a case with the FBI, even though their backlog of similar cases would mean it would be weeks until they would respond.
- A Spade Cyber Security Specialist cross-referenced the BitCoin ID in the FBI database to confirm that the hackers were not associated with a known Terrorist Organization. If they were, paying the ransom would lead to more trouble for the firm.
- A Spade contact was able to negotiate the ransom down to $30,000, saving the firm $17,000.
- Spade facilitated the conversion to BitCoin through a partner in Canada, who also received and tested the decryption key to ensure it was valid before paying the ransom.

"There are so many different parties that get involved," says this firm's CEO. "It's cheaper to pay the ransom than it is to recreate the data."

# Spade Technology Made Sure This Construction Firm Was Properly Protected Against Future Ransomware Attacks

With the ransom paid and the data decrypted, the next step for Spade was to make sure this firm's systems were properly protected so that they wouldn't get hit with ransomware again.

The Spade team made a wide range of improvements to the IT systems and provided ongoing management, testing, and training services to help mitigate the risk of another ransomware attack

- **Cybersecurity System Enhancements:** Spade configured and deployed a range of solutions to prevent malware from compromising this New England construction firm's systems:
  - Consolidated data to one server, including a properly configured Active Directory with Group Policies deployed to standardize and secure the environment.
  - Deployed new and rebuilt existing PC's, incorporating them into the new Active Directory, and customized them based on the user's role to prevent unnecessary permission to access data.
  - Deployed a new firewall and remote access solution to harden perimeter security.
  - Deploying a commercial grade, secure wireless solution.
  - Deploying DUO for Multi-Factor Authentication (MFA) to prevent unauthorized access (e.g. when the hackers logged into this firm's CEO's bank accounts).
  - Redesigned and implemented a more efficient network switching infrastructure.
  - Deployed a robust antivirus and antimalware solution.
- **Data Backup:** Spade implemented a robust backup, disaster recovery, and business continuity solution that is tested regularly via virtualization tests. This ensures that this construction firm can recover to a recent backup of their data in the event they are infected with ransomware again.
- **SupportWerks Services:** Spade's ongoing IT services would further help to proactively prevent cybercrime events, lower the risk of malware infections, and comprehensively secure their IT environment:
  - Cyber Awareness Training and ongoing testing of users to make sure that employees wouldn't put the organization at risk.
  - Regular Network Penetration Testing to confirm that cybersecurity measures are effective.

- Dark Web monitoring and alerting to discover if usernames and passwords associated with this New England construction firm have been leaked online.
- Weekly Operating System, MS Office, and third-party patch management to keep systems up to date with recent security patches.
- Cloud-based umbrella security to protect devices while in and outside of the office.
- Quarterly audit reviews that give this firm's team peace of mind that precautions are in place to prevent a future attack.

“Working with Spade, you find out a lot of what you don’t know by doing what they say,” says this firm's CEO. “You find out what a strong defense really looks like.”

## This New England Construction Firm Invested In Spade Technology To Make Sure This Never Happens Again

Even though Spade’s services are more expensive than this firm's CEO’s previous IT company, if it means he can avoid another ransomware attack like this one, it’s a worthwhile investment.

“It’s not cheap, but you get what you pay for,” says this firm's CEO.

While the Spade team is glad they could help this firm minimize the extent of the damage caused by this attack, they’d rather start working with a client long before it ever happens.

When it comes to cybercrime, an ounce of prevention is worth a pound of cure. By working proactively to protect your organization, you can avoid attacks like the one that hit this construction firm.

“Small businesses don’t typically have a lot of money to put together the type of systems you need to put together to be reactive, and so owners will turn a blind eye to it,” says this firm's CEO. “One of the lessons is, ‘don’t think you’re safe; pretend you’re not’.”

And don't think that just because you haven't had to deal with ransomware yet, you never will. It's a major threat to businesses and will strike without notice.

According to Coveware's Q4 Ransomware Marketplace report:

- The average ransomware payout is $84,116
- The highest ransom paid by a target organization was $780,000
- The average ransomware attack results in 16.2 days of downtime

**Spade Technology** can help you avoid that kind of damage to your organization. All you have to do is get in touch and to get started proactively protecting your business.

> ***"I'm loyal to Myles because he came in and helped me and he takes his job really seriously, Spade is a good company with a very strong culture of service that is top-down.***
>
> - New England Construction Firm's CEO

SPADE TECHNOLOGY
MAKING YOU BETTER

(508) 339-5163 | www.spadetechnology.com
info@spadetechnology.com