Why Reactive Recovery Doesn't Work

How ETC TechSolutions prevents Cryptowall catastrophes using StorageCraft backup solutions.

STORAGECRAFT®

STORAGECRAFT.

Data protection has many layers. Between anti-virus and anti-malware programs, firewalls, encryption, and more, it's a complicated process. And despite best efforts to keep systems protected, viruses and other malicious programs can still get in. That's why one of the best defenses against a variety of threats is a good backup and disaster recovery plan.

Emerson Yerian is the president of ETC TechSolutions, an Ohio-based IT managed service provider specializing in small and medium-sized businesses. He knows the value backup and recovery brings to small businesses, though he says a lot of business owners don't, and therefore might not be willing to invest in it. He's met a lot of people in his twenty-plus years in IT and says there are generally two types: those who value their technology and those who don't. These two types of people have very different outcomes when trouble comes their way, but as Emerson notes, it's always the ones who don't want to invest in technology that cry the hardest when something like ransomware brings their business to a standstill.

The trouble with reactive response

Proactive protection is crucial in the technology world, but one potential client ETC recently encountered wasn't willing to take the appropriate steps. ETC found this client while they were running a promo offering two free hours onsite. These free hours let ETC offer advice on how they might improve the network they're auditing, but one person who called them wanted to save his time for when he had a problem rather than preemptively addressing potential problems.

"We asked him to let us come take a look at his systems, give him an audit, and look at where we might be able to fix issues—we even told him he could hang on to the two hours for later if we could do an audit. He refused and wanted to just wait until there was a problem," Emerson says.

Sure enough, it wasn't long before Emerson's phone rang. "We got a call one afternoon and he said every time he scanned a document into his accounting software, it would get corrupted. He wanted us to look at his scanner," he says.
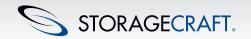
> "We told him he had three options: pay the ransom, go out of business, or rebuild his business after losing all the data... The guy didn't have a backup and he ended up in trouble."
>
> Emerson Yerian, President,
> ETC TechSolutions

Emerson's team found the problem, but it wasn't the scanner. The server had been infected with Cryptowall 3.0, a common ransomware virus. Ransomware like Cryptowall makes its way into a system through a seemingly innocuous email attachment or from a malicious website. It will find files on the infected computer and encrypt them. After locking the files, the virus warns you that you must pay a ransom within a time limit or your data will be encrypted forever. This could be important client data, intellectual property, or any variety of data critical to operations.

Emerson knew the solution was to restore the system with a backup. The trouble was, this business had no backups. Without them, the business was low on choices.

"We told him he had three options: pay the ransom, go out of business, or rebuild his business after losing all the data. He kept asking how much it would be to get the data back but we had no idea—we don't decide that—whoever makes the virus decides that. There's a lesson here. The guy didn't have a backup and he ended up in trouble," Emerson says.

If ETC had been allowed to give an assessment in the first place, one of their first suggestions would have been backups, and this business would have been fine. Once again, it's all about how a business values the role technology plays in their operations.

The benefits of being proactive

Ransomware doesn't have to result in lost data. Businesses that take proper measures can get around it, which is just what H&S Tool, a manufacturer of various hand tools, discovered. In their case, the relationship with ETC started not because of a virus, but because of a backup solution that was never properly implemented.

"H&S was using an online backup company," Emerson recounts. "A vendor came in and sold them a backup solution, but the vendor never actually installed it. H&S was paying for a backup solution that they never even got close to using. One day they called the vendor and said, 'hey we lost some information, can you recover it for us?' Lo and behold, they couldn't get any information back because it was never backed up in the first place—they were toast. Luckily, in this instance it was just a file or two and it wasn't a major catastrophe."

After this issue, H&S searched around until they discovered ETC, which could upgrade some of their equipment and provide them with IT management. H&S was ready to make some proactive investments in their technology. Emerson explains,

"They called around and found us. We started evaluating what they had and quickly realized that nearly all the equipment in the office needed to be replaced. We put together a proposal with a new server, twelve or thirteen new PCs, set up new networking and rewired the whole place top to bottom."

As many IT providers know, backup is a crucial part of any managed services agreement. Considering the importance, and considering the trouble H&S already had, Emerson made backups with StorageCraft® ShadowProtect® a priority.

"The big piece for us was the backup. In this case, we were using a basic ShadowProtect backup to a NAS drive, then a secondary copy offsite just in case. A lot of our customers are really small and don't have the need to be back up and running in thirty minutes, so these are designed to give them a basic backup if something goes wrong."

"Without StorageCraft, these guys would have had no choice but to pay the ransom or go out of business."

Emerson Yerian, President, ETC TechSolutions

But even with the best laid plans, trouble can still find you. Despite having their entire environment managed by ETC, and despite anti-virus, firewalls, and other measures that lock down a network to prevent any sort of attack, Cryptowall still managed to infect their systems.

"The call came in when they couldn't access their accounting software—we thought it was a problem with the accounting program and started looking there first. About a half an hour in we realized it was a virus causing the problem. Once we realized it was Cryptowall we decided we had to restore data from a backup. We weren't even going to take a chance on other options," explains Emerson.

Emerson got to work as quickly as he could.

Why Reactive Recovery Doesn't Work

"The call came at 4:30 and by 6:30 I was onsite. I wasn't sure how the Cryptowall virus worked exactly, so we backed up the corrupt data just in case we needed to go back—we actually could've solved the problem faster if we weren't being extra cautious. We restored the backed up data from the NAS to the affected equipment and had them back up and running by about one o'clock in the morning. Without StorageCraft, these guys would have had no choice but to pay the ransom or go out of business," he says.

Since Emerson had their server back on track by morning, H&S Tool had no downtime and didn't miss any crucial manufacturing deadlines—they barely noticed a problem at all.

Conclusion

No one can say when a problem will bring systems down or cause you to lose data, so it's wise to invest in backup and disaster recovery sooner rather than later. Taking proactive measures to protect your systems is the only way to be certain you can quickly recover from malware, hardware failure, or any other data disaster.

About ETC TechSolutions

ETC TechSolutions was founded in 2007 by Emerson Yerian and provides computer services and solutions to small business and nonprofit organizations. ETC has provided break/fix services since the beginning, but to improve their services, has also added managed services to proactively monitor the health of client's computer systems. Actively managing systems lets ETC receive warnings when issues arise so they can minimize downtime and save clients money.

Their mission is to deliver technology services and solutions that provide economical, scalable solutions to maximize technology investment.

www.etctech.net

About StorageCraft

StorageCraft Technology Corporation develops best-in-class business continuity software and services for physical, virtual, and hybrid environments running on Windows and Linux systems. StorageCraft's award-winning solutions for backup, disaster recovery, system migration, data protection, and cloud services, help you and your clients recover every time, everywhere, from any disaster.

www.storagecraft.com