STORAGECRAFT®

Backup Fast, Recover Faster

CASE STUDY: CPI SOLUTIONS

STORAGECRAFT®

THE BEST DEFENSE IS SOLID BDR

When your company is responsible for managing 4,000+ servers and desktops for several small businesses in Southern California, the best defense against downtime is a solid backup and disaster recovery (BDR) solution.

StorageCraft® partner CPI Solutions (www.cpisolutions.com) knows this from experience. They take care of technology for companies throughout Ventura, Los Angeles, and San Bernardino counties.

"At CPI, we're about keeping your business up and running, resolving your problems quickly, and providing you with reliable IT support when you need it," says Arnie Friedman, president and CEO of CPI Solutions.

A few months ago, their support team was put to the test when 10 clients experienced ransomware attacks.

"Typically, ransomware will encrypt all local files on the machine, then all network attached storage drives and the files on them," says Jerry Wissinger, lead NOC technician for CPI Solutions. "This data is 'locked up' and cannot be retrieved unless the user pays a ransom."

Examples of ransomware include CryptoLocker or Crilock, CryptoDefense, CryptoWall, and Reveton. This type of malware may invade an unprotected computer through an email attachment or a download from a scam website.

The ransomware "worms" through the computer's files and encrypts them so the user can't access the data without a key to unlock the encryption code. A pop-up screen (like the one above), usually with a countdown clock, appears with instructions for how to pay the ransom and get the key to unlock the computer.

The hackers use anonymous payment systems such as MoneyPak and Bitcoin to collect ransom. According to Geek.com, the creators of CryptoLocker may have collected as much as $30 million in ransom.

CPI Solutions didn't want clients to be forced to pay criminals who were holding their data hostage. So, when the first call about ransomware came in, CPI was ready to restore the client's data – with no ransom paid.
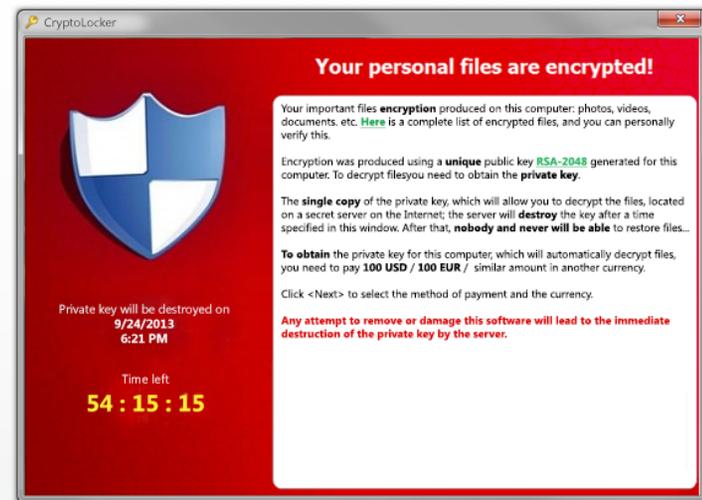
DEFENSE SAVES BUSINESSES

The first sign of trouble was when a client called CPI Solutions because she couldn't open a spreadsheet file – or any of her files, as it turned out. The client was a property management company with three locations in California.

The CPI support tech inspected the file server and discovered that all of its files had been encrypted by ransomware, not just the files on the client's workstation. Ransomware had infected the entire server, locking up all of the company's sensitive data, including financial information dating back several years.

Because CPI Solutions uses StorageCraft ShadowProtect® to back up and protect its managed IT client data, there was a very recent backup that was still unaffected by the ransomware.

"ShadowProtect allows us to take backups at frequent intervals with little interference with a client's server resources. This enables us to choose from a variety of restore points, limiting the impact the malware has on the customer," explains James Oberhaus, vice president of managed IT services for CPI Solutions.

After accessing the most recent clean backup with ShadowProtect, the CPI technician was able to fully restore the servers within a couple of hours. While the company's servers were fully restored and functional within two hours, the user's computer had to be rebuilt. The workstation was fully functional within a business day.

"If we had not been able to restore the servers, sensitive customer and financial data – from the years leading up to the attack – could have been lost," Jerry says. "This particular user had access to all of the company's financial and operational information, so the malware spread from her computer to the server, locking up the entire company's data. It all could've been lost without ShadowProtect."

What happens when companies hit by ransomware don't have ShadowProtect?

"Without an effective backup solution, data must be retrieved from the hacker thieves by paying ransoms," he says. "The typical ransom is $500. This will usually be for only a piece of the data."

Once the ransom is paid, the user is sent a decryption key to retrieve their encrypted data. Depending on how much data was encrypted by the ransomware, a company could end up paying tens of thousands of dollars to retrieve all of their data – assuming the hackers send the decryption key. Sometimes they don't.

"The whole ransom process can take days and doesn't always help retrieve all of the data. If it does, it usually costs the company thousands of unbudgeted dollars," he says.

Since the first client's call, CPI Solutions has used ShadowProtect to help nine more clients recover from ransomware attacks and save their businesses from loss.

STORAGECRAFT®

CPI Solutions has been a StorageCraft partner for less than two years. Prior to using ShadowProtect, they used multiple products for BDR.

"We were looking for a more reliable and usable backup solution for our clients. We'd been experiencing a 15% to 20% failure rate with other backup solutions. We wanted to consolidate down to one standard option, and StorageCraft offered the best solution for us," James says.

Using multiple backup technologies wasted time and resources. After CPI Solutions standardized on StorageCraft, their business changed.

"Now our failure rate for backups is only about 1% to 2% at most, typically due to hardware and networking issues and not the backup technology itself. StorageCraft has opened the door for us to have a fully managed off-site backup solution for our clients," he says.

The reliability of ShadowProtect means CPI doesn't have to send technicians to client sites as often as before. As Jerry describes it:

"ShadowProtect just works every time – it's simple. Other products have presented a variety of issues. ShadowProtect is just the best all-in-one solution for us and our clients."

STORAGECRAFT.
SHADOWPROTECT ®

STORAGECRAFT.

ABOUT CPI SOLUTIONS

Founded more than 30 years ago, CPI Solutions is a regional leader in IT consulting and technology services in Southern California. They offer consulting, managed IT services, application development and audio-visual solutions, 24 x 7 technical support and cloud services.

CPI Solutions provides end-to-end managed IT services for companies throughout Ventura, Los Angeles, and San Bernardino counties. They offer the ability to offload individual IT functions and workloads, or clients can fully outsource all IT functions.

"With a managed IT services program in place, you can shift your focus to the things that make a real difference to your organization – while lowering costs, eliminating distractions, and attaining superior levels of service," explains Arnie Friedman, president and CEO of CPI Solutions.

The company has been recognized for its business and technical leadership with awards that include CRN Tech Elite 250, SFV Business Journal Largest IT Consulting Firm, Inc. 5000 Fastest Growing Company, and SFV Business Journal Best Places to Work.

In addition to StorageCraft, CPI Solutions has technical alliances with Cisco, Citrix, Dell, HP, LifeSize, Microsoft, NetApp, Nimblestorage, PaloAlto Networks, ShoreTel and VMware.

STORAGECRAFT®

ABOUT STORAGECRAFT

At StorageCraft®, the goal of complete disaster recovery drives everything we do. Our StorageCraft® Recover-Ability™ solution is an end-to-end, best-in-class backup and disaster recovery solution that is both fast and reliable.

STORAGECRAFT RECOVER-ABILITY

It starts with a good backup. Our award-winning *StorageCraft® ShadowProtect®* takes complete, pristine images of your machines, including all your operating systems, applications, services, and settings.

It then records changes at the sector level, so you always have an up-to-date copy of every machine in your IT environment, whether it's a critical server or an employee laptop, physical or virtual. We even work with specialized database servers, like SQL, SharePoint, or Exchange. You can get granular recovery in Exchange with *ShadowProtect Granular Recovery for Exchange*.

You have complete control over the frequency of your backups and you can set rules for consolidation and retention to manage your precious storage space using *StorageCraft® ImageManager™*.

Plus, with *StorageCraft® ShadowControl® CMD™* you can monitor the machines in your backup environment from a single interface and get alerts when a machine is running out of space, when a backup doesn't happen, or when any of a variety of conditions you specify is met.

We also give you tools to test your backups using *StorageCraft® VirtualBoot™* and *StorageCraft® Image-Ready™* technologies, which gives you confidence that your data is safe and that a disaster won't shut you down or hold you up.

Then we make it easy to replicate your backup images with *StorageCraft® Cloud Services™* or to our cloud or to your own offsite location so you can always have your data close when you need it and at a good safe distance when a disaster comes.

When it does, you can launch your backups as virtual machines with VirtualBoot or mount them as drives for complete, granular access to your data.

Or you can pre-stage the recovery of a backup image in a virtual machine with our patented *StorageCraft® HeadStart Restore®* technology, so if your main server blows up, you can be up and running in minutes. You can even virtualize your data in our cloud so even Mother Nature can't keep you down.

Then, you can rebuild your infrastructure and recover to all kinds of machines, physical or virtual, using our *StorageCraft Hardware® Independent Restore™* technology or *ShadowProtect IT Edition*.

You can't be sure what kind of disaster will strike you next, but with the StorageCraft Recover-Ability solution, you can be sure it doesn't matter. You'll be just fine.

CONTACT US

StorageCraft Technology Corporation

11850 S. Election Road, Ste. 100 Draper, Utah 84020 USA

Phone: 801.545.4700 Fax: 801.545.4705

www.storagecraft.com

contactus@storagecraft.com