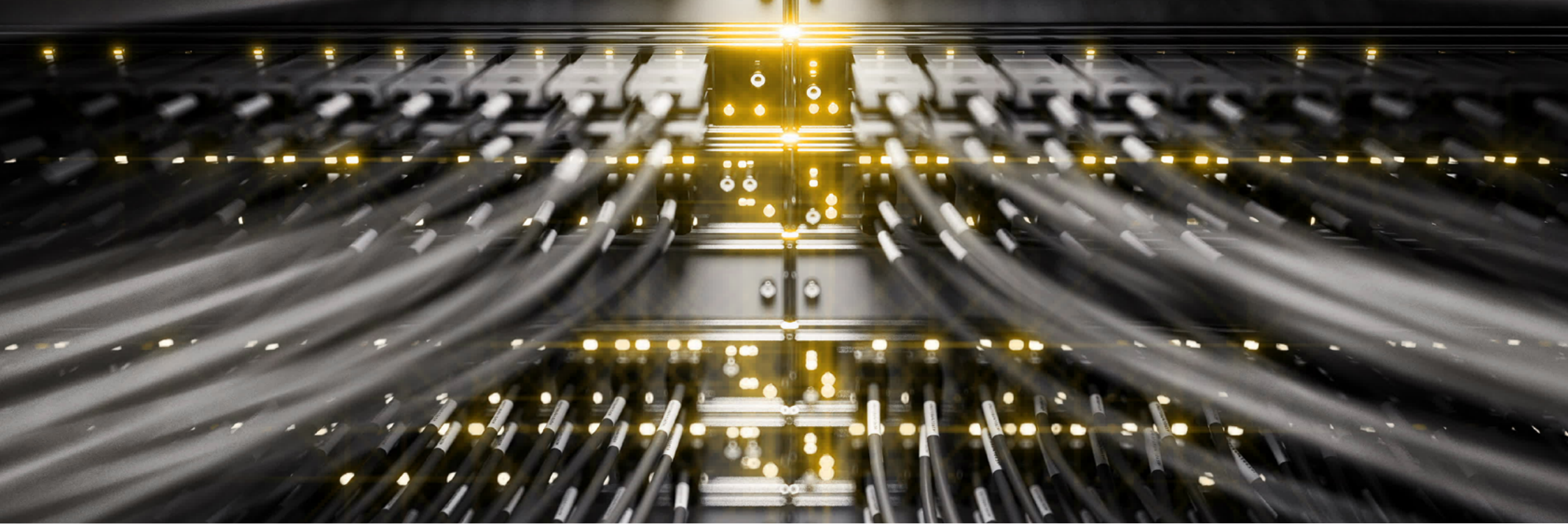


Ransomware Has Crippled Your Data Center – Now What?

A DCK guide to the options available to IT organizations whose data is held hostage by criminals demanding ransom.

MARIA KOROLOV

Published October 2019

DataCenter Knowledge™

Table of Contents

Introduction

Earlier this year, an employee at a European law firm received an email that appeared to be a legitimate message from a legitimate source with a link to a legitimate website. The person clicked the link and saw a message that said the page did not exist anymore. “They weren’t immediately suspicious,” said Ilia Kolochenko, CEO at the Swiss cybersecurity firm ImmuniWeb. But the page – which didn’t even seem to load – was home to a drive-by malware download, which infected the employee’s machine.

“And it started spreading,” said Kolochenko. The company didn’t have any internal network segmentation, so once the malware was in, it could spread to other machines, network devices, and storage… Then the ransomware activated. “Half of their mission-critical machines were encrypted,” Kolochenko, whose firm the victim company turned to for help, said. While some data remained available, the law firm had lost access to key documents related to upcoming litigation and court appearances. “They couldn’t perform their daily tasks,” he said. “They needed this information urgently.”

And, unlike your garden-variety ransomware attackers who typically ask for a small ransom they figure an average user is willing to pay, these attackers asked for the equivalent of $200,000 in bitcoin. That’s a sign that the attack was targeted, Kolochenko said. Not only were the emails designed to appeal to this company’s employees, the attackers knew how much money the company could afford to pay.

The firm tried to see if the ransomware could be reversed or removed without losing crucial data. “The answer was negative. And they decided to pay the ransom.” Not only did they need to get back to work as quickly as possible, the ransom would go up in a week, then again a week later, then again, and again.

Kolochenko helped the firm find a company where it could buy Bitcoin, and they were able to make the payment within 24 hours. Two business days later, they had received all the decryption keys.

But it doesn’t always work out this well.

CyberEdge recently surveyed 1,200 IT security professionals who had suffered a ransomware attack in the 12 months preceding the survey, whose results came out this February. While 28 percent said they paid the ransom

Introduction (continued)

and recovered their data, 17 percent said they paid but lost their data anyway. More than 44 percent did not pay but recovered their data, and about 11 percent said they didn't pay and lost their data.

A 2018 global ransomware by SentinelOne found that 42 percent of organizations that paid a ransom did not get their files decrypted.

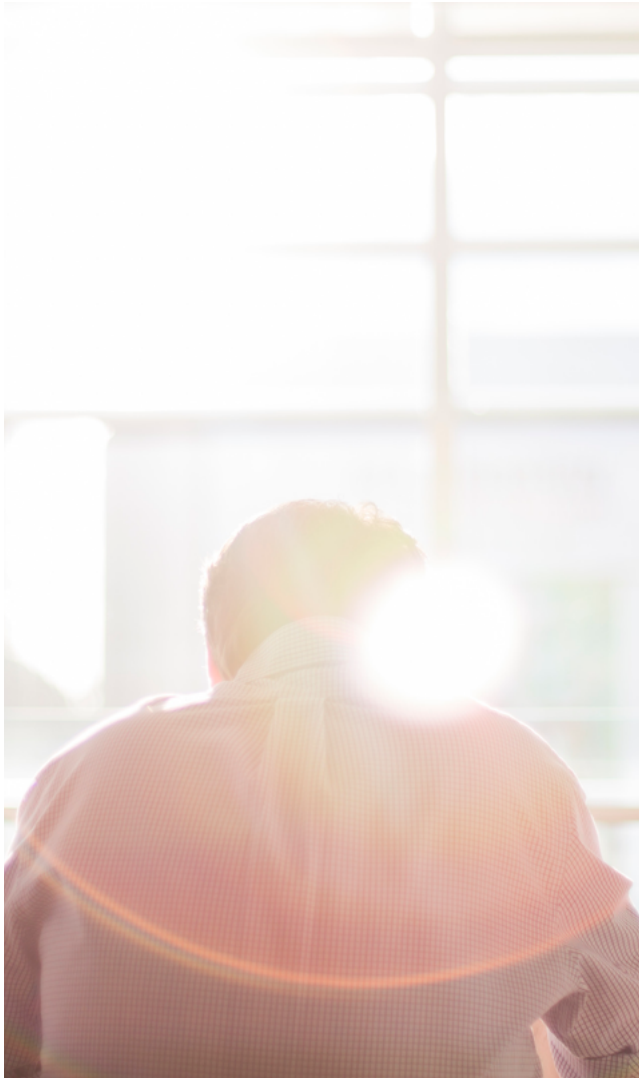
Other experts put success rates of paying the ransom higher. Coveware, a ransomware response company, said 96 percent of its customers who paid a ransom received a working decryption key and were able to recover 92 percent of their encrypted data.

So, who's right? If your organization has been paralyzed by ransomware, should you pay up and hope for the best?

Ransom amounts are rising quickly. In June, for example, two cities and Florida wound up paying more than $1 million to attackers. According to Forrester Research, the number of ransomware attacks on businesses was up 500 percent from the same time last year, projected to cost businesses $11.5 billion in 2019. If there's a good chance that the criminals will just take the money and run, the cost-benefit calculation for the victim changes.

CyberEdge CEO Steve Piper stands behind his firm's numbers. The independent research company has been doing this survey for six years, he said. "Our survey margin of error is 3 percent, and our results are consistently comparable year after year," he added.

Ransomware is holding data hostage in your data center – NOW WHAT?



1 Identify and Contain the Damage

The first thing to do is not to panic.
"Ransomware is not literally life-and-death for most companies," said Curtis Fechner, principal consultant, threat management, at Optiv Security, a Denver-based security firm. "There is some time to think things through." For example, rushing to restore from backups might make things worse. "Think about the scope of the incident. Figure out what systems and users are impacted. If possible, isolate infected resources from the rest of the corporate network."

Also, see what hasn't been affected, he added. This is a good time to take backups offline, for example, to protect them from the attack.

Data center managers can also slow or stop the spread of ransomware by closing Remote Desktop Protocol ports, since RDP-based attacks are prevalent. And, in case the ransomware compromised administrative credentials, change administrator passwords and end all logged-in administrator sessions. If attackers are hanging out in your network, watching what you're doing, this should kick them right out. Other user credentials should also be changed. The attackers got in somewhere, and if the passwords aren't changed, they'll try to get in through that channel again.

This is also a good time to run immediate backups of all critical data that hasn't been touched by the ransomware. Even if an infection looks like it's been contained, there might still be malware lurking somewhere, lying in wait before springin out again.

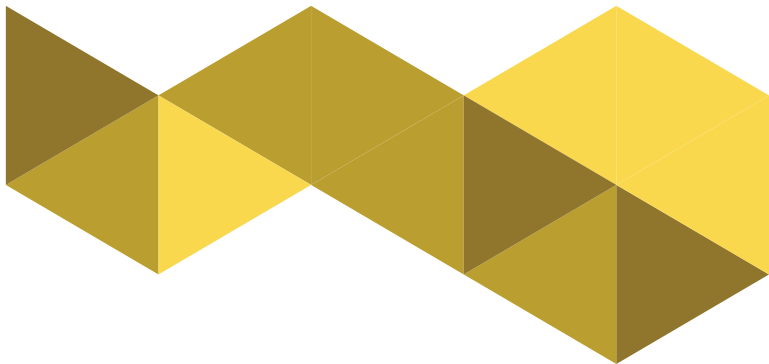
To identify the type of ransomware, take pictures of the ransomware announcement screens. "File names may have extensions on them that can help," said Fechner. A data center's antivirus vendor may also have resources to help identify the ransomware and what damage it tries to do.

It's important to contain the damage before restoring from backups, since otherwise the ransomware will just reinfect the restored machines – or, worse yet, see where the backups are and go after those files.

Akshay Bhargava, senior VP of products at Malwarebytes, said a financial services firm recently called his company in to help with a ransomware attack. "They have a data center, and a few machines had been hit and encrypted," he said. "And they were concerned that they had a breach." The data on the affected machines was lost.

"But we were able to identify what the threat was, how it entered, and what it was doing in the network. And we were able to remediate the trojans and the worms trying to propagate. We were able to limit the bleed, prevent further damage."

Bhargava added that it can be useful to make an image of a couple of infected machines to help with diagnostics. "But if you have limited resources and time, you want to try to get a backup of the machines that haven't yet been infected."

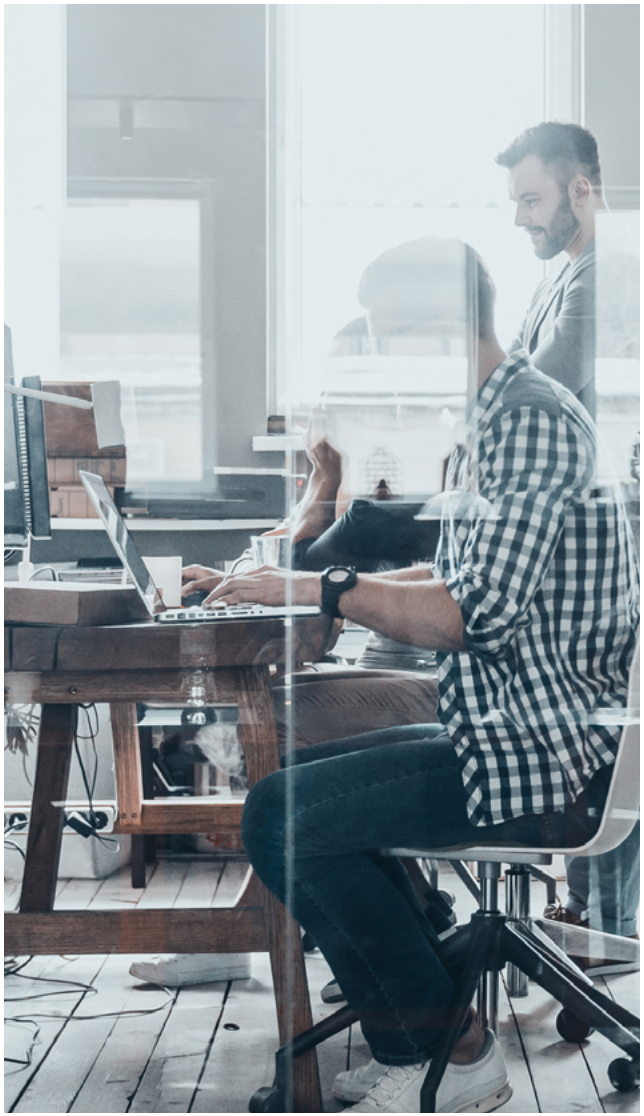


2 Notify Relevant Contacts

If a company has an incident response plan in place, there should already be a list of people to contact – security experts who specialize in ransomware removal, legal and compliance teams, public relations, and, of course, senior management. Affected clients or internal users should also be contacted and kept up to date as the situation progresses.

If there's no plan, there might not be an established relationship with a specialist incident response firm that can step in and help deal with the crisis. But most big security firms will probably be able to offer some help, though there might be a delay or additional costs involved in setting up a new relationship. "If you call me out of the blue, what happens is that you pay the full rate, because you haven't set up a retainer type of process," said Chris Scott, global remediation lead of IBM X-Force IRIS (Incident Response and Intelligence Services). A managed security service provider or the legal counsel's office might be able to recommend a vendor to contact.

Even if the ransomware only hit one machine and was contained quickly, it could have already spread feelers elsewhere. An expert will be able to tell how far it got – and what else, in addition to the ransomware, the attackers might be planning.



A call to the FBI's cybercrime division may also be warranted. A cyberinsurance policy may require a police report, and if the attack is big enough, the FBI might actually be interested in helping.
Plus, if the bureau can better track attacks, it will be better positioned to take action.

Report your attack to your local FBI field office or to the FBI's Internet Crime Complaint Center.

Click to view the US Federal Government Cyber Incident Reporting Guidelines

You may also want to notify the local police department to get a paper trail going, reach out to the US Computer Emergency Response Team and file a complaint with the FTC.

3 Try to Restore

The best solution to a ransomware attack is to simply roll back all affected machines to their last good state, the most recent backup before the ransomware hit. Before doing that, scan the backups for malware and be careful not to open a gateway to your backups for the attackers. Cybercriminals have been getting better at targeting backups, but they can only hit backups that they can access.

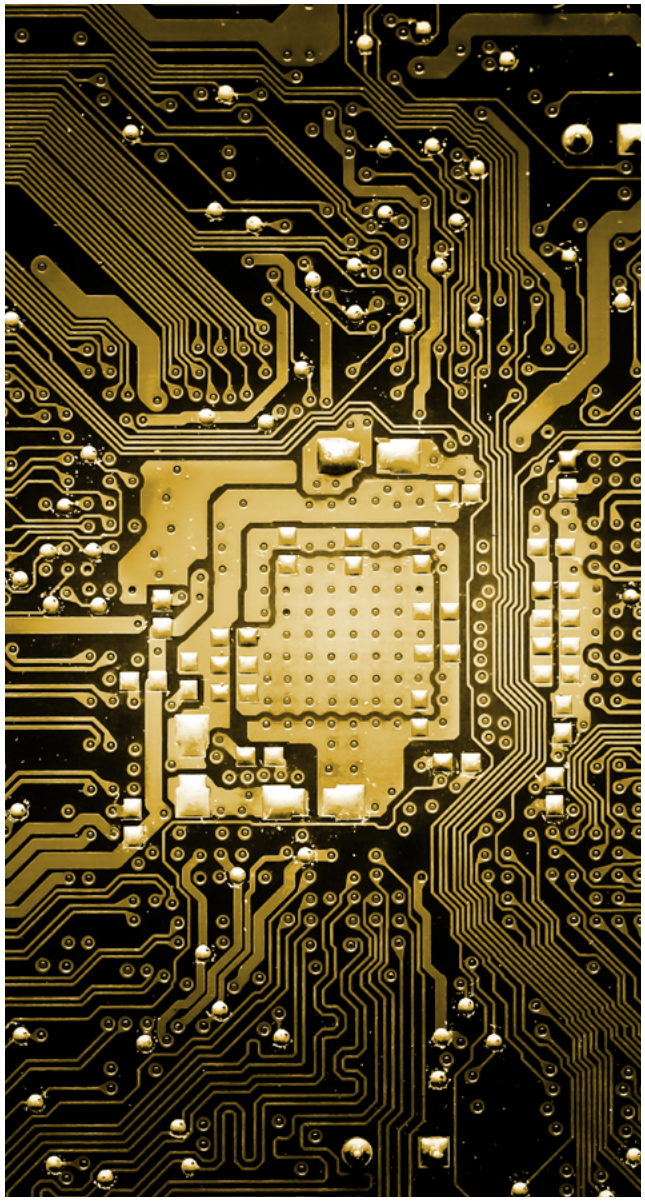
Offline backups, "air gapped" storage, and any backup that has WORM (write once, read many) functionality are safe from ransomware.

These days, all the major cloud storage vendors offer low-cost long-term backups that can't be modified after they've been written. On Amazon Web Services, check out the Glacier Vault Lock on Amazon Glacier Storage; on Microsoft Azure it's the Azure Blobs Immutable Storage; and Google has its own version, known as the Bucket Lock for Google Cloud Storage.

"Leveraging cloud services for this kind of backup is a very cheap, effective way of ensuring that your backups are safe," said Brian Johnson, CEO and co-founder at DivvyCloud, an Arlington, Virginia-based cloud security vendor. "All the cloud providers have something like this."

If a data center already its data in the cloud, copying the data over to these WORM backups should be quick and easy, he added. "There are no technical reasons why people don't do it, just people reasons. You're basically spending time and energy and effort on what is basically an insurance policy, which is what backups are. Sometimes companies think, 'This isn't going to happen to me.' Or they say, 'I've never been hacked before. As long as I build a wall high enough, I'm okay.'"

If a data center that's been attacked doesn't have good current backups, there might be an older set, suggested Joe Partlow, CTO at ReliaQuest, a Tampa-based cybersecurity company. "Some data is typically lost," he said. "But most data history is likely intact, and other methods of catching up the data transactions may be available, such as paper records or other event or transaction logs."



4 Check If the Ransomware Can Be Reversed

Sometimes, the ransomware is a bluff.
"We've seen fake ransomware," said Shawn Kanady, director of SpiderLabs DFIR at Trustwave Holdings, a Chicago-based cybersecurity firm. "It will look and feel just like real ransomware and will throw up a page that says 'pay us' just like real ransomware would. But it doesn't do anything – it doesn't actually encrypt the files." The idea is that some people will panic and pay the ransom. "What we would do is have our clients disconnect those systems from network access and manually go through those files and try to open them to see if they're actually encrypted."

Even if the ransomware is real, there might be a way to get around it. For example, older ransomware versions might have decryption keys available online. One good resource to start with is the No More Ransom Project, sponsored by Europol and McAfee. Another free service is ID Ransomware.

You can also search for the name of the ransomware and the word "decryptor," said Jonathan Tanner, senior security researcher at Barracuda Networks. But if you do download a decryption tool, be careful with the source. "Take care that you verify that the author is a legitimate anti-malware or security company so you don't download something that further infects your infrastructure."

Security vendors might also be able to reverse-engineer the ransomware. "Sometimes, the ransomware had bad programming, and we're able to reverse and decrypt," said Scott of IBM's X-Force IRIS. But that happens less than 10 percent of the time, he added. If a security vendor is promising a higher success rate because of some secret sauce they've got, that secret sauce might be that they just pay off the hackers.

According to a recent report by ProPublica, some ransomware recovery companies – including Proven Data Recovery, MonsterCloud, Dr. Shifro, and Red Mosquito – promise to decrypt your data while actually just charging a huge markup and then paying the ransom.

"A service to simply decrypt ransomware files does not exist," said Kevin Latimore, former law enforcement investigator and enterprise malware removal specialist with Malwarebytes. "That's what people want, but many of those services are fake."

5 Should You Pay the Ransom?

No organization wants to pay ransom money to criminals or terrorists. Giving them money just helps them improve their malware and encourages more people to get into the ransomware business. Plus, there's a good chance that paying the ransom won't work, and criminals don't offer money-back guarantees.

If the data lost isn't mission-critical or can be recovered through some other means, it might make sense to just wipe the affected machines and rebuild from scratch. If you do that, save a copy of the encrypted system first. Even if a decryption key is not available now, it might become available in the future, as security experts work to create decryption tools.

Sometimes though, you don't have a choice.

"If you have ransomware in a data center and have hundreds of thousands of servers or petabytes of data that you're concerned about, you might lose the business," said Shawn Kanady, director of SpiderLabs DFIR at Trustwave Holdings, a Chicago-based cybersecurity company. For example, Trustwave once had a case where a medium-sized manufacturing company's corporate data center was hit. "The ransomware spread very fast," he said. "The initial impact was a system administrator who had mapped drives to where the backups resided. The ransomware spread to those backups, and when they called us, they knew they were in some trouble. It was crippling their business – they were faced with production losses at this point." This ransomware was brand-new, without a known cure. "They were looking to us to try to decrypt and create a key, which is almost impossible to do."

In another case, a company that operated a foundry was hit by ransomware and decided to pay the ransom. It was able to shut down network access to the infected machines and stop the attack from spreading from an infected laptop to its data centers – but not before the attack hit the foundry floor.

"The foundry did not have active backups it could restore for the foundry controller machines," said David Hobbs, security evangelist at Radware, an Israel-based security company. Each day of lost productivity would cost the company up to $1 million and rebuilding the computers would take too long. "The ransom request was $40,000, and the foundry was able to get a discount down to $35,000," he said. "This was paid to the hackers via a wire transfer through Western Union. They were back in business within two hours."

In some cases, companies have decided to pay the ransom even if they have backups, because it takes too long to get to those backups. According to Coveware, average downtime increased in the second quarter of 2019 to 9.6 days, from 7.3 days at the beginning of the year. And downtime can add up to significant costs – often much higher than the ransom amounts.

The SentinelOne survey shows a similar effect. According to the survey, US companies that paid ransomware in the previous twelve months paid a total of about $57,000 on average. But the total average business cost of the attacks, including ransom, lost business, and time spent responding, was more than $900,000.

Cyber insurance may or may not be able to pay for the ransom. "We're in the wild west of it," said Shawn Kanady, director of SpiderLabs DFIR at Trustwave. "Each contract is going to be different in how they handle this situation." In some cases insurance only covers the ransom payment if the company hit by ransomware had all the recommended security in place but the ransomware was so advanced that it still got through.

Some insurance companies may penalize firms for giving in to extortion. "A cybersecurity insurance policy could be invalidated because of a ransom payment," said Rick Holland, VP of strategy at Digital Shadows.

There might be other problems associated with paying ransoms. For example, some ransomware attackers have been linked to Iran. No ransomware victims have been prosecuted for sending money to terrorists, but that could change, especially if those terrorists use the money to stage a particularly devastating attack. There could also be significant public relations damage if the news gets out, so some due diligence is called for here.

6 How to Pay the Ransom

For smaller amounts, a company can go ahead and pay the ransom on its own, by buying bitcoin on Coinbase or another large, reputable cryptocurrency exchange. But if the ransom is in the tens or hundreds of thousands of dollars, an outside expert might be helpful.

And even if the initial ransom demand is small, attackers may up the amount if they discover they have a big fish on the line. According to the SentinelOne survey, 58 percent of attackers demanded more money after a victim organization paid the first ransom demand.

Since most companies don't have a large supply of bitcoin on hand, a ransomware specialist can be helpful by facilitating the payment and avoiding delays associated with creating a new bitcoin wallet.

Forrester recommends bringing in a ransomware payment specialist to negotiate with the attackers and validate the decryption key before making the payment. The analysts identified six vendors in this space: Coveware, Cylance, Cytelligence, Flashpoint, Kivu Consulting, and NEST Consulting. They recommend keeping communications "respectful" – something that might be difficult when a company is about to lose major customers, or, as with health care organizations, when lives are at stake.

If there's a good line of communication, however, a company might be able to negotiate a discount, especially if it doesn't need to decrypt all its systems. For example, if a company decides to pay a ransom even though backups are available, because restoring from backups would take too long, it might buy decryption keys for just the most critical systems and restore the rest later.

Before making the payment, especially when large sums of money are involved, ask for "proof of life." For example, you can send the attackers an encrypted file and see if they can decrypt it.

7 You've Paid the Ransom and Got the Keys. NOW WHAT?

If the attackers follow through on their promises and send the decryption keys, these keys can now be used to unlock the infected machines.

"But that doesn't mean that all of a sudden all your systems are back online," said Scott, with IBM's X-Force IRIS. "It may take you weeks of labor, touching each computer, entering the decryption key, and reconfiguring all your systems." And even then, your work isn't done. "When you recover, you don't want to trust the machines the attackers have been on. You'll want to rebuild and rearchitect, because you don't know what you missed."

Then, you should go ahead and harden the security of your entire organization. The hackers now know that you have weak security and are willing to pay ransoms. They might come back in the future with new attacks, and they might have even left some malware hidden on your systems that can reemerge at any point.

In fact, according to the SentinelOne survey, organizations that paid ransoms were targeted again 73 percent of the time. "Attackers treat paying companies like ATMs," said Migo Kedem, director of product management at SentinelOne.

This is the time to review all security systems, including network segmentation and advanced endpoint protection – or make plans to put them in place if you don't have them yet. Other security basics include enabling two-factor authentication, implementing least privilege access controls, and upgrading and patching all systems.

And, most importantly, set up multiple levels of backups. Live backups that can be immediately and easily accessed if a system goes down or a critical file gets erased can effectively address simple ransomware attacks that hit individual computers and don't spread. A second set of backups should be kept on isolated systems that advanced, aggressive ransomware can't touch.

In addition, companies should have a schedule to test the backups to make sure they're working correctly and are easy to restore from. If a data center paid a ransom even though backups were available because restoring would take too long, it's time to look for a new backup system.

"It really comes down to if you have backups, and how much downtime can you suffer," said SentinelOne's Kedem.

Ransomware Has Crippled Your Data Center – Now What?

MARIA KOROLOV

Published October 2019

DataCenter Knowledge™