The best defence against Ransomware

ITPro.

In association with

wasabi hot cloud storage

Welcome

EDITORIAL

Editor
Maggie Holland
maggie_holland@dennis.co.uk

Contributors
Adam Shepherd

Design
Friyan Mehta

Head of Content Strategy
Riyad Emeran

ADVERTISING & REPRINTS

Advertising Director
Chris Cannon
chris_cannon@dennis.co.uk

LICENSING & SYNDICATION

International Licensing
Dharmesh Mistry

MANAGEMENT

Chief Revenue Officer
Julian Lloyd-Evans

Chief Executive
James Tye

Company founder
Felix Dennis

Dennis Publishing Ltd

Ransomware is a threat that has been with us for a long time, and thanks to some recent, high-profile cases – coupled with our increasingly dispersed, and therefore increasingly vulnerable, networks – the spotlight has swung back around to this key area in IT security. In this report, brought to you in association with Wasabi, we will explore how these threats are evolving – and the new solutions that are emerging to keep our critical systems safe.

- Maggie Holland, Editorial Director, B2B

Contents

About Wasabi

Since 2017, Wasabi has been changing the cloud storage landscape with hot cloud storage, a disruptively simple, one size fits all cloud storage technology that is one-fifth the price and faster than the competition with no fees for egress or API requests. Wasabi is game-changing, leading-edge cloud technology that allows users to affordably store an unlimited amount of data. Wasabi is an entirely new approach to cloud storage... a bottomless cloud that grows with your business.

01 Ransomware Rising

How this global threat and its countermeasures continue to evolve

If you're reading this report, then chances are you're concerned about the threat ransomware poses to your organisation. It's a sensible fear – ransomware attacks are never far from the headlines, but the last 12 months have seen a string of particularly troubling incidents.

For example, in May 2021, the DarkSide hacking group hit the systems of Colonial Pipeline with a ransomware infection. The company is responsible for operating a fuel pipe network running from Texas to New York, and transports more than 100 million gallons of petrol, diesel, and other types of fuel every day. The pipeline supplies almost half of the US east coast region's fuel, so when the ransomware outbreak halted operations, it led to fuel shortages, price increases and widespread turmoil across huge sections of the country.

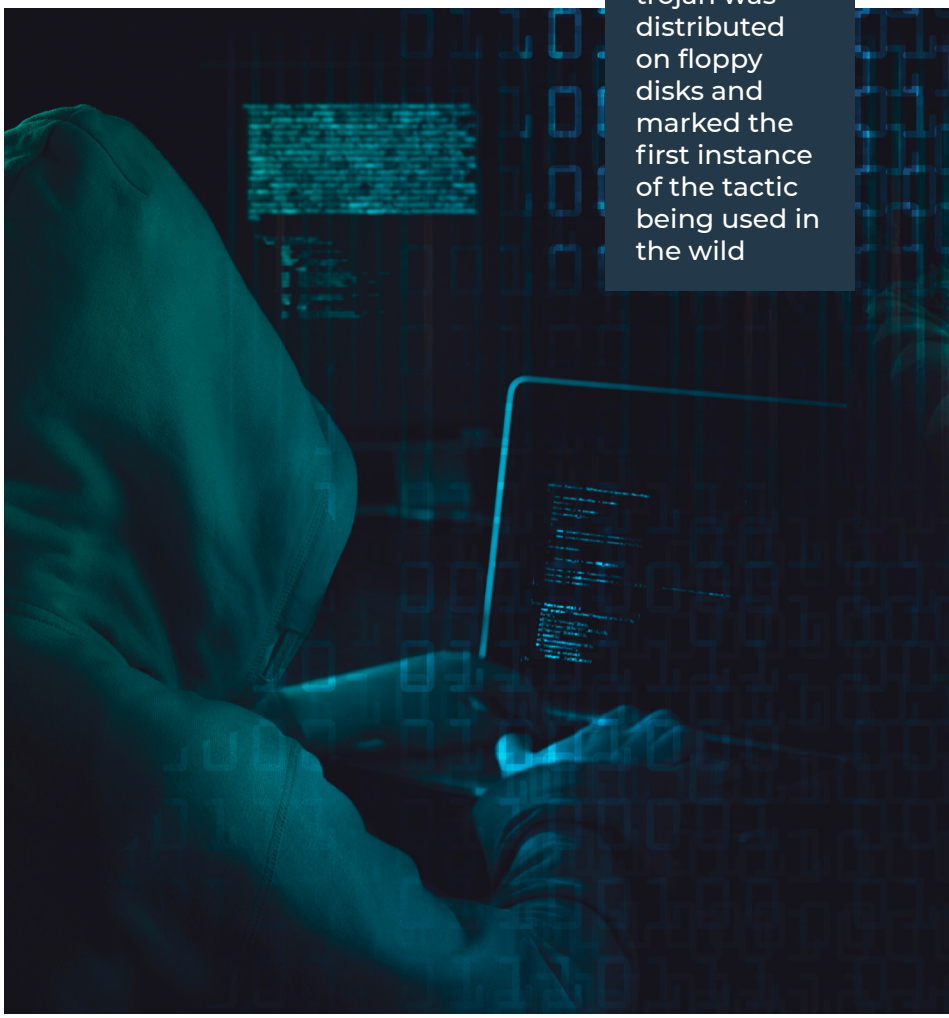
Even more recently, IT provider Kaseya was hit by another ransomware attack – this time courtesy of the REvil group. The hackers used a security flaw in the company's VSA software to deliver ransomware to around 50 of Kaseya's customers. While this may sound like a relatively manageable number of victims, the incident was complicated by the fact that a large number of those customers were managed service providers (MSPs) that each oversee the IT and security for a number of their own clients – each of whom was then potentially vulnerable too.

AN ONGOING STRUGGLE

Ransomware itself is far from a new phenomenon. It's generally agreed that the so-called 'AIDS trojan' of 1989 – which was distributed on floppy disks and used basic symmetric encryption to lock users files – was the first example of the tactic being used in the wild, but even the CryptoLocker ransomware that kickstarted the modern wave of attacks is coming up to ten years old. Malware creators have spent the intervening years iterating and innovating on this foundation. Much like biological viruses, new ransomware variants emerge with such frequency that combating them is an almost Sisyphean task.

1989

The AIDS trojan was distributed on floppy disks and marked the first instance of the tactic being used in the wild



Much like biological viruses, new ransomware variants emerge with such frequency that combating them is an almost Sisyphean task

There has been progress: Sophos Security's annual State of Ransomware report indicated that the number of organisations impacted by ransomware has fallen by almost 15% compared to last year, and cases where hackers successfully encrypted their targets' data were down by almost 20%.

Sadly, however, this does not mean that ransomware is less of a threat. The number of organisations that paid hackers to decrypt their data actually rose in the last year. Coupled with the fact that, on average, only 65% of the data was restored once the ransom was paid, this presents a fierce dilemma for victims.

If businesses don't have the technology in place to rapidly recover from an attack, the losses incurred by prolonged downtime can actually make handing over the money a more financially attractive option. This is the decision Colonial Pipeline made when it coughed up $4.4m to DarkSide in exchange for its systems. With all this in mind, it's little wonder that, according to Sophos' report, the cost of recovering from the average ransomware attack has more than doubled to $1.85 million.

This can partly be attributed to a continual evolution of the tactics used by ransomware gangs. While perennial favourites like phishing emails, drive-by downloads and credential stuffing remain among the most popular tools used to deliver their payloads, hackers are continually researching new vulnerabilities in popular software that can provide them with routes into their targets. Even pre-existing flaws can be exploited, if they remain unpatched.

$4.4m

The sum coughed up by Colonial Pipeline to Dark-Side in exchange for its systems

The last three years have seen swathes of public sector institutions across the globe falling victim to ransomware

THE POLITICS OF RANSOMWARE

A further issue is the growing overlap between criminal activity and state-sponsored attacks. While a substantial amount of ransomware campaigns are operated by organised criminals with purely profit-driven motives, national military and intelligence organisations around the world have increasingly been subcontracting these groups to carry out politically motivated attacks. North Korea, Russia and China have all been linked to major malware outbreaks, and this trend has led to cyber criminals being given access to government-level tools and resources in order to target their victims.

The SolarWinds attack of 2020 was a prime example of this. A group of hackers compromised a popular software platform belonging to the network monitoring company, and then used it to plant trojans within the networks of many of its customers, including US-based tech companies, government agencies and cyber security companies. According to a joint statement by various US law enforcement agencies, the operation was carried out by a group linked to Russia's Foreign Intelligence Service in order to conduct espionage, but the attack also opened up a swathe of unrelated victims to opportunistic data theft and extortion.

This attack also demonstrates the changes in how cyber criminals are selecting their targets. The SolarWinds attack, as well as the Kaseya incident mentioned above, both involved supply chain attacks, where hackers compromised an upstream partner in order to infiltrate more valuable targets further down the supply chain. This strategy can be particularly devastating for industries that rely on multiple layers of procurement, as each successful new intrusion multiplies the potential target list, which can lead to exponential increases.

2020

A group of hackers compromised a popular software platform belonging to SolarWinds, and used it to plant trojans within networks of its customers

The last three years have seen swathes of public sector institutions across the globe falling victim to ransomware, as well as countless private companies, and while law enforcement and security firms are working together to try and stem the tide, attackers are continually innovating new ways to circumvent defences and exploit weaknesses. Despite the progress that has been made, the threat remains as real as ever.

However, there are steps that you can take to protect your organisation and its data. Over the following pages, we'll lay out the current ransomware threats facing businesses and how best to mitigate them, helping to ensure that you're able to avoid – and, crucially, recover from – this developing danger.

02 What makes a company vulnerable?

Understanding ransomware is the first step to protecting your business from it

Clearly, ransomware remains a threat for organisations of all sizes across multiple sectors. In order to defend against it, organisations must be aware of what it is that makes companies vulnerable to these attacks. To explain that, however, we first need to understand how ransomware works.

In broad terms, ransomware attacks leverage security flaws to gain access to a computer system, whereupon a malware payload is dropped. This malware encrypts all of the files and data on the system, rendering it unusable. Ransomware packages generally come pre-loaded with instructions for victims, informing them how to deliver a payment to the perpetrators (usually in cryptocurrency) in exchange for having their data unlocked.

Ransomware comes in many different flavours, including common examples like Cryptolocker, BadRabbit and GandCrab which are repeatedly tweaked and re-used by numerous criminal organisations. These are often deployed in large-scale campaigns, aiming to target the largest number of potential victims, and while they're easier for security software to detect and quarantine in the event of a suspected infection, the sheer scale at which they're used is difficult for security companies to keep up with.

Many ransomware attacks are random and opportunistic in nature, often driven by automated delivery mechanisms. What's more, for more precise strikes against specific targets, unique custom malware is often created. This is much harder to guard against, as it likely won't have been seen anywhere else. For particularly important attacks, hackers may even exploit zero-day vulnerabilities which have yet to be identified or patched.

These factors, coupled with the rapid pace with which cyber criminals adapt their tactics and methods, make ransomware infections exceedingly difficult to prevent – particularly for larger organisations. The broad attack surface of modern IT infrastructures is challenging to protect: to paraphrase a famous IRA quote, hackers only have to be lucky once, whereas defenders have to be lucky all the time.

RAPID RECOVERY

With this in mind, what makes an organisation vulnerable to ransomware isn't necessarily how robust its front-line defences are, or how well it can stop ransomware infections from occurring. Instead, the true measure of how susceptible a business is to ransomware should be taken from how prepared it is to respond to the all-but-inevitable outbreak when it does happen.

As noted in the previous section, the cost of extended downtime can be severe, so organisations that are not able to recover quickly from attacks often have no choice but to capitulate to hackers. Security initiatives like No More Ransom have made progress in creating free decryption tools for some of the most common forms of ransomware, but these aren't always an option.

In fact, in some cases, the attackers do not even have the ability to decrypt their victims' data. The so-called 'NotPetya' outbreak, for example, was designed to destroy target machines under the guise of a straightforward ransomware attack, and the encryption it used was all but impossible to reverse.

Instead of focusing exclusively on prevention, then, one of the more popular strategies for combating ransomware is to ensure that you have a robust incident response plan which includes a comprehensive backup strategy. In the event of an infection, this allows a victim to simply restore their last working backups, getting up and running again with a minimum of downtime and lost data.

NotPetya

An outbreak that was designed to destroy target machines under the guise of a straightforward ransomware attack, and the encryption it used was impossible to reverse

BUILDING A BACKUP STRATEGY

There are some important considerations around how your backup strategy should be configured for maximum effectiveness with regards to ransomware, though. Backups should cover employee workstations, as well as file storage systems and any critical server infrastructure, preferably at a VM level. This will minimise disruption in the event of widespread infection.

Backups should also be configured to run at regular intervals, depending on how regularly each system is used and how critical the files within are. Fileservers and storage arrays, for example, will need to be backed up daily, or even hourly, while employee machines can probably get by with weekly backups. The key question to ask is: what is

the maximum length of time between backups, and what is the most data we could theoretically lose if we had to restore?

Resilience is the watchword, and the more confidence you have in your ability to restore a state of stable operation from your backups, the less danger a ransomware infection poses. If your backup strategy means more lost data as part of the restoration process and involves long recovery times, you may find yourselves at the mercy of your attackers.

It's also important to consider the different kinds of backup infrastructure available to you. On-premises backup stores snapshots and recovery files on an appliance within your own data centre, while cloud backup (as the name suggests) offloads the storage duties to a third-party provider. On-premises backup has certain advantages for general tasks – it's lower-latency, you have more control over the environment, and it's sometimes cheaper to run at large scale – while cloud-backup is better suited for guarding against ransomware specifically.

The reason for this is that if an attacker makes their way onto your network to deliver ransomware in the first place, there's a good chance that your on-premises backups may be compromised as well. If your organisation has been targeted directly, then attackers may seek out and destroy your backups before activating their payload, while an inadvertent infection may find its way into your backups by chance.

Cloud backups remove this threat by physically separating your backups from the rest of your IT infrastructure, and while the industry previously struggled with the misconception that cloud was inherently less secure than on-premises, it's now generally accepted that cloud infrastructure is no riskier than self-hosted appliances. In many ways, it can even be safer, as dedicated cloud providers like Wasabi may have more resources to dedicate to things like security patch application and proactive threat monitoring.

Instead of focusing exclusively on prevention, one of the more popular strategies for combating ransomware is to ensure that you have a robust backup strategy

In the world of cyber security, prevention is usually better than cure, but ransomware bucks that trend somewhat. While a strong threat prevention strategy should by no means be overlooked when combatting this particular breed of malware, a robust and well-thought-out backup strategy is a far more effective way to safeguard business continuity.

The technology ensuring that backups remain unencrypted

The rapidly-shifting ransomware threat landscape makes stopping infections outright a challenging prospect, and a robust incident response strategy is essential for ensuring a strong defence against disaster. With that in mind, it's important to consider how best to configure your backup processes for maximum effectiveness.

As we touched on in the previous chapter, backups aren't always a foolproof defence against ransomware. If the network that your backups are on is compromised, there's a reasonable chance that they might also be encrypted. This isn't to say that local backups serve no purpose, though – having a copy of your data that you can quickly access can be incredibly useful in the event of a software glitch, an OS update that breaks compatibility with a specific program, or even just the perennial problem of accidentally erasing an important folder. For relatively minor issues like these, local backup snapshots are perfectly adequate for ensuring speedy business continuity. What they're not so good for, however, is recovering from ransomware.

PROTECTING YOUR BACKUPS

This is where the famous '3-2-1 rule' comes into play. A guiding star of data protection policies for decades, this principle states that you should ideally have three copies of your data, kept in two separate locations, with at least one of those situated offsite, disconnected from your network. This belt-and-braces approach greatly reduces the possibility of all of your backups being lost, deleted or tampered with.

There are also other methods that organisations can use to protect their backups, including data protection policies like WORM (Write Once, Read Many). WORM policies, also known as 'immutability' rules, can be configured to ensure that once data has been written to a given storage pool, that data cannot be deleted or modified in any way, not even by the admin who created the pool. These policies can be applied for the lifetime of the storage pool, or they can be set to specific time periods such as a certain number of days, weeks, months or years. With properly-configured WORM policies, even if your backup location is hit by ransomware, it can't be encrypted.

The final component of the 3-2-1 rule relies on the concept of 'air-gapping', which simply means disconnecting a system or network from other machines within the IT estate. For example, an appliance which is used to store offline backups could be air-gapped by ensuring it can't connect to the public internet or the local network, and by keeping it in a dedicated facility away from any other equipment. The logic is that, if there are no digital or physical links between a critical system and other, potentially hackable, machines, that vital system will remain untainted even if the rest of the network is compromised.

3-2-1 rule

A guiding star of data protection policies for decades, this principle states that you should ideally have three copies of your data, kept in two separate locations, with at least one of those situated offsite, disconnected from your network

The problem with air-gapped offline backups is that, by definition, they are inconvenient and time-consuming to maintain. Backup data must be physically taken to the off-site location in question, and manually transferred to the air-gapped system. This also means that the backup data must be physically retrieved from the site before it can be used to perform a system restore, which adds additional time to the already costly process of recovering from a ransomware infection.

FINDING SAFETY IN THE CLOUD

Cloud backup services can be an effective way to marry the security of offsite, air-gapped backups with the convenience of local backup, allowing rapid data access in the event of a catastrophe without introducing unnecessary risk. Cloud services aren't inherently immune to the dangers of ransomware – just like physical backups, any cloud storage services with a persistent connection to your network can be affected by an outbreak – but by combining cloud backups with immutable WORM policies and robust data retention periods, the potential downsides can be minimised.

Because backup jobs are run based on a defined schedule, cloud backup platforms like Wasabi don't maintain the same constant connection to the user's network that a real-time syncing tool like Microsoft OneDrive or Dropbox does. Instead, it's only connected while the backup job is being run, which may only be on a weekly or monthly basis, depending on the desired frequency. Even if a ransomware payload is hidden in a backup file, Wasabi's immutable buckets are immune from being encrypted, assuming WORM limits and retention periods have been properly set up.

These retention policies, incidentally, can also be helpful for meeting compliance requirements. Wasabi's immutable storage buckets, for example, can be configured not only to prevent any alteration to their contents for a certain period, but to delete the contents entirely after that period has elapsed. This can aid in complying with GDPR, which states that personal data should only be retained for as long as it is needed. On the other hand, the ability to set indefinite retention periods helps meet data protection requirements like HIPAA and MiFID, where records must be kept for longer.

Backup management is a crucial part of a strong security posture, and it requires a commensurate level of time and attention. There's no such thing as a 'set it and forget it' backup solution – even once you've established your destinations based on the 3-2-1 rule, you should still be performing regular tests on your backups to ensure that they're up to snuff. When you fall prey to ransomware, the last thing you want is to discover that your backups haven't maintained their integrity.

Fortunately, however, while maintaining a backup strategy is a demanding task, there are elements of it that can be streamlined. Wasabi's immutable storage buckets merge the convenience of local backups with the security of offsite air-gapping, forming an ideal foundation for a resilient defence against ransomware infections and helping your business bounce back as soon as possible.

THE BACKGROUND

Located 30 miles north of San Francisco in the highly desirable city of Novato, the Novato Unified School District (NUSD), which started out as a one-room schoolhouse in 1859, today serves 7,500 students and employs 1,200 staff across its 16 schools.

Amir Kioumars, data systems supervisor for NUSD, is part of the IT team of 13 that supports students and teachers. "IT is the heart of the organisation because of the processes we create and the services we provide," Kioumars explains. "I'm part of the data team which focuses primarily on back-end data management and networking infrastructure."

THE CHALLENGE

When Kioumars first joined the NUSD IT team, he was surprised to learn that the district did not have a disaster recovery solution.

"Not having a DR plan in place caused me a number of sleepless nights because I knew that at any moment, we could get hit by a ransomware attack and we would be defenseless against it," Kioumars says. "At the district where I worked previously, we were hit twice by ransomware and were down for 10 days. I was afraid the same thing could happen at Novato at any time."

In addition to lacking ransomware protection that could ultimately result in business downtime, the legacy backup solution was cumbersome and risky. It required manual babysitting, which was eating into the team's valuable resources, and also posed a concern with data inconsistency as backups weren't routinely performed.

"It got to a point where we just had to change," says Kioumars. "The legacy solution was holding us back. My main goal was to have our mission-critical data backup application running 24/7 at a secure, offsite location. And I wanted to automate it as much as possible, allowing the system to do the job faster and more reliably, freeing up my time to focus on higher value-add initiatives for the school district."

THE SOLUTION

Kioumars evaluated data backup solutions from ten different companies, putting each through an extensive comparison process. He ultimately chose to collaborate with Wasabi – working alongside cloud data management company Rubrik – to protect the district's critical student and financial data.

For its cloud storage needs, NUSD went with Wasabi hot cloud storage which serves as a highly secure, off-prem storage repository. "We chose Wasabi based on price, customer support, and ease of setup and use, supported by Rubrik," he says. "Unlike legacy cloud storage services with confusing storage tiers and complex pricing schemes, Wasabi provides straightforward and predictable pricing with no charges for data egress. So even if I have to restore data from the cloud, I don't pay an egress charge penalty to do so.

"The difference between them and the bigger players in the market was staggering. I am confident I made the right choice with Rubrik and Wasabi."

THE RESULT

Working with Wasabi and Rubrik, NUSD was able to create a security solution that is not only faster and a better fit for its needs, but also saved the school district money. "We're looking at an 85% cost savings on our data backup with Rubrik and Wasabi over five years," he says. "Due to COVID-19, our district has limited funds. That made it imperative that we choose an affordable offsite cloud backup solution. It was such a relief that Rubrik could integrate seamlessly with the most affordable solution on the market – Wasabi hot cloud storage."

The backup solution has massively reduced the downtime threat of ransomware attacks. Restoring used to take days, but can now be accomplished in a matter of minutes. Automation means that NUSD doesn't have to commit valuable time to its maintenance, and Kioumars has peace of mind knowing that his systems are properly backed up and won't be suffering another ten days of downtime.

Drew Schlussel, director of product marketing at Wasabi, on the evolution of ransomware and how organisations can best protect themselves

Crypto ransomware has been a known threat for years. Why is it still such a major problem for organisations?

Because organisations are made up of people. Engineers will tell you that they build secure systems, if they're used properly. And yes, there are always bugs or defects that are exploited, but for the most part, they're exploited because somebody gets an email that says, "I need to see this report right now." And they don't know what report they're talking about. And they click, and they open the link – and game over. So unless we can completely abolish human emotion, there will always be ways for people to manipulate other people emotionally, perhaps even logically.

I'm a little bit old school – I remember [hacker] Kevin Mitnick. And the things that he pulled off, the crux of what he did, was not technology based. It was his ability to manipulate people's emotions, to have them send him information they should never have sent him.

How have the tactics of ransomware operators changed over the past several years?

Well, I think probably the biggest example is the supply chain attacks. SolarWinds and Kaseya are probably the two most obvious examples, right? You don't have to try to bash your way through the front door, or even the side door – you just find somebody who is already embedded with thousands of customers, infiltrate their supply chain, and they do the heavy lifting for you. They bring your malware into your target.

Are there any patterns that you've seen in how these groups pick their targets?

I think the most interesting thing I've seen is that the hackers are targeting insurance companies. For the reason that they want the list of companies that have cybersecurity insurance, so that when they go ahead and then attack those companies, they are keenly aware of the insurance policy and their maximum payout and so forth. And they basically tell the people, "We know you are insured, we know you can pay this ransom. Let's make this easy for everybody: go ahead and give us what we want, and we'll give you back your data." I mean, talk about account-based marketing!

Is there anything organisations can do to make themselves less attractive targets for ransomware?

Well, I mean, it's not like you can put a placard outside of your business that says that you're protected by Bitdefender, or Acronis, or any of the cyber security companies. There have been guidelines issued by the White House, there have been guidelines issued by NIST – there are very fundamental things that you can do.

Every company around the world is being probed constantly, and so if you provide just some modicum of resistance to those initial probes, they just go to the next one. It's kind of like a cat burglar walking down the street – if your doors are locked, and your windows are shut, they go to the next house. Why would they risk making noise and creating a stir? These people don't want to be detected, they don't want to be tracked down, they don't want to be patterned. They want to appear out of nowhere, act seemingly randomly, take their money and run.

Once upon a time, I worked for a company whose slogan was 'the network is the computer' – Sun Microsystems, way back. But behind that was a fundamental understanding that everything inside and outside of the corporate network was exposed, whether it's exposed to the general public or whether it's exposed to the private citizens of the corporation, and therefore, everything must be secure.

So in creating that zero-trust culture, you need to maintain a cadence of education and evaluation and reflection on how are we doing? I'm a big

> *I'm a big believer that for anything that you want to work well, you need to practice, you need to test*

believer that for anything that you want to work well, you need to practice, you need to test. You can't just wake up in the morning and go run a marathon.

What's the biggest mistake you see organisations making when configuring their backups?

I would say that there is, in many cases, kind of a blind trust that the backup has full integrity, and that when you come back to it, in a couple of days,

it will have exactly what you're looking for. And this goes for whatever media, whatever technique you're using.

I did a webinar with a gentleman from Veeam, and he told a story about a company that bought an old bank. And they thought they were geniuses, because they said, this is fantastic. It's underground. It's sealed and environmentally controlled. We can put all our tapes in there, and we will know that everything is immaculate.

And so that's what they did for months and months and months – until they actually had to go and grab a tape and do a restore. And guess what was on the tape? Nothing, because that vault was also electronically wired, and essentially created a giant magnet that was de-magnetising all the tapes that they were putting in the vault.

I think the mistake there, is that you have to be diligent about testing your backups. And for Wasabi, that's actually one of our advantages. When you're backing up with Wasabi, because we don't tap the customer for additional fees when they extract their data, they can execute tests to their heart's content, to maintain a high degree of trust that the integrity of those backups is meeting their requirements.

What advice would you have for organisations looking to limit the impact of ransomware within their IT estate?

I think they have to recognise that on-prem will be completely compromised, including their backup systems. And that's annoying, because they paid a lot of money for these very expensive, very large capacity deduplicating backup systems, because they want fast recovery. And the reality is that their best bet really is going to be in a multi-cloud approach. Putting two copies into the cloud, utilising immutable storage, protects them from themselves as well as from the ransomers. And they need to get comfortable with the fact that whatever they've defined as an RTO is going to have to be redefined, given the fact that their on-prem systems will be compromised. There's just no way around it.

Wasabi

Don't tap the customer for additional fees when they extract their data, so the client can execute tests to their heart's content