DigitalXRAID
CYBER SECURITY EXPERTS

RANSOMWARE

Stop Relying on Back-ups in the Fight Against Ransomware

ACCESS TO YOUR FILES AN
PRIVATE DATA HAS BEEN LOCKE
Enter your payment details to gain access.
$300 USD / €250 EUR
Card Number
Exp MM/YY
MAKE PAYMENT
YOUR DATA WILL BE DELETED IN:
23:12:01
ACT NOW!

With the ransomware threat increasing, it is imperative organisations understand why back-ups are no longer sufficient and recognise the need for supplementary or alternative solutions

Ransomware vs. back-ups: the story so far

Data back-ups have long been fundamental to business continuity and considered an insurance against cyberattacks. However, the progression and proliferation of cybercrime, and ransomware in particular, is rendering the back-up less efficacious and practically redundant in the face of increasingly sophisticated cyberattacks.

Although this cyber threat has been around for over four decades, it has grown exponentially in the last two years. Over 620 million ransomware attacks were detected in just 12 months, with corporate IT teams facing a 105% increase in attacks compared to the previous year.

Working from home and hybrid working practices have become the new normal. As a result of this, the number of devices and endpoints has risen substantially.

Combined with a rise in IoT devices, rapid and often unplanned acceleration to the cloud, and a lack of sufficient cybersecurity training for employees, the remote working environment has left businesses far more vulnerable to ransomware attacks.

The rise of ransomware-as-a-service (RaaS) from the likes of REvil and Conti also demonstrates the maturity of the cybercrime economy and that hackers may not even need to understand how to gain initial access to victim networks – this is done for them by separate groups which sell their services, known as Initial Access Brokers (IABs).

Cybercriminals are becoming more innovative in how they deploy ransomware.

The proliferation of supply chain attacks - from SolarWinds in 2020 to Toyota in 2022 - shows how hackers are leveraging smaller companies to use as a backdoor into the wider IT network

In 61% of ransomware attacks over the last year, attackers have used compromised access credentials to have uninterrupted access to IT environments, including back-ups. This allows them to lock up back-ups before surreptitiously removing data. This also means that organisations who rely solely on back-ups to recover from any cyberattack will need to spend weeks, or even months, in recovery mode.

What's more, 83% of successful ransomware attacks now involve alternative extortion methods – from using stolen data to extort customers, to leaking data on the dark web. With hackers now relying significantly more on data exfiltration, back-up strategies are proving unreliable for organisations looking to protect their organisation from data loss and ransom demands.

What does having your data stolen actually mean?

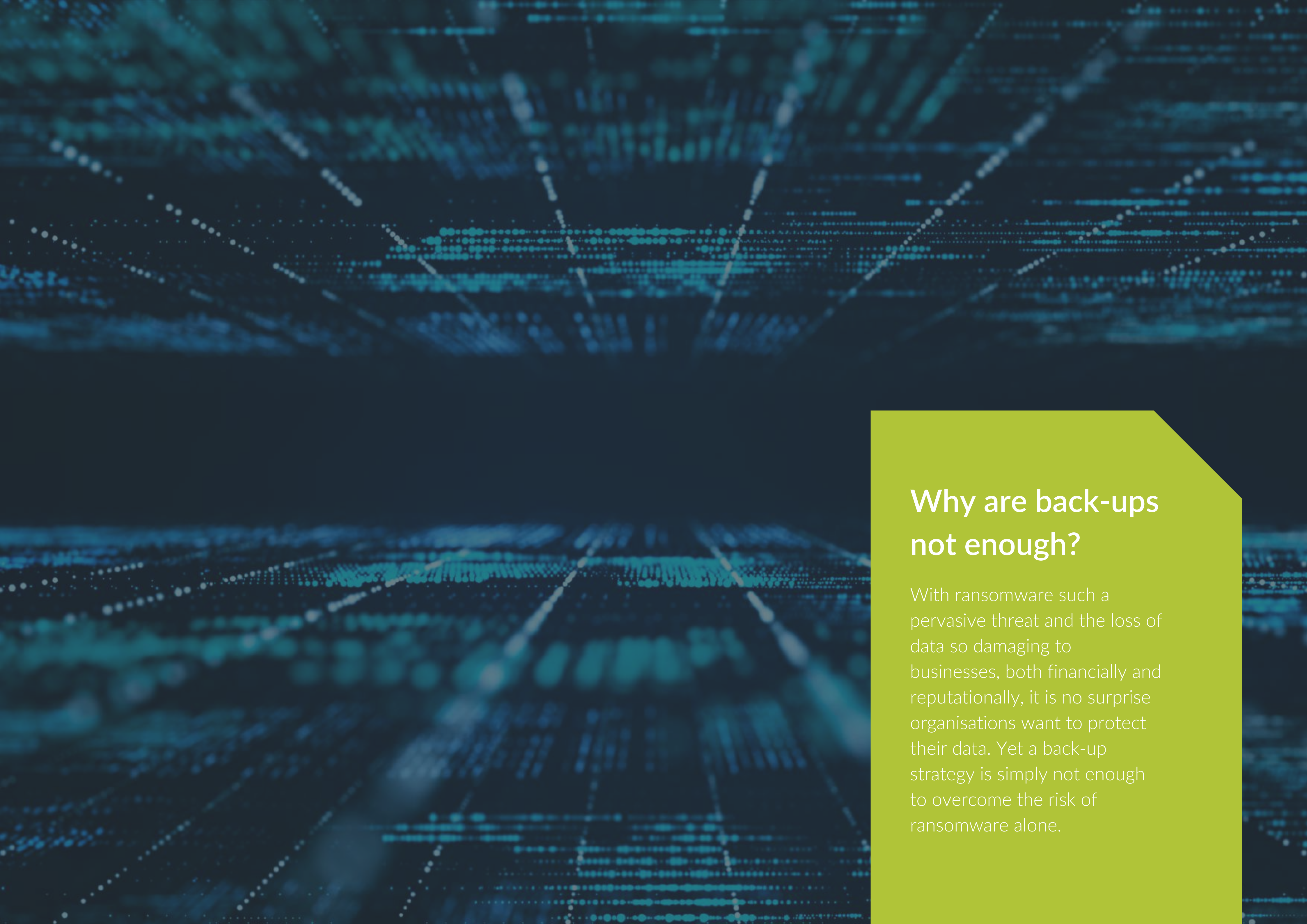
Now that ransomware is becoming an inevitable threat for any company, what does it actually mean to have your data stolen? Ransomware gangs can steal and destroy data, threaten to make sensitive information public and hold back-ups to ransom.

In the event of a ransomware attack, businesses must understand that data is compromised as soon as it is breached – even if they pay a ransom. This is why paying must stop.

Once a breach occurs, instead of paying up, it must be reported straight away based on guidance issued by the ICO, particularly personal data breaches.

Personal data is naturally more sensitive and, if posted online by cybercriminals, this will constitute a breach of GDPR, with significant fines associated.

> **“The continued willingness of victim organisations to pay ransom, combined with greater take-up of insurance policies to fund these payments, only serves to encourage more affiliate groups.**



Why are back-ups not enough?

With ransomware such a pervasive threat and the loss of data so damaging to businesses, both financially and reputationally, it is no surprise organisations want to protect their data. Yet a back-up strategy is simply not enough to overcome the risk of ransomware alone.

5 reasons you need a more holistic approach to cybersecurity

Back-ups are a continuity consideration, not a security one

Creating a set of data back-ups, or multiple sets if you follow the ‘Rule of Three’, is a key part of ensuring businesses can recover from either external or internal issues.

This may be a cyberattack, but it can also be as simple as a user error or an IT infrastructure failure that means files are lost. However, back-ups are not made to protect an organisation from being breached in the first place.

Instead, having a back-up of critical files will simply reduce the impact when a breach occurs. With so many solutions that can protect you from ransomware attacks, why would you wait for your last line of defence to keep your data safe?

Cybercriminals are becoming smarter and more sophisticated in their attacks

The criminals deploying ransomware across your network are no longer un-skilled and opportunistic amateurs.

These hackers are now often extremely sophisticated in their Tactics, Techniques and Procedures (TTPs) and will likely be choosing the organisations they target carefully.

By taking a smarter and multi-pronged approach, these cybercriminals will have penetrated a corporate network months before they deploy malware and therefore it is extremely likely they would have accessed, deleted or compromised back-ups to ensure their attack is successful.

Encryption is not the panacea

While encrypted data is harder to compromise, it is not impossible for cybercriminals to access it as long as they know what they are looking for.

What this means is hackers can access, de-crypt and re-encrypt critical data, to then hold at ransom. They may not be able to get sight of the information, but neither can you. The irony in today's threat landscape is that encryption is now often used against IT security teams, rather than being a useful cyber security tool to support them.

In fact, more than 90% of malware recorded over just 3 months was hidden in encrypted traffic.

Back-up failure rate is high

Did you know that 50% of back-ups fail? Therefore, organisations that are relying solely on the back-up data to ensure they can recover quickly from a ransomware attack will have a 50% chance that those back-ups are inaccessible or unrestorable.

This can be due to anything from a software or hardware flaw, human error following a lack of training and knowledge, or simple infrastructure issues caused by the accelerated shift to remote working and virtual environments.

Back-ups are rarely used to their best ability

Even though the majority of organisations recognise the importance of backing-up their data, and around 90% deploy a back-up strategy, only 26% back-up daily.

Therefore, while a ransomware attack may not result in all data being lost, even the compromise of just one day or one hour's worth of information could be critical for a business.

Depending on how well a back-up strategy has been followed, recovery is typically slow and arduous. Take the KP Snacks ransomware attack: the discovery team first had to identify the last clean back-ups for each system, then restore the safe files and eradicate malware from the system. This typically involves the analysis of thousands of documents and the organisation predicted two months of supply chain disruption.

While organisations may escape the financial damage of paying ransom, the time it takes to restore data will ultimately mean weeks of delayed operations and reduced revenue while teams focus on restoration rather than customer service.

What can businesses do instead?

There are various solutions businesses should be adopting to achieve a more holistic approach to cybersecurity and better protect themselves against ransomware.

At the bare minimum, understanding the inevitability of a cyberattack is an important step for organisations to take. It's no longer a case of if ransomware occurs, but when.

Once this is realised, IT leaders can be realistic about how well-equipped they are in the event of a breach and proactively look at how they can best protect their business.

Organisations could add offline back-ups as an additional step as part of a standard back-up strategy. However, this will still cause data loss and administrative overhead due to the manual process of capturing the back-up.

This is a safeguard to protect your back-up against attacks and provide a recovery point, however alternative measures should be addressed as a priority to avoid the escalating costs and resource needed.

Network separation and better architecture can help prevent cybercriminals from moving laterally across IT systems. By avoiding a flat network architecture and implementing well-defined separation policies,

NetOps teams can prevent hackers from accessing the wider IT system. This can be the difference between a breach that shuts down an entire organisation, versus just one compromised device.

A multi-pronged approach combining elements like penetration testing and staff training will mitigate external and internal security risks. Pen tests give assurance any weaknesses in a network have been identified and remedied before an attack occurs.

Concurrently, training programs that are run frequently, with phishing simulation exercises to teach employees about the latest scams, can be hugely valuable to workforce education. These two approaches help keep security front-of-mind across all levels of an organisation.

Get complete protection

To provide complete protection for an organisation, an outsourced Security Operations Centre (SOC) means early detection, 24/7/365 threat monitoring and boardroom peace of mind.

By drawing on the aggregate value of a security partner with varied knowledge of the wider threatscape, companies are better protected against cyberattacks and reclaim both time and money to invest in their core business operations.

In the context of the ongoing cyber skills gap, an outsourced SOC offers extensive expertise, protection day and night, and relieves the pressure being felt by IT teams experiencing a mass exodus of cyber skills.

While back-ups may have traditionally been seen as a solution to data breaches, they can no longer match the pace at which the threatscape is moving.

> **Criminals are becoming more organised and innovative in how they operate and target organisations. Businesses need to be addressing the unavoidable risk of ransomware proactively and adopt a holistic cyber security approach tailored to the threats of today.**

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence Against Cyber Threats? Call us now on 0800 090 3734

info@digitalxraid.com digitalxraid.com

ISO 27001 ISO 9001 CYBER ESSENTIALS CERTIFIED PLUS IASME CONSORTIUM CREST CHECK IT Health Check Service