An IDC InfoBrief • October 2020

Building business resiliency in Australia and New Zealand using a **ransomware remediation backup strategy**

Doc #AP241193IB

IDC ANALYZE THE FUTURE

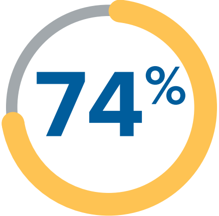
Sponsored by rubrik

A ransomware attack in A/NZ is not a matter of if, but when

According to the Office of the Australian Information Commissioner (OAIC), there has been a growing risk arising from ransomware attacks in the region. **From January to June 2020, the number of data breach notifications attributed to ransomware attacks increased by more than 150% compared to the previous six months—increasing from 13 to 33[1].** Ransomware is a strain of malicious software which encrypts the data stored on the affected system, rendering the data either unusable or inaccesible. The malicious actor behind the attack then demands a sum of money be paid for the decryption key. The decryption key may or may not be provided after the ransom is paid.

Insights from the Australian Cyber Security Centre's (ACSC) latest *Annual Cyber Threat Report* (Sept 2020) show that ransomware is now one of the most significant threats in Australia[2]. This assessment is based on the fact that ransomware requires minimal technical expertise, is low cost, and can result in significant impact to an organisation, potentially crippling core business functions. IDC specially commissioned a survey of 154 Australia and New Zealand (A/NZ) organisations for this report. Our analysis of the survey findings confirms that ransomware is a growing risk.

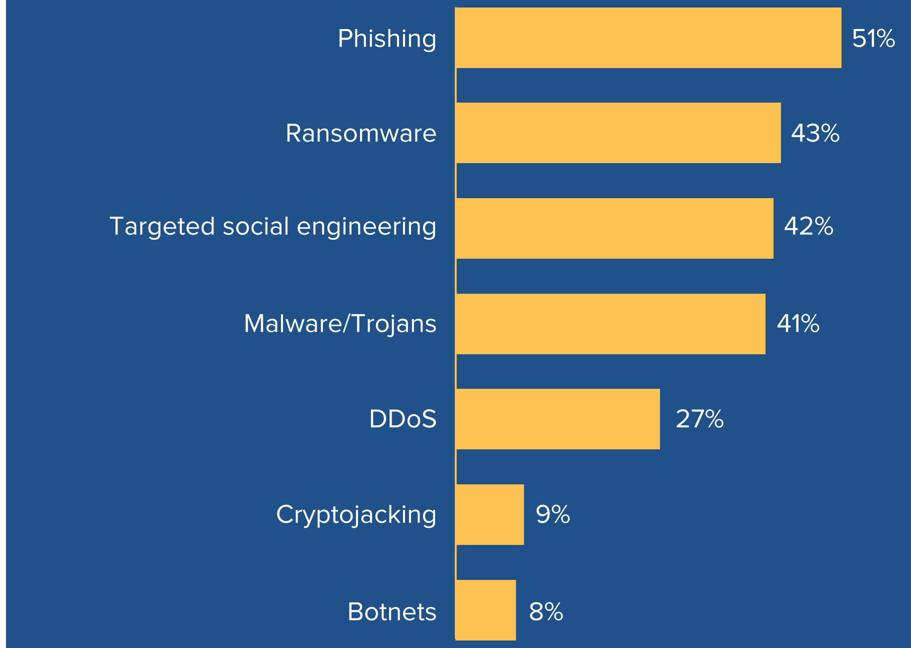
Eighty percent of A/NZ organisations surveyed agree that the volume and severity of ransomware attacks have been increasing in the last 24 months. The research indicates that ransomware attacks are increasing in frequency, second only to phishing. A ransomware attack in A/NZ is not a matter of “if”, but “when”.



of A/NZ organisations said that ransomware is becoming harder to detect and remediate. This should make organisations ask themselves: **How prepared is my organisation to remediate versus just focusing on perimeter security[3]?**

Increasing cybersecurity threats

What cybersecurity threats at your organisation have increased within the last 24 months?



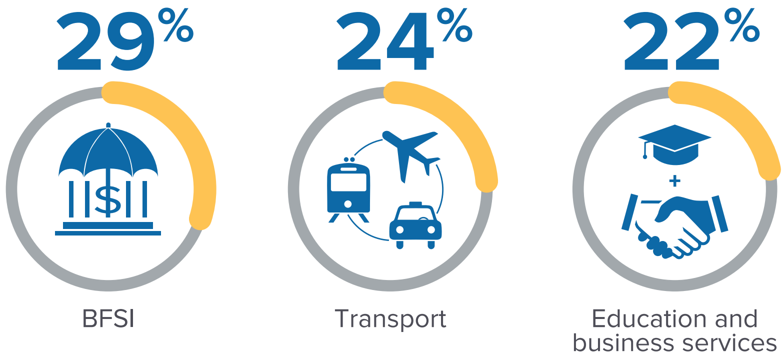
In this IDC InfoBrief, we take a look at A/NZ organisations' perspectives and experiences in recovering from ransomware attacks. We explore best practices and plans to recover or remediate from ransomware.

Sources: 1. *OAIC's Notifiable Data Breaches Report: January–June 2020*
2. *ACSC Annual Cyber Threat Report, July 2019 to June 2020, Sept 2020*
3. *IDC ANZ Ransomware Recovery Survey N=154, August 2020*

A/NZ organisations face the rising threat of ransomware

In terms of actual attacks, the survey revealed that **18%** of A/NZ organisations had experienced ransomware attacks in the last 24 months. Large enterprises with 1000+ employees were most affected, with percentages being much higher in the banking, financial, and insurance (BFSI), and transportation sectors.

Top industries impacted by ransomware in the last 24 months



With the COVID-19 pandemic, the ACSC also cited increasing ransomware campaigns targeting the healthcare sector[4]. About 10% of government respondents reported attacks. While lower than in other sectors, this is an alarming trend, considering the sensitive nature of the targeted information.

Of greater concern, of those organisations that experienced attacks, **almost one in three (29%) respondents paid the attackers.**

The ACSC strongly advises against paying ransomware demands as this only fuels the criminal activity; there is no guarantee that adversaries will provide decryption keys.

In a separate IDC study of 700 European enterprises[6], the top security concern in European enterprises was ransomware, which topped malware for the first time.

Recent reported attacks

Australian logistics company, Toll. The company was forced to disable its digital systems and use manual processes after a ransomware attack earlier this year, causing delays throughout the country. And, despite their best efforts, they took a couple of months to recover[5].

Trans-Tasman brewer, Lion. Lion has fallen victim to ransomware attacks in recent months, with hackers threatening to "auction“ off Lion's confidential documents, unless the company paid a million-dollar ransom[5].

Sources: 4. Cyber.gov.au
5. ia.acs.org.au and stuff.co.nz articles
6. IDC's European Security Strategies Survey 2019

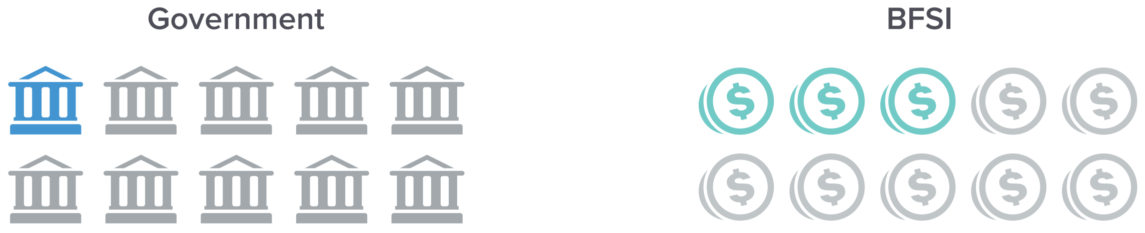
A spotlight on government and BFSI

BFSI and Government are among the largest sectors in A/NZ. Here are some noteworthy research findings from the two sectors.

Research findings

	Government	BFSI
of respondents agree that the volume and severity of ransomware attacks had increased in the past 24 months	80%	82%
of respondents agree that ransomware attacks were becoming harder to detect and remediate	67%	71%
of respondents agree that remediation and recovery following a ransomware attack was an important issue for their organisation	93%	100%
of respondents agree that remediation and recovery from a ransomware attack was just as important/critical as prevention	83%	83%

Organisations that have experienced a ransomware attack in the past 24 months



One out of 10 government organisations surveyed experienced a ransomware attack in the last 24 months. Of that, **33%** paid the attackers.

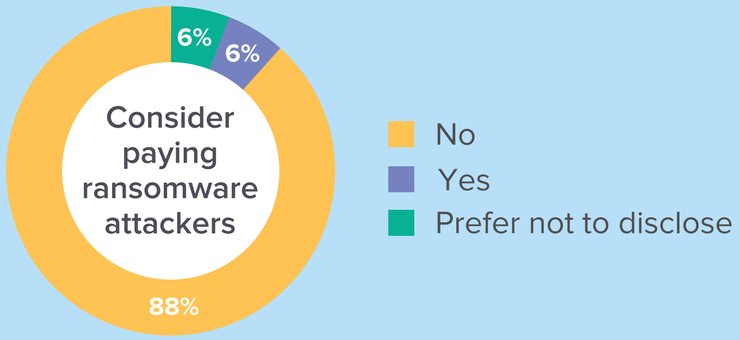
Three out of 10 BFSI organisations surveyed experienced a ransomware attack in the last 24 months. Of that, **60%** paid the attackers.

The hardest part of recovering from a ransomware attack, according to respondents:

	#1	#2	#3
Government	Reliability of data recovery	Speed of data recovery	Assessing the damage
BFSI	Speed of data recovery	Reliability of data recovery	Detection

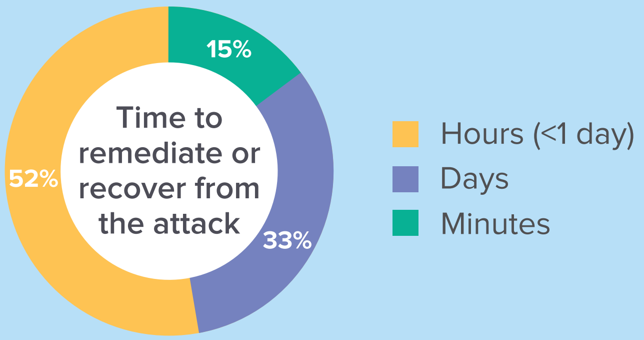
Reality bites, when it comes to ransomware attacks in A/NZ

Ransomware is a top concern, now and in the future, and will continue to be one, no thanks to cyber criminals' increasing sophistication and access to technology. The evidence is mounting that cyber crime is on the rise in A/NZ, despite organisations' best efforts at preventing access to critical resources. IDC data supports this, as 89% of A/NZ businesses said ransomware remediation was just as critical as prevention in an effective response strategy. The *ACSC Annual Cyber Threat Report* reiterates this–it mentions that recovering from ransomware is almost impossible without comprehensive backups.



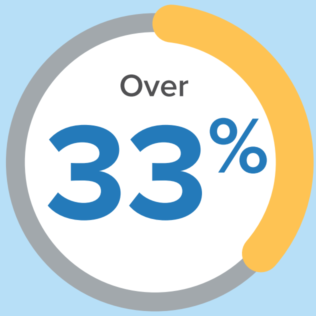
To pay or not to pay: that is the question

- When we asked A/NZ organisations whether they would consider paying ransomware attackers, **88% said a resounding NO[1].** This sentiment is aligned with the official Australian and New Zealand government advisory that recommends non-payment for these attacks as there is no guarantee of resolution[2].
- Unfortunately, when subjected to actual ransomware attacks, it is a much lower number (67%) that did not pay. **A third of A/NZ organisations paid the ransom.** This tells us that the reality of an attack can put additional pressure on the organisation, especially if private information could potentially be released online. This indicates that many organisations might not be ready to execute on their remediation plan, when it comes to a ransomware event.



Prolonged remediation time

- **96% of respondents agree that ransomware remediation is critical.** In reality, though, many remediation plans and responses might not be as good as organisations perceive, as mentioned in the column on the left.
- While respondents prefer attacks to be remediated in a matter of minutes, **the reality is that the majority experienced many hours and even days of remediation time.** In a highly publicised ransomware event this year, Toll Australia took a couple of months to recover despite best efforts[3].
- **Ransomware breaches that take longer to remediate cause significant business disruptions and impact productivity and output.** The stakes are higher in some sectors, such as the heath sector, where the exposure of private electronic health records would set off a public relations nightmare, because it could cause potentially irreparable damage to a company's reputation.



of respondents said backup data had been impacted by ransomware, prior to detection

Gaps in backup capabilities

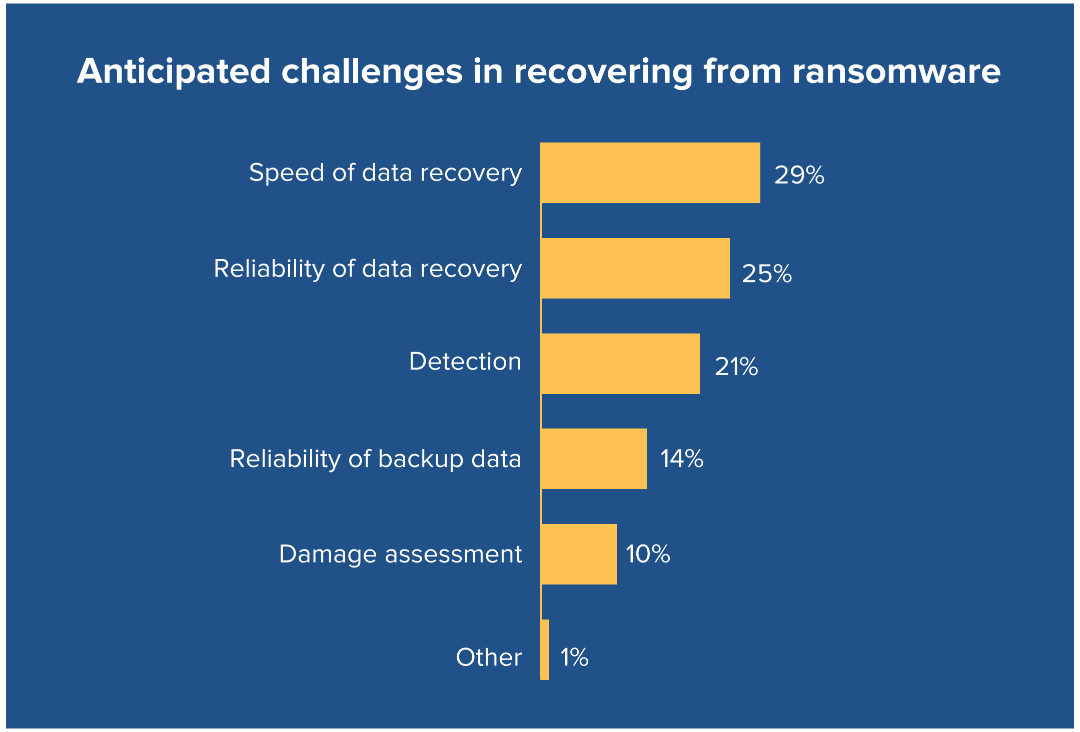
- **A third of organisations that experienced attacks revealed that their backup data had been impacted prior to detection of the ransomware.** This finding has raised concerns that A/NZ organisations could be facing the risk of not being aware of gaps in their backup capabilities or are over-confident in their ability to recover data.
- An attack's impact on backup data complicates the recovery process as many A/NZ organisations rely on online real-time data sources as well as multiple data sources. This further emphasises the need for an enterprise-wide backup remediation plan.
- **IDC research shows that "data security" and "privacy" are now ranked top investment priorities[4].** A current review of backup capabilities is a key part of a cybersecurity audit or assessment process.

Sources: 1. IDC ANZ Ransomware Recovery Survey N=154, August 2020
2. Cyber.gov.au
3. AFR article
4 IDC's IT Services Survey, May 2020

Challenges to achieving a speedy recovery

Our research shows that 63% of A/NZ organisations are confident in their ability to recover or remediate from ransomware attacks*. But, the reality is that **one-third** had their backup data affected prior to the ransomware attack being detected and **29%** of the respondents are still concerned with the speed of data recovery.

Furthermore, ensuring reliability of data sources after recovery will likely be a major concern for many A/NZ organisations. Many A/NZ enterprises rely on multiple disparate but yet connected databases. Recovering these distributed data sources will likely take time with no guarantee that the process will yield reliable data, if the data is compromised, corrupted, or out of date.


Anticipated challenges in recovering from ransomware

Speed of recovery has a tremendous impact on business continuity in today's environment. Many A/NZ organisations will likely take hours, days, or even months to fully recover. Toll (see p3), for example, took from late January until early March 2020 to recover. Within this period, it was unable to inform its customers where their parcels were, resulting in loss of business and reputation. Soon after recovery, though, the company was hit again by a different ransomware in early May 2020.

**8 or higher rating, out of a 1-10 confidence rating scale*

Sources: 1. IDC ANZ Ransomware Recovery Survey N=154, August 2020

Backup features used in ransomware recovery

Point-in-time recovery, which has long been in practice, is the most common feature cited in respondents' backup solutions and rightly so, given it has the people, process, and technologies to support it.

Instant recovery has risen significantly over the years, as solutions have matured with storage and cloud technologies to offer the best in recovery times. Some instant recovery configurations, however, are risky, as attackers' access to network or cloud resources may compromise backups.

Two-thirds of our respondents utilise **policy-based management within enterprise backup solutions** because they allow for fine-grained control and abstraction over multiple applications, databases, and architectures. Looking at the results in this figure, there is already significant risk of a prolonged recovery process if attackers can access backup data.

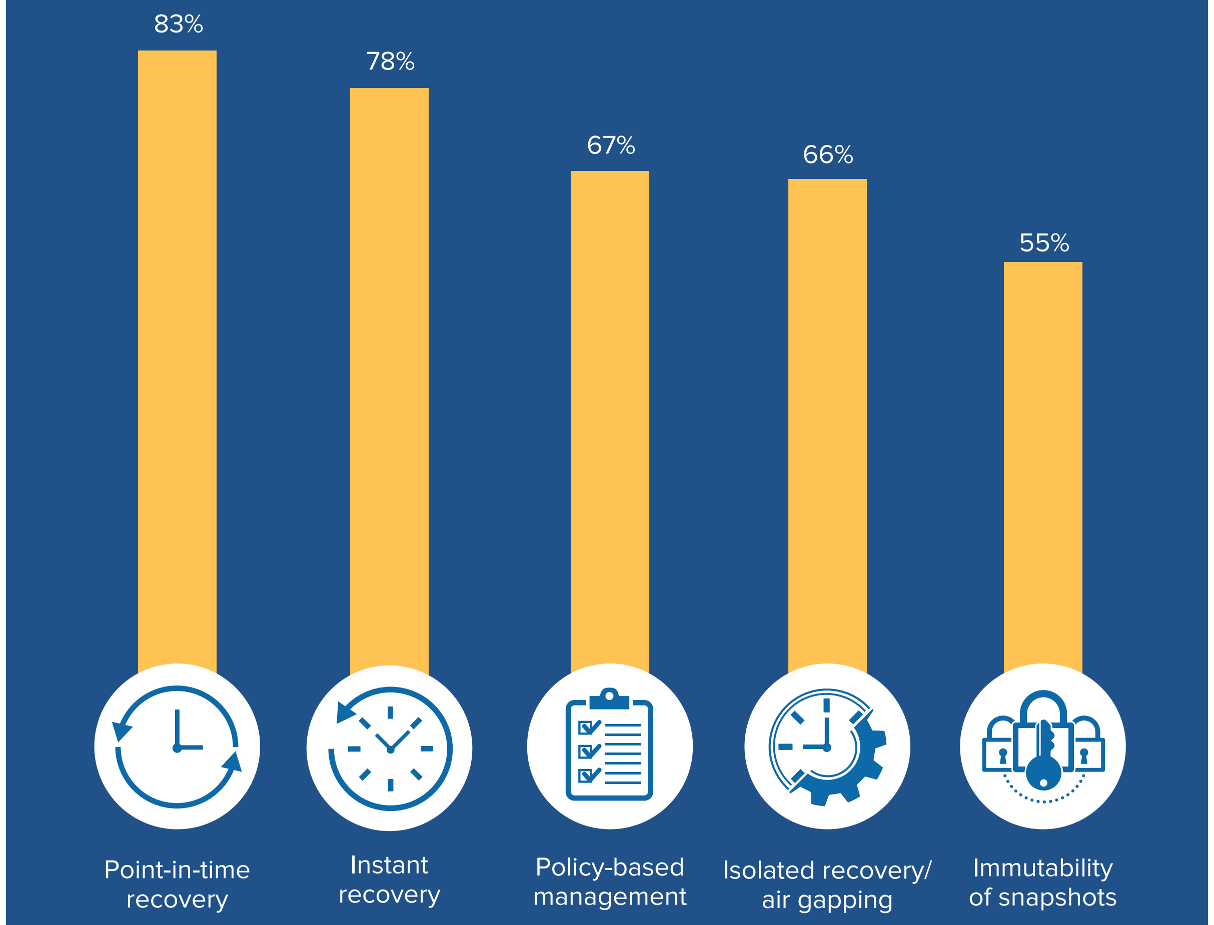
Air-gapping or isolated recovery has also been implemented by two-thirds of respondents.

Immutability of snapshots comes in at the bottom of the pile (55%). This is a concerning finding, given the importance of immutability in enabling organisations to follow the ACSC Data Backup and Restoration guidance, which recommends that organisations protect their backups from unauthorised modification, corruption, and deletion. Immutability offers this level of protection in the worst-case scenario of an attack and unauthorised access to network resources.

At this point, it is important to know that backup solutions differ in how they 'implement' immutability. Some questions organisations should ask themselves are: Is it an added feature? Has it been configured properly? Is it native to the solution and, hence, requires no added burden of management risk?

Backup solution features

Which of the following features does your backup solution utilise?



Source: IDC ANZ Ransomware Recovery Survey, August 2020

Conclusion

Ransomware is here to stay

2020 will be marked as the year ransomware became one of the biggest threats in Australia[1]. By combining new and critical vulnerabilities with social-engineered spear phishing, attackers can gain access to critical IT and network resources, which they are using as a launchpad to deliver ransomware payloads. It requires minimal technical expertise, is low cost, and can result in significant impact to an organisation, potentially crippling core business functions, according to the ACSC. Organisations must be better prepared with a ransomware-ready remediation backup strategy.

Lasting business impact and reputational damage

This study has exposed the assumption that enterprises have overestimated their ability to recover from a ransomware attack. **Very few respondents believe that they will be able to recover in minutes (15%).** We have seen how this expectation has not been met, with business and reputational damage to the brand. A ransomware attack may scuttle a business for good, especially during the deep recession that Australia and New Zealand are in now. Shifting more activity online and increasing remote access will only exacerbate organisations' concerns over the ability to recover from a ransomware attack. Of great concern is the fact that one in three enterprises have paid a ransom, even though there is no assurance that the encryption keys will be handed over.

Confidence in backup efficacy may be misplaced

Most organisations readily say they have strategies in place with a variety of backup features in their solutions. These features alone, however, do not guarantee readily accessible backups in the case of a ransomware attack. While online and connected backup solutions may offer faster recovery speeds, the ACSC again recommends that organisations protect their backups from unauthorised modification, corruption, and deletion. **Assuring backup solutions are not prone to misconfigurations, policy gaps, and network and data access rights have been secured is imperative.** Immutability is a feature that meets ACSC Data Backup and Restoration guidance. Ensure that it is always on by default, can't be switched off and is native to its file system.

Source: 1. OAIC's Notifiable Data Breaches Report: January–June 2020

Essential guidance

Organisations in Australia and New Zealand should consider the following guidance when putting together a backup remediation plan from ransomware:

Audit and assessment for readiness

- It's not a matter of if, but when your organisation may be locked out of its own data. With advanced persistent threats and targeted spear phishing on the rise, it's no wonder that Australian businesses saw an increase of data breaches in the first half of 2020 compared to the same period last year. Most breaches have been linked to secondary data stores and email records, but there is too much at stake to risk your organisation's primary data sources due to the lack of an incomplete backup and remediation strategy.

- Recovering from ransomware is almost impossible without comprehensive backups, according to the *ACSC Annual Cyber Threat Report*. Start by assessing your organisation's current state of backup and recovery effectiveness, when it comes to ransomware remediation.

- When under attack, have a clearly defined recovery plan that addresses not only the actual process but also the responsibilities of different stakeholders in the organisation. This will minimise the risk of a prolonged recovery, which may result in the loss of business and reputation.

Build and test an incident response plan

- Data is at the heart of a ransomware attack. Having an incident response plan is necessary, and part of it must address data integrity. IDC recommends that organisations take steps to comply with the ACSC's Data Backup and Restoration guidance of which immutability is a key element.

- Ensure that backups can be restored; this should be tested from time to time, especially when architectures, technologies, and applications change. This enables instant real-time operating systems (RTOs) and policies to be tested and audited for compliance, if necessary.

- A response plan should include a communication and public relations response plan that complies with regulatory requirements (for example to address data breach notification mandates). The right communications strategy will limit any damage done to an organisation's reputation, in the event of a ransomware attack.

- Ransomware and other types of attacks are becoming increasingly sophisticated. Periodic and regular updates, and testing of the recovery playbook is essential to ensure preparedness and confidence in execution.

Case study

Lang’s Building Supplies stops ransomware attack due to next-gen backup solution

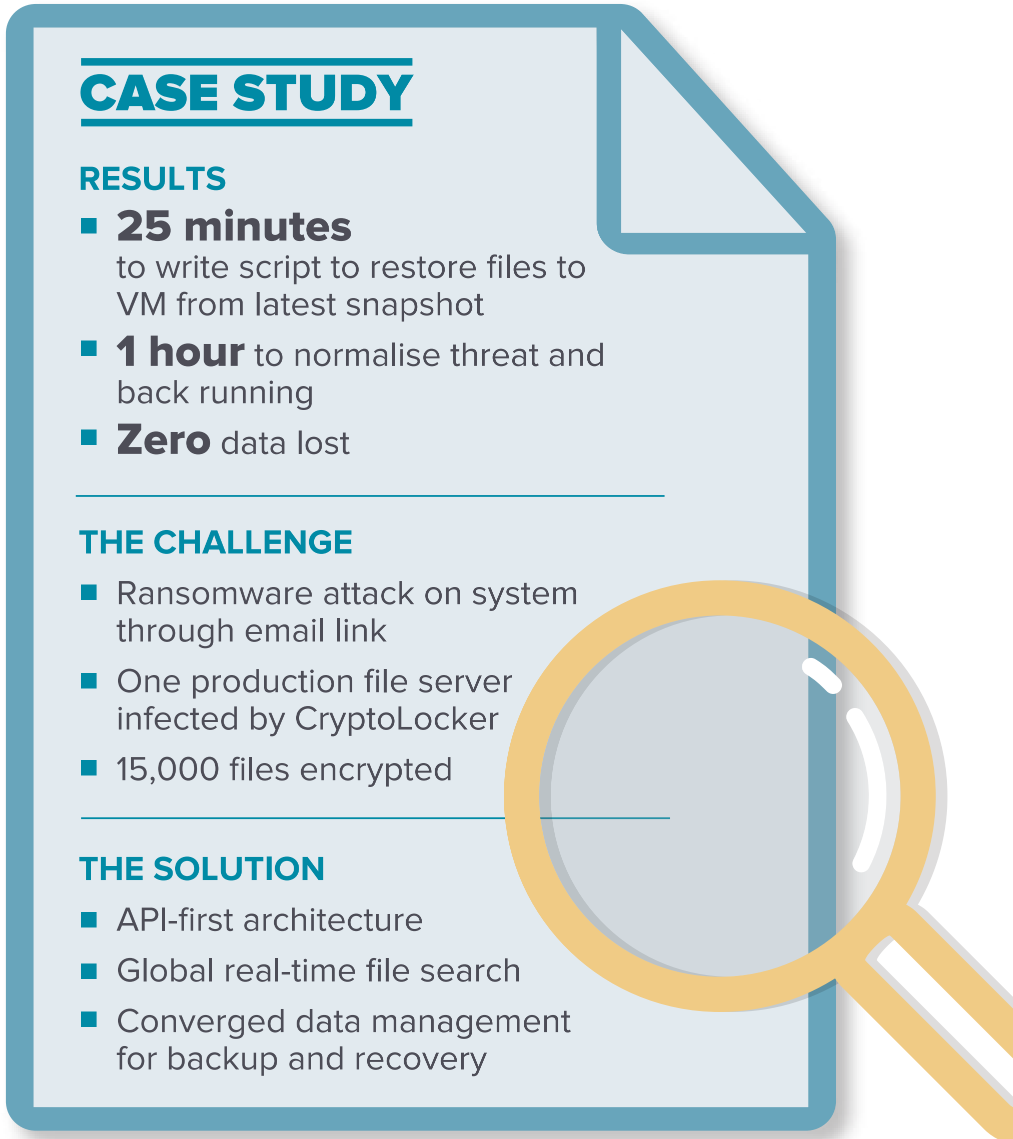
> *“We were able to write a script to restore files back to the VM from the latest version of the file because of our backup. We had all of our files back to the file server in approximately one hour. No damage done. Having a top-notch data management solution in place means I can go about my day-to-day job without worrying about data loss. I know I have it covered.”*
>
> *Matthew Day,*
> *ICT and Support Manager,*
> *Langs.*

Langs Building Supplies, a leading manufacturer and supplier of products for the construction industry based in Stapylton, Queensland, Australia, was recently hit by a ransomware attack.

In early June 2020, one production file server at Langs Building Supplies was infected by the CryptoLocker ransomware through an email link. The IT team was alerted within 10 minutes of the attack through monitoring tools that tracked high change rates in data structures. As a result, only 15,000 files out of millions were renamed as .encrypted, a file extension that prevents those files from being accessed without a passcode from the attacker.

After receiving an alert from the monitoring system, Matthew Day, ICT and Support Manager at Langs, was able to isolate the affected VDI desktop and prevent the attack from spreading to the rest of the firm’s infrastructure.

Due to its effective backup infrastructure, the company was able to thwart the threat and restore its data without paying a ransom. The company relied on Rubrik's instant recovery and API-first architecture to stop the ransomware attack. With Rubrik, they recovered ransomed files and resumed business in less than an hour.



CASE STUDY

RESULTS

- **25 minutes** to write script to restore files to VM from latest snapshot
- **1 hour** to normalise threat and back running
- **Zero** data lost

THE CHALLENGE

- Ransomware attack on system through email link
- One production file server infected by CryptoLocker
- 15,000 files encrypted

THE SOLUTION

- API-first architecture
- Global real-time file search
- Converged data management for backup and recovery

This IDC InfoBrief was produced by IDC Custom Solutions. Copyright 2020 IDC. Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC.

For more information, visit: www.ap.idc.asia or email: gmsap@idc.com

Source: Rubrik