computing research

RESEARCH PAPER

Belt and braces: Is your ransomware recovery plan good enough?

May 2020

Sponsored by

CONTENTS

- Introduction **p3**
- Key findings **p3**
- Ransomware in the threat landscape **p4**
- The reality of ransomware **p5**
- Remediation and recovery **p6**
- Backup plan **p8**
- Conclusion **p10**
- About the sponsor, Rubrik **p11**

Introduction

Most business processes today are digital. So, when an organisation is hit with ransomware, the damage to productivity, privacy, and reputation can be massive. This is because many organisations have taken their eye off the recovery component and instead solely focused on prevention. Backup solutions reduce risk of paying ransoms – but not if they can be compromised in the same way as other IT infrastructure. It is therefore vital to take a belt and braces approach to securing your organisation. Prevention still matters, but remediation and recovery plans must be underpinned by solutions up to the job of minimising data loss and productivity damage.

Computing surveyed 150 decision makers representing organisations from a wide variety of industries including banking and finance, logistics, manufacturing, retail and education to establish the ransomware threats facing organisations, how businesses are reducing the risks, cleaning up after attacks, and how long it is taking them to do so. It will explore the confidence businesses have in their ransomware recovery plans, and in both the reliability and speed of their backup and recovery. Finally, it will discuss the importance of features such as an immutable file system and instant recovery in reducing the risks businesses face from ransomware.

Key findings

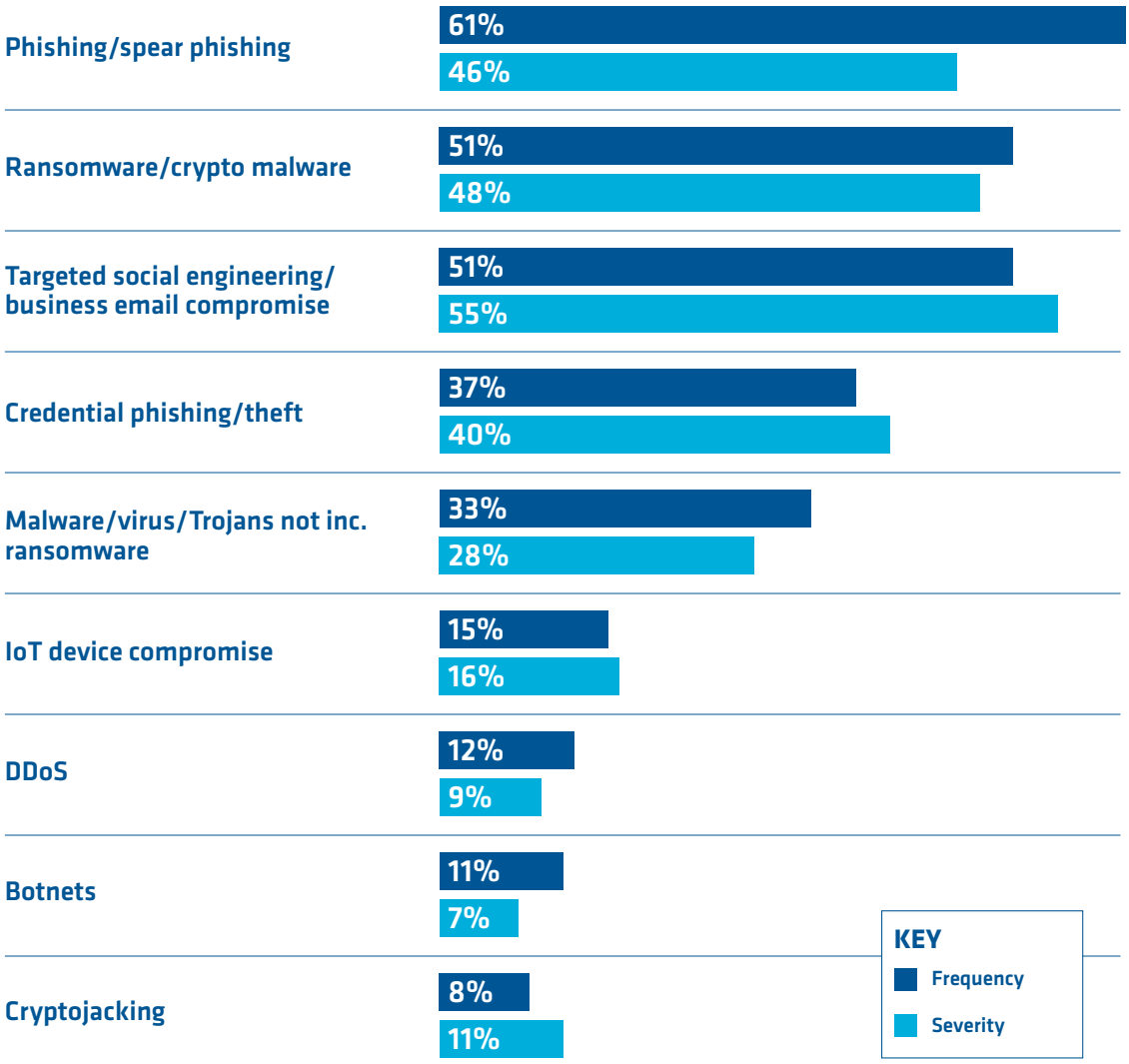
- Fifty-seven percent agree that both the volume and severity of ransomware attacks were increasing and 32 percent said the nature of the attacks are making them harder to detect and remediate.
- Twenty-six percent said that their organisations had experienced a ransomware attack within the last two years.
- Twenty-eight percent of respondents had at some point, paid off those behind a ransomware attack.
- When asked if they would consider paying a ransom in a hypothetical attack only 59 percent gave a definite “no.”
- Eighty-four percent agreed to at least some degree that ransomware remediation is just as critical as prevention in an effective response strategy.
- Thirty percent of those who had experienced a ransomware attack said that it took days to recover.
- In 23 percent of cases, backup data was affected prior to the ransomware attack being identified.
- Speed of data recovery is the biggest concern for respondents when assessing their organisation's ability to recover from a ransomware attack, and damage assessment second.
- Respondents were nonetheless confident about the level of ransomware protection that their backups afforded them.

Ransomware in the threat landscape

When discussing ransomware – and how best to mitigate and recover from it – it is worth first taking a wider view of the threat landscape itself and ransomware's place within it. Organisations are used to the frequency and volumes of cyber security threats ebbing and flowing but those behind the threats are becoming increasingly ruthless. A criminal ecosystem, organised and collaborative, share stolen data, hacking tools and criminal expertise.

Not to mention, the increase in remote work with the most recent pandemic. Whilst levels of remote working have been increasing for years, it is usually combined with office working to some degree. Few spent their whole working week at home. Now huge amounts of people are still getting to grips with the new normal and figuring out how to remain economically productive, and secure, from inside the home.

Fig. 1 : Pick up to three types of threat you believe are increasing the most in terms of frequency and, secondly, severity



Computing asked respondents to our exclusive survey what they thought the main threats facing their organisations were – in terms of volume and severity. Figure 1 illustrates their answers, and the consensus around the prevalence of certain threats. The most likely threat in terms of frequency is considered to be phishing. These responses reflect the fact that newly minted home workers are more likely to be distracted and easier prey for phishing lures than they would be in the office – and security firms from all over the world are reporting an associated increase in activity to exploit it. In joint second place is ransomware/crypto malware and targeted social engineering/business email compromise, but it's quite likely that in reality these attacks may be blended.

In terms of severity, the most feared attack is targeted social engineering/business email compromise, but ransomware moves up to second place. There are good reasons for this concern. Our respondents had no doubts about the severity of risks from ransomware. Fifty-seven percent agree that both the volume and severity of this type of attack were increasing and 32 percent said that the volume of attacks is decreasing, but the nature of the attacks are making them harder to detect and remediate.

The reality of ransomware

What is the likelihood of falling victim to a ransomware attack? Certainly, a perception exists that some sectors are more at risk than others. US local governments have had a particularly bad time of it, and there have been recent attacks on local government in the UK.[1] However, despite the publicity that public sector attacks receive, business still constitutes the majority of ransomware victims.

There is also a perception that SMBs are more likely to be targeted. The logic behind this is that these businesses are less likely to have mitigation and recovery strategies in place and are consequently more likely to quietly pay the ransom – although this is no guarantee of the unlocking of compromised data. However, data published in Q3 2019 showed the average size of compromised organisations at 645 employees,[2] and the largest proportion of respondents to this particular survey (32 percent) fell into this category. Overall, a little over one quarter (26 percent) of those responding to our survey said that their organisations had experienced a ransomware attack within the last two years.

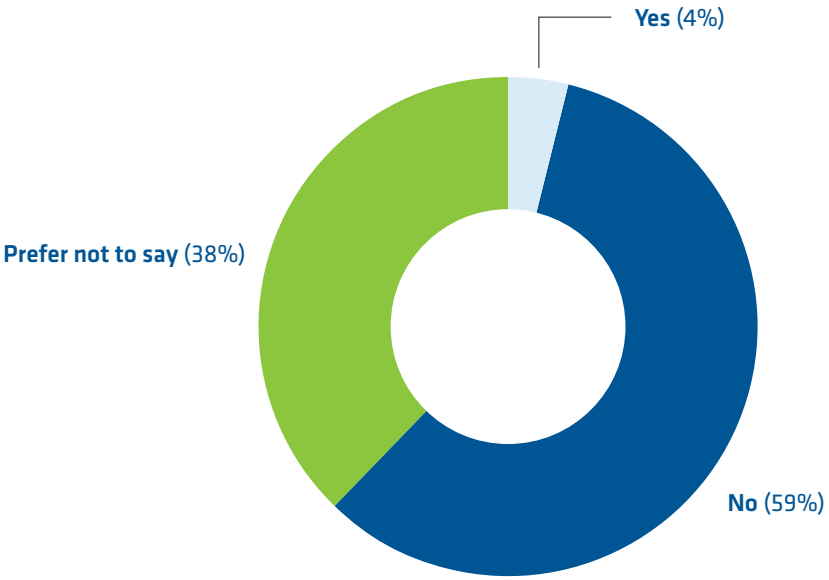
The ongoing and apparently increasing frequency of ransomware attacks is influenced in part by the likelihood that victims will pay up in the event of compromise. Official guidance given to businesses in most countries is that paying up should be avoided. However, some hacking groups are pivoting on their extortion tactics, beginning to steal data and hold it to ransom with a view to publishing it rather than encrypting it. Groups like Maze are very public about their activity, publishing lists online of the companies and organisations they have compromised. If victims fail to pay up by a given date, the group publish a small amount of stolen data online and if payment is still not received, they continue to drop increasing quantities of data into the public realm. A number of large organisations, both public and private have been compromised in this manner.[3]

[1] https://www.theguardian.com/technology/2020/feb/27/redcar-and-cleveland-council-hit-by-cyber-attack

[2] https://www.coveware.com/blog/q3-ransomware-marketplace-report

[3] https://cointelegraph.com/news/maze-hacker-group-claims-infecting-insurance-giant-chubb-with-ransomware

Fig. 2 : Would your organisation consider paying off a ransomware attacker?



Twenty-eight percent of those responding to our survey had, at some point, paid off those behind a ransomware attack. Seventy percent had not. This compares favourably (depending on your point of view) with other research conducted which has found pay rates of nearer 40 percent.[4]

That proportion is discernible in responses to a question *Computing* asked about whether or not organisations would consider paying off an attacker – not whether they already had. A startlingly honest four percent admitted that they would consider paying but 38 percent preferred not to say rather than give a straightforward "no." This indicates that in the event of an attack, non-payment was not a forgone conclusion. For many organisations, it clearly is not an easy decision.

Remediation and recovery

The reason that so many organisations would at least consider the possibility of paying a ransom in the event of an attack, is the varying ability of organisations to remediate and recover from such an attack. For some organisations, paying for the return of their data is by far the least expensive option. One attack last year cost the victim £45 million and the organisation affected has chosen to go public with the attack as well as complying with legal requirements to report it.[5]

It is clear that ransomware is collectively causing huge amounts of disruption and downtime when defences are breached. This is why cyber security strategies have evolved in recent years to encompass the widespread acceptance of the idea that even with strong defences in place security breaches are inevitable to some extent. After all, a cyber criminal only has to be successful once. *Computing* asked participants in our research to what extent they agreed with the following

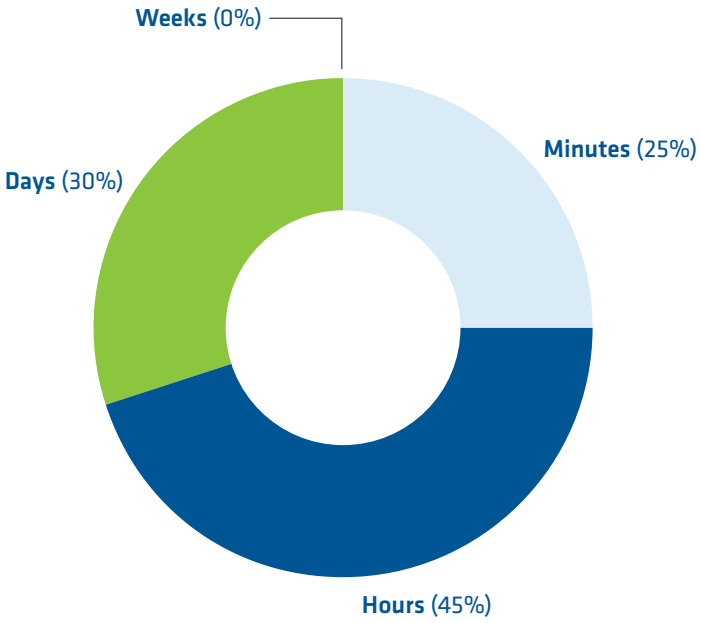
[4] https://www.itproportal.com/news/uk-organisations-paying-hacking-ransoms-increases-by-100-per-cent/

[5] https://www.bbc.co.uk/news/business-48661152

statement. **"Ransomware remediation is just as critical as prevention in an effective response strategy."** Eighty-four percent of respondents agreed either somewhat or strongly. Only five percent disagreed, with the remainder neutral.

Given this consensus, we would expect to see widespread cyber incident response plans in place across businesses – plans that are tested regularly and can scale. However, the reality on the ground is a little patchier, as Figure 3 below illustrates.

Fig. 3 : How long did it take to remediate the attack?



When we asked the respondents who had been subject to a ransomware attack, how long it took them to remediate it, the answers were mixed. For 30 percent it took days. Those days would have involved a great deal of time and resource expended in clean up and restoration of the affected data. Not to mention the lost productivity and frustrated customers.

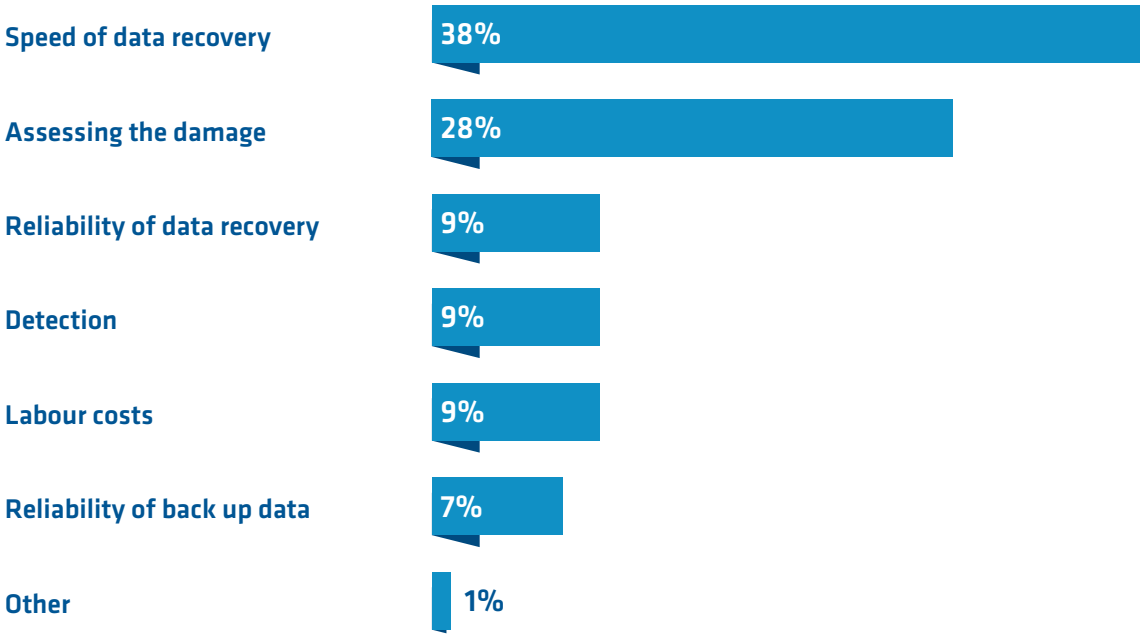
Therefore, backup should be a crucial part of cyber incident planning. Ransomware attacks are designed to spread through networks, and, in many cases, backups will be part of that network. Speed of data restoration is also critical. If it takes days to go through backups to find clean copies of the affected data, the cost of the attack begins to mount significantly.

We asked our respondents who had experienced a ransomware attack if the attack was identified before or after backup data was affected. In 23 percent of cases the answer was no. These organisations are likely to be the same ones who took longer to remediate their attack with all of the cost that this entailed.

Backup plan

Our research suggests that many organisations are having to work hard to ensure that the focus on detection and mitigation does not leave them open to much bigger risks than a strategy more focused on prevention. Figure 4 shows the stages of the detection, remediation and recovery process that those participating in our survey consider more likely to be troublesome. The biggest concern by far was the speed of data recovery. Visibility was also a standout concern. Assessing the damage to applications and data was the second highest scoring issue.

Fig. 4 : What is/would be the hardest part of recovering from a ransomware attack at your organisation?



Computing also asked respondents how confident they were in the level of ransomware protection their backups afforded them. Those surveyed were asked to rate their confidence on a level of one to ten, with one being the least confident and ten the most. The majority of respondents clustered around the seven and eight mark which could be described as reasonably confident.

These findings indicate that, whilst organisations are fairly confident about the reliability of their backups, this confidence doesn't extend to the speed of recovery – which, if the goal is to minimise business disruption in the event of a ransomware attack, is not a reassuring finding.

Our research also revealed that the faith respondents had in the reliability of their backups may not always be completely justified. When we asked whether they were aware of the immutability and security principles of their backup solutions, fewer than half said yes. In fact, 51 percent said they were not aware of these features and a further 4 percent said that their solutions did not offer such features or principles. Why does this matter? If backup data is not immutable it can

be modified – deleted or encrypted by ransomware. No backup architecture should ever have the ability to modify previous backups. These previous backups should only be available in a read-only format.

Fig. 5 : Which of the following features does your backup solution utilise?

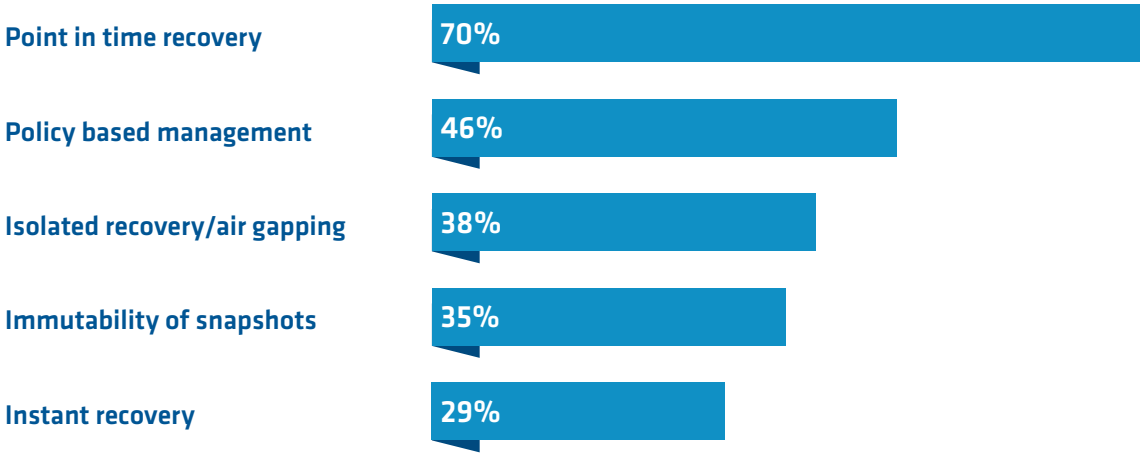


Figure 5 shows a list of features of backup solutions and proportions of our respondents who have such features in place. At 35 percent, immutability of snapshots is one of the least common attributes of backup solutions, despite it being critical for reliability. Even where vendors claim immutability, prospective customers should do their research to ensure it is truly an immutable file system. The most widespread feature was point-in-time recovery. The only surprising aspect of this finding was that the number wasn't higher because the ability to restore data from the point just before an unforeseen event occurs is a fairly core component of a backup solution.

Fewer than half of respondents enjoyed policy-based management as part of their solution. Non policy-based solutions are significantly more labour intensive than their policy-based counterparts because each specific backup instruction has to be individually configured. A policy-based management simply allows administrators to input a data protection policy and the policy engine does the rest. The simpler the solution the less the scope for issues – and the time expended in finding out where those issues have occurred. This makes policy-based solutions more reliable.

Isolated recovery/air gapping is an interesting one. In theory it should provide complete reliability (provided you don't have an undetected ransomware attack when a scheduled update occurs and the gap is open) but the speed of restore for isolated recovery is likely to be considerably slower, including all of the cost and complexity involved in running a separate backup infrastructure. It is notable that instant recovery is the least widespread feature – which probably explains why respondents were concerned about speed of recovery overall.

Conclusion

It feels like an understatement to say that 2020 is shaping up to be a particularly challenging year – both in general and cyber security terms. Remote workers who are now home based for the foreseeable future are being relentlessly targeted by cyber criminals.

These malicious actors are exploiting remote workers' need to feel connected with their employers. Phishing lures and exploiting all of these desires are being reported in great numbers as are more targeted business email compromise attacks – and greater volumes of ransomware. Fifty-seven percent agree that both the volume and severity of this type of attack were increasing, and approximately one third of respondents said that the nature of the attacks were making them harder to detect and mitigate.

A little over one quarter of those we surveyed had experienced a ransomware attack within the last two years and 28 percent had, at some point, paid off those behind a ransomware attack. Seventy percent had not. When asked about the principles of whether they would consider paying out, only four percent admitted they would do so but a further 38 percent preferred not to say rather than give a straightforward "no." This indicates that for many businesses hit with attacks, traditional moral certainties about the inherent wrongness of paying a ransom are likely to give way under pressure from the considerable costs of lost data and reputational damage.

This is why 84 percent of respondents agreed to one extent or another that ransomware remediation is just as critical as prevention in an effective response strategy. However, when it came to the reality of remediation on the ground, the response was patchy, with 30 percent taking days to remediate. In 23 percent of cases of those who has experienced an attack, the attack spread to their backup data before it was identified.

For our respondents, the hardest part of recovering from a ransomware attack was the speed of data recovery. The process of assessing the damage was viewed as the second most likely area of difficulty. Nonetheless, respondents are fairly confident about the level of ransomware protection that their backups confer.

Further questioning on the features of backup solutions shows that in some cases this confidence may not be completely justified. Only 35 percent of respondents believed their solutions had immutability – meaning that the remaining 65 percent run the risk of being overwritten by attackers. Policy-based management is another crucial aspect of the level of protection from ransomware that backup can confer, because older, more configuration heavy solutions are more labour intensive and error prone – and less reliable as a consequence.

Respondents were less confident about the speed of data recovery than the reliability of their backups. Only 29 percent of our respondents had an instant recovery solution in place which enables them to instantly identify files and data affected by an attack and restore clean versions quickly. Not having a solution like this in place means that even if your back up is reliable, it takes a considerable length of time to access and rehydrate the relevant data – and that's once you've actually established what data has been affected, which was the second most likely area of remediation likely to prove difficult.

There is a consensus that remediation is as important as prevention in risk reduction strategy. Yet the reality of what existing remediation solutions can provide is, at best, mixed.

In order to optimise remediation and recovery strategies and reduce risk, organisations should consider their backup as part of a data management platform which provides multi-level defence against ransomware, consisting of automated anomaly detection, threat impact analysis and truly immutable instant recovery. By taking this approach, businesses will have a detection and mitigation strategy they can feel justifiably confident of. This is an approach that accepts the reality of ransomware and reduces the risks arising from lost data, disruption and downtime – a bona fide belt and braces strategy.

About the sponsor, Rubrik

Rubrik, the Multi-Cloud Data Control Company, enables enterprises to maximise value from data that is increasingly fragmented across data centres and clouds. Rubrik delivers a single, policy-driven platform for data recovery, governance, compliance, and cloud mobility.

For more information:

Visit: www.rubrik.com

Follow: @rubrikInc on Twitter