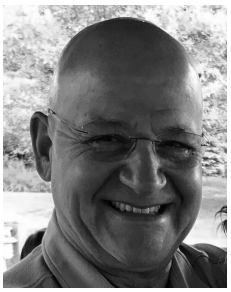
Cyber-compromised data recovery — The more likely disaster recovery use case

Received: 3rd October, 2021

John Beattie and Michael Shandrowski

Principal Consultants, Sungard Availability Services, USA



John Beattie

Michael Shandrowski

John Beattie *is a principal consultant at Sungard Availability Services, where he advises clients on operational risk and resilience programmes encompassing business continuity, compromised data recovery, crisis management, and more. He previously held positions with News Corporation as Global Director of Business Continuity and Ernst & Young as a senior manager within the management consulting practice. John is a Fellow of the BCI.*

Michael Shandrowski *is a principal consultant at Sungard Availability Services where he advises clients on establishing and maturing their disaster recovery and business continuity programmes, and then enhancing them to address compromised data recovery. He was previously the business continuity programme leader for a global insurance company.*

Abstract

To create extort a ransom payment, ransomware actors must make the threat sufficiently compelling that payment seems like the only option. This is achieved by encrypting or disabling a company's data replicas and backups as well as its production data — data that are essential to the organisation's success. To prevent this happening, it is essential to extend one's thinking beyond the organisation's cyber security incident response plan and disaster recovery programme and give active consideration to a cyber incident recovery risk management (CIR-RM) programme. This paper explores what this requires, including the right thinking, the right approach, the right team and the right plan.

Keywords: cyber crime, cyber attack, ransomware, malware, data recovery, disaster recovery, immutable backups, cyber incident recovery, cyber incident response

INTRODUCTION

Most organisations recognise the need to reduce their potential exposure to a cyber attack that compromises (eg encrypts, deletes, alters) their production and backup data. Furthermore, they are beginning to recognise that responsibility for executing data recovery falls squarely on the shoulders of the disaster recovery team, with strong support from the cyber security team to ensure that backup data and configurations are free from malware before being repatriated back into the production environment.

However, there is a caveat: the plans and capabilities established and tested for disaster recovery purposes are generally not effective for this new, unique, and much more likely recovery case. Simply stated, recovery time objectives (RTOs), recovery point objectives (RPOs), plans and capabilities that have been established for disaster recovery purposes might not apply either cleanly or universally to a data recovery effort. Moreover, because data recovery is a somewhat different recovery case, it must be planned for accordingly.

So, why might traditional disaster recovery not be sufficient to address this new recovery case referred to as 'data

Sungard Availability Services,
Unit B,
Heathrow Corporate Park,
Green Lane,
Hounslow,
Middlesex,
TW4 6ER, UK

E-mail: brian.royer@sungardas.com

Journal of Business Continuity & Emergency Planning
Vol. 15, No. 2, pp. 1–13

1749–9216

recovery'? Table 1 helps explore this question.

First, there is the triggering event. Disaster recovery declarations are triggered by events that compromise the physical data centre. These include incidents like fires, floods, power loss, and so much more. Conversely, data recovery actions are triggered by malicious activity, such as a successful ransomware attack or perhaps the malicious actions of a rogue employee.

When it comes to production impact, disaster recovery efforts take place in a whole new site (ie some place other than where the triggering event actually happened). In other words, the organisation fails over to the disaster recovery site in the event of a major incident impacting the viability of all or part of the data centre.

Data recovery efforts, however, are different. Data recovery happens 'in place', meaning that the production hardware that was impacted will either be rebuilt from bare metal or replaced to ensure that it is malware-free. Organisations often plan to stand up new hardware so they can preserve the malware-impacted hardware for further forensic analysis, once the immediate heat of malware removal and data recovery has subsided.

Then there is the matter of data currency and recovery objectives. Standing up a disaster recovery environment requires access to the most recently replicated or backed-up data. Said data will be available for immediate use as soon as it is possible to make the switch. The RTOs and RPOs should be met — assuming of course that previous disaster recovery tests have been successful and recovery objectives have proven realistic.

In a data recovery situation, however, only clean, malware-free data should be repatriated back into the production environment — that is, after validating and cleaning the data. The recency of such data will depend on the sophistication of the attackers' attempt to disrupt the organisation's backups. Indeed, said data could be days or weeks old — perhaps even months old in some cases. In other words, the RPOs are unlikely to be met. Furthermore, given the time this will take to sort out, one may as well forget about

Table 1: Key differences between disaster recovery and data recovery

	Disaster recovery	*Data recovery*
Triggering event	Data centre compromising event (eg fire, flood, power loss)	Data compromising event (eg ransomware, wiper malware, rogue employee)
Production impact	Production shifts to a predetermined disaster recovery site	Data recovery 'in place' — Malware-free data repatriated back to the production environment
Data currency	Most up-to-date or backup data available at the disaster recovery site	Most up-to-date 'clean' backup data
Recovery objectives		
RTO	Assumes successful prior test experience with a proven team	Recovery time is predicated on duration of malware-clearing activities; potentially taking a week or more
RPO	Assumes successful prior test experience with a proven team	Data loss may be days, weeks or more, depending on the backup compromising actions of perpetrators

achieving the RTOs, or even coming close.

The reality is, replicated data and recent data backups established for disaster recovery purposes will likely be of little or no value as threat actors invariably start their attacks by targeting such data in order to have sufficient leverage to extort the ransom payment.

Given the changing dynamic of production compute platforms and of disaster recovery — in a time of prolific ransomware attacks — it is becoming increasingly challenging for organisations to recover cyber-compromised data. While it is a major problem that most organisations recognise, it is one that few have addressed programmatically and can honestly claim that they are truly ready with a planned, structured and proven response. Indeed, patchwork readiness is commonly thrown in place without addressing the totality of what it takes to be ready to respond.

The bottom line is simple: reducing the risk of a failed data recovery effort requires considerably more than merely adjusting disaster recovery focused backup schedules and retention history. It is essential to be ready for the second and far more likely 'DR' incident: data recovery.

THE CYBER CRIME THREAT

Cyber attacks are top of mind for most organisations today. That concern usually extends across the executive team, and often upwards to the board. But what is not consistent is the level of preparation and true readiness to respond and address the uniqueness of a given attack vector and scope of impact. Therefore, the perception of readiness by those at the top may be flawed.

This is especially true of a specific type of cyber attack — ransomware that compromises the integrity of an organisation's data in ways that continue to make near-daily headlines. When the integrity of data is compromised, the availability of said data is also compromised. On top of this, attackers will often exfiltrate data before compromising access so that they can make the data publically available should the ransom not be paid. In essence, they completely disrupt the confidentiality-integrity-availability triad. In the words of the US Cybersecurity & Infrastructure Security Agency, ransomware may be defined as 'an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption'.[1]

Consider the following statistics:

- *86 per cent*: The volume of breaches that are financially motivated — a further 10 per cent of attacks are motivated by espionage;[2]
- *2 weeks*: The initial downtime experienced by Travelex in 2020 after the Sodinkibi ransomware attack — some customer-facing capabilities take even longer;[3]
- *US$10m*: The amount reportedly paid by GPS technology company Garmin in July 2020 for the restoration of services following a ransomware attack carried out by the operators of WastedLocker Ransomware;[4]
- *US$350m*: The estimated total reaped by ransomware gangs in 2020 — a 311 per cent increase over ransomware payments recorded in 2019;[5]
- *26 per cent*: The percentage of ransomware victims that paid the ransom and got their data back — a further 1 per cent paid the ransom but did not get their data back.[6]

Industry analysts have also weighed in on the threat. According to Forrester Research:

- 'Ransomware attacks have rocketed up the charts to become the second leading cause of IT outages.'
- 'DR planning must account for the impact of ransomware attacks…'
- 'DR programme owners need to develop recovery options, runbooks, workflows, and plans for the inevitable ransomware attacks, as the recovery runbooks will differ significantly from those in more commonly addressed disaster incidents.'
- 'Don't treat ransomware, DDoS, or other cyber attacks as the exclusive domain of the security team.'[7]

Gartner adds:

- 'A successful cyber attack can shut down operations — not just for a few hours, but, potentially, for days or weeks.'
- 'Cyber attacks can easily derail your documented and tested recovery time and recovery point objectives, because production and recovery IT assets are likely to be infected.'
- 'Your backups might also be infected. If so, then a traditional cutover to the IT disaster recovery (DR) environment might be wrong, because the cyber attacker will be right there in the recovery environment as soon as you switch operations to your alternative data centre facility.'[8]

Lastly, in the words of Databarracks:

> 'Be prepared for a significant outage. This type of incident is the most troubling for IT resilience. There are few things that can cause downtime for over a week, this is one of them. A week of downtime here for a website is massive. Other causes of downtime like human error, hardware failure, software failure are fixed quickly, without significant disruption. Major disasters like fires and floods can have a similar impact but often, there is goodwill from partners and customers. That is because they can affect lots of businesses at the same time and because they are a disaster that happens *to* you. Cyber attacks however carry the implication that your downtime was caused by a lack of competence or care.'[9]

A growing tactic among cyber criminals today is the 'double-extortion' ransomware attack. In these cases, attackers not only demand a ransom to return the stolen data, but also threaten to publicly release said data in the event that the ransom is not paid, thus making it available to possible competitors, as well as customers and news outlets.[10]

According to Emisoft research: 'We anticipate that exfiltration + encryption attacks will become increasingly standard practice and, consequently, both the risks and the costs associated with ransomware incidents will continue to increase'.[11]

No longer are ransomware attacks made solely by rogue actors working with larger dark web organisations. There is also a growth in crimeware-as-a-service by nation-state actors.[12] Nation states are buying tools and services from the dark web, while tools developed by nation states are also making their way onto the black market. According to one recently published study,[13] almost two-thirds (65 per cent) of experts believe nation states are making money from cyber crime, while 58 per cent say it is becoming more common for nation states to recruit cyber criminals to conduct cyber attacks.

Indeed, while hardware failures take the top spot as the leading cause of IT outages, ransomware attacks come in, convincingly and conclusively, at number two.

In other words, ransomware continues to escalate in frequency, sophistication and creativity. Cyber-compromised data

recovery extends beyond the domain of the information security team, and it differs from traditional disaster recovery. As a result, it requires its own set of predefined well-rehearsed plans, teams and capabilities.

THREAT CHARACTERISTICS

In understanding threat characteristics it is helpful first to define what a malicious cyber attack entails. Such attacks are conducted by groups or individuals seeking to disrupt the integrity and availability of an organisation's data and take control of it in order to harm the organisation — typically, but not always, for monetary gain.

It is important to recognise that this is different from a typical disaster recovery situation where a destructive data-centre event results in the sudden loss of in-flight transactions and, for example, the loss of data over the past 24 hours — in essence, a situation where data equivalent to predefined RTO values cannot be recovered in line with approved recovery objectives.

A ransomware attack is about the loss of days or weeks or months' worth of targeted data — a subset of data. As such, it is a different recovery case from what one might typically plan for in a disaster recovery programme. For an attacker to extort a ransom successfully, they must first make it impossible for the organisation to recover useful data — this is essential if they want to get paid. The first step is therefore to disable or destroy the backups; only then do the attackers target the production data. Sadly, the fact that ransomware extortion is a multi-billion-dollar industry (and growing) suggests that this is an area where cyber criminals excel.

It is also worth considering that external cyber threat actors are highly sophisticated and can dwell undetected in networks for a long time — often many months. According to InfoSecurity, ransomware intrusion dwell time now averages 17 days in the USA,[14] and longer still in other regions. This means the criminals have time to explore and plan before executing the attack. Again, their goal is to create a situation where paying the ransom is the best (ie only) option to restore the encrypted data. After all, if the data could simply be recovered from backups, paying the ransom would not be a consideration.

A further problem is that malware and ransomware are ever-changing. In other words, everyone is susceptible to zero-day attacks because detection and prevention tools are not yet aware of their threat profiles. On top of this, every organisation is susceptible to internal threats, such as a disgruntled employee or contractor with privileged access to the network, and human error, where, in spite of awareness training, network access is only one embedded link-click away.

In summary, the problem statement would be: is your organisation prepared to recover its most vital data following a cyber attack? Or, stated differently, have the risks of a failed data recovery effort been materially reduced in line with the organisation's risk appetite?

In this respect, the following considerations are vital to note:

- Cyberattacks are a major threat to organisations of all sizes and industries, and all indicators point to the fact that the problem is escalating rapidly;
- *All* copies of network-connected data can be compromised;
- Off-network or immutable failsafe copies (ie gold copies) are the only way to ensure that encrypted, altered or deleted data may be fully recovered;
- Traditional disaster recovery planning typically does not address this risk and related recovery case, so it is essential to review existing plans and start thinking about the differences between

the disaster and data recovery cases and whether the current disaster recovery plans provide any kind of leg up on this risk.

In short, the goal is simply to improve the odds that the organisation will be able to recover cyber compromised data, recognising that failure will always be a possibility, even with significant advanced planning and investment.

The fact is, the likelihood of an attack has never been higher and — even more problematic — the likelihood that an attack will be successful has never been higher. Compounding matters, ransomware demands have also never been higher — and now often reach well into seven figures. Furthermore, as the analysts agree, this trend will only continue. Readying one's organisation for what is very likely ahead necessitates rethinking disaster recovery — perhaps with a new equation — DR^2 — which rightfully implies the compounding effect of having to plan for both kinds of recovery cases within the disaster recovery programme.

CYBER INCIDENT RECOVERY RISK MANAGEMENT

To address these recurring challenges it is worth establishing a cyber incident recovery risk management (CIR-RM) programme based on the good practices depicted in Table 2.

The four segments of this framework can be defined as follows:

- *Identify:* Identifying and justifying the scope and requirements for protecting the organisation's vital data assets (VDAs) — the data requiring an additional level of protection due to the material and impactful consequences should said 'must-have' data be lost;
- *Protect:* Implementing the capabilities to improve the odds of there being clean, up-to-date data to restore (ie failsafe copies that are protected from attack);
- *Respond:* Preparing the overall response framework including plans, multi-disciplinary teams, enabling capabilities, and the role of the business in it all;
- *Recover:* Defining the detailed procedures for recovering cyber-compromised data including the tests and exercises that prepare everyone for such an eventuality;

While there is a logical flow to the CIR-RM framework, organisations implement those elements that best fit their needs. Some may start with a ransomware tabletop exercise just to get some immediate awareness for their teams, and to assess their readiness; others will elect to identify the VDAs that require an additional level of protection and investment; and still others will focus on a data recovery management plan to ensure they can manage this type of event and to this end identify roles, responsibilities and assignments across their enterprise. Ultimately, it is up to each organisation to look at the big picture, based on its unique points of view and the perspectives that inform it.

Before a ransomware attack forces the organisation to take action, it is important to be able to explain to executive management just how well prepared the organisation is.

CHARACTERISTICS OF VITAL DATA ASSETS

When data are classed as vital, this means that the loss of such data can directly and significantly influence a company's financial and operational performance. This means data that, if compromised, could realise some of the ever-present worries troubling the minds of executive

Table 2: Cyber incident recovery risk management (CIR-RM) good practice framework

Identify	*Protect*	*Respond*	*Recover*
VDA identification criteria and process: Business and IT infrastructure data	*Unchangeable backups:* Immutable backups	*Data recovery management plan:* Multi-disciplined roles, responsibilities, guidelines	*Isolated recovery strategies:* Approach to leverage backup solution features to validate and restore clean data to production
VDA dependencies: Logical recovery groupings	*Unreachable backups:* Secured offline backups	*Experienced ransomware adviser:* Proven ransomware incident response and forensics investigation subject matter expert	*Isolated data and application recovery procedures:* Guideline and scripts for recovery
VDA approved scope: Management approved VDAs	*Unreadable backups:* Encryption at-rest and in-flight	*Situational analysis process:* Data damage assessment and compromise scope identification	*Post-recovery clean-up procedures:* Clean and re-stage isolated analytic: and recovery environments
VDA recovery requirements: Minimum acceptable recovery configurations	*Inaccessible backups:* Identity and access controls	*On-demand clean room:* Off-network environment for forensic analysis and data validation	*Continuous alignment procedures:* Change management over time
VDA backup requirements: Useful history, change and growth rate, vault size	*Backup anomaly recognition:* Scanning tools to identify potential compromise	*Unrecoverable data: recreation procedures:* Business-owned strategies and actions	*Validation regime:* Compromised data recovery tests and exercises

VDA, vital data assets

leadership — the data needed to sustain the viability of the organisation and to meet the organisation's obligations to its customers and other external stakeholders.

The key concern here is the company's overall performance, so it is vital to focus on data that could have a big-picture, large magnitude impact at a higher level — in short, the *must-have* data. Here, one must identify and consider the sources of vital data — what they are and where they come from.

Start with the data within the scope of the existing disaster recovery programme. Experience would suggest that most disaster recovery programmes fail to focus on the truly vital data. Most recovery programmes include non-vital data, while many omit data that should be considered vital. For example, one oil exploration and production company found that the massive amounts of geological and ecological research it had invested tens of millions of dollars to obtain was outside of its disaster recovery programme's scope, despite the fact that its loss would be catastrophic from both a financial and regulatory perspective. Simply stated, the data were 'vital', but not protected.

Most VDAs are a subset of tier 1 critical data within a disaster recovery programme, representing, on average, 10–20 per cent of the data — or, in other words, a subset of a subset of an organisation's total data footprint. They could include business applications that support the core products or services and they could also include infrastructure operational and control data, like Active Directory. In fact, VDAs can come from a myriad of places in an organisation's network. Vital data may be structured or unstructured — and may even be in the hands of third-party processors.

It is also important to consider data that might impact any forward-looking

financial statements that analysts may be watching. Has the organisation made commitments and how would it be materially impacted by data loss?

Again, it is important to focus on the must-have data — the data essential to the business and its ability to meet its key obligations to its stakeholders and, where relevant, stockholders. It is important to evaluate data from an enterprise, rather than a departmental level.

VDAs can vary by industry, by sector, and they may not even rank as a top disaster recovery priority. Consider, for example, a pharmaceutical company that is gathering research and clinical trial data as part of a multi-year study. These data may not even be in the top tier for traditional disaster recovery planning; however, the fact that the data support new products and future long-term revenue, the loss of such data could have a major impact on the company in both the short and long term.

In what follows, this paper will explore the programme-level good practices framework in more detail.

Identify

Having emphasised the importance of thinking about vital data beyond the scope of one's disaster recovery programme and the RPO values within it, it is time to explore how to identify and justify the VDAs within the organisation.

The first step is to establish a VDA qualification framework that is specific to the organisation. This requires developing an approach and/or the criteria to assess VDA candidates consistently across the entire ecosystem. It is important to do things consistently in order to normalise the data both initially, as data assets come and go, and as business priorities change.

Keep in mind that it may be difficult to keep business and even IT people focused on this new and different recovery case as they are likely to be wed to the concept of disaster recovery related RTOs and RPOs. Be sure to ask if each data asset is the single source of the data. Is it the source of record within the organisation? Can it be recreated automatically from other sources?

Impacts must be identified and measured at the enterprise level. In the event of data being lost, will this have local, regional or global implications? Will there be financial market implications and are they going to be reported on the news the same night? What is the level of potential impact? Will it cause the organisation to miss yearly goals or growth initiatives?

Viewed another way, would the loss of specific data assets realise risk factors previously defined as unacceptable?

Based on this assessment, one can establish a data asset scoring mechanism in order to arrive at an impact score. In this way, it is possible to create an objective business justification to define what constitutes a VDA and what does not.

The next part is VDA qualification assessment and the consideration of possible mitigation factors. There could be temporary workarounds — maybe a quick fix to keep key operations running should data be compromised (eg running the previous week's inventory report). This might not be ideal solution, but if it is possible to retrieve data from a system that has not been compromised, it may be possible to achieve 80 per cent accuracy.

Still, there remain further questions to ask. For example, is it possible to rebuild the data from data held in other systems? Can accurate data be recreated manually? For example, were all the inventory data to be lost, would it be possible to go back and manually re-inventory a distribution centre to see where things stand? How much data would it be technically possible to recover or recreate — and how feasible would this be? How long would it take

and how many people would have to be reassigned to do it?

The last pieces of the puzzle are the business and technology profiles. Having identified the vital data and committed, as an organisation, to putting a solution in place, it is possible to start the process of turning the collected business data into technical solutions and requirements. Components that play into this include data types, content and/or configuration, size of the data store, growth rate, archive requirements, and much more.

Protect

The next consideration is protection — that is, having the capabilities to safeguard the VDAs beyond what may be in place for disaster recovery purposes. First and foremost, this requires a failsafe data protection capability to reduce the overall risk of a failed data recovery effort.

A reliable recovery strategy is about having clean data available to recover — something that requires immutable backups. This may also entail having retention locks that set durations and timeframes for preserving the data and securing them offline to make said data as unreachable as possible by a threat actor. These backups also need to be fully encrypted both in-flight and at-rest to reduce the risk of the data being sold or publicly released. In essence, the data must be protected against the threat of double extortion.

One must also consider so-called 'smart analytic' tools that can detect anomalies and data behavioural changes within the backup environment. These tools can provide early warning of an attack. It is also vital to have a rapid-response team that can evaluate the alerts emanating from the analytic tools to determine whether there is a logical business reason for the alert or if someone is tampering with the organisation's backups. This essential capability should make it possible to limit damage and, in most cases, stop the attack before it affects production.

Respond

Formally planning a response to any threat, including ransomware, is essential.

This requires a plan that guides the overall response across a multi-disciplinary team. This plan must ensure that response is well managed, well controlled and well integrated with other processes within the organisation.

Certain elements of a technical disaster recovery management plan can be repurposed here, such as team notification, communications, collaboration protocols and tools. Beyond that, however, there is much more to consider over what is in a typical disaster recovery plan, including what the infrastructure and operations team are doing while waiting for the cyber security team to confirm the scope of the attack and the point-in-time when it started.

Expert support is vital, and these experts must be retained well before any attack is identified, because they must be able to jump into action within minutes. Having an experienced ransomware 'quarterback', on retainer, is both essential and prudent.

Also to define is the situational analysis process for ascertaining the scope of data to be recovered. The data to be recovered may well fall outside the scope of what was actually encrypted as certain data may be required to sync fully with other data. In short, the scope for data recovery could extend beyond the data targeted in the attack.

After this, one must factor in how data will be analysed to ensure its cleanliness prior to bringing the data back into production. This represents a considerable undertaking as restoring malware-infected data will simply re-infect the production environment. Where this will happen is also important. It is worth making

arrangements for an on-demand clean room — a secured analytic environment in which it is possible to verify that the malware has been eradicated prior to repatriating the data into the production environment. All too many organisations have re-infected their production environments in their haste to return to normal operations.

Lastly, everyone else in the business must be ready to do their part. This is likely addressed in the organisation's business continuity plans and may include alternative work procedures and manual workarounds to keep the business moving in the absence of key applications being available.

Unfortunately, given the nature of cyber attacks, application downtime will likely far exceed predefined RTO values. In other words, the business continuity plans may fall short when it comes to extended-duration workarounds.

This is where it is important to know which applications are dependent on vital data, in order to make sure the business plans properly for extended application outages caused by the loss of VDAs.

It is also important to make sure the organisation has a plan for how it is going to fill in the unrecoverable gaps in data. If the organisation is lucky, such gaps may simply equate to the RPO values defined for disaster recovery. Quite possibly, however, the data loss could far exceed RPO values.

It is also important to make sure the organisation has a plan for how it is going to fill in the unrecoverable gaps in data. If the organisation is lucky, such gaps may simply equate to the RPO values defined for disaster recovery. Quite possibly, however, the data loss could far exceed RPO values; especially for VDAs, which are prime targets for threat actors seeking to extort ransomware payments. For such assets, assume a potential loss of loss of at least one week, or even better, one month. Business continuity plans should define exactly how the organisation will respond to such material data loss possibilities. This will help everyone in the organisation be better prepared to do their part in the event of a data-compromising cyber attack.

Recover

When the attack happens, it is imperative to have predefined yet flexible strategies for data recovery. These need to address both compromised data and the recovery of impacted applications, inclusive of synchronisation with non-impacted but interdependent data. It is good practice to define such procedures for all VDAs along with a more generic approach for non-VDAs.

Then there are the more detailed recovery procedures to be defined — the guidelines and scripts to make 'recovery' happen. This also includes such issues such as whether to rebuild compromised production servers from bare metal before repatriating the data, or repatriating data onto fresh servers only.

Naturally, there will also be the inevitable post-recovery clean-up procedures where all 'unclean data' and the hardware used for clean data identification are wiped clean.

Keeping everything in alignment with a changing production environment is also a key, but by no means simple task. So, just like for the disaster recovery programme, it is essential to adjust the change management process to include all aspects of compromised data recovery.

It is important to assemble a team of people who are capable of jumping into an intense, pressure situation at any time of the day or night, without advance notice, and for those people to be well aware of what is expected of them, and how the organisation at large (based on their actions) will be responding.

Therefore, just as with disaster recovery

and business continuity, it is important to plan awareness coupled with focused exercises and extensive tests.

In fact, just like any other plan, it is important to build awareness across the entire multi-disciplinary team expected to use it. Planned walk-throughs are a good start, and tabletop exercises are an excellent way to further advance understanding. Such exercises also build confidence in both the process and the decision-making. Multiple tabletop exercises, delivered over time, are recommended in order to continue to build that awareness and confidence. Of course, some exercises and testing may be focused on the recovery of specific data — for example, the VDAs — previously identified as being critical to the organisation.

Validation of everything is a must, and this requires both exercises and tests. Tests should address a variety of challenges, including the approach and the environment for analysing data to ensure everything is free from malware before being bought back into the production environment, as well as readying the production environment to receive clean data approved for repatriation.

Once the difference between data recovery and disaster recovery is recognised, rethought and recalibrated, organisations will be able to address the various differences and be in a position to respond and recover across both 'recovery cases'.

Without such recognition, no individual charged with disaster recovery, much less data recovery, is going to look good in the eyes of executives when a ransomware attack or other form of malicious data compromise happens.

TEAM INTEGRATION AND OWNERSHIP

Data recovery also requires a centralised and coordinated response including multiple teams, myriad disciplines and many pieces, including:

- *Cyber security*: Responsible for removing malware, performing forensics and identifying clean data;
- *IT data recovery teams*: Responsible for restoring the data or applications that have been compromised;
- *Business continuity*: Focused on workarounds or process shutdowns or processes and workflows; and
- *Third-party ransomware coach/advisers:* Specialists who are often on retainer and are experts in all aspects of ransomware response and malware-related forensics.

Naturally, it is also important to consider how each of these teams and stakeholders will coordinate. Simply put, ransomware attacks are both a business problem and a technology problem.

In any integrated teams approach, the question, 'who owns it?', is inevitable. If an incident should occur, it is one thing to have planned and tested the response, and to have buy-in from stakeholders, but again, in the long run, who owns it? This is an important question to answer.

Responding to a ransomware (or other malware) attack is a drawn-out process, and it can take anything from days to weeks to restore data and conduct the necessary forensic analysis. This is why it is important for any integrated teams approach to have a champion, as it requires ownership to see the problem through from start to finish.

CONCLUSION

It may be an over-simplification of the facts, but when it comes to ransomware, there are no guaranteed defences to prevent its insurgency.

Fortunately, by taking a holistic approach

to the threats and applying appropriate risk controls and risk management principles, one can 'buy down' the risk of a failed data recovery effort. So, identify vital data assets; protect them by leveraging immutable backup technologies; monitor them for anomalies as their integrity is essential; develop threat-focused plans to guide response to an actual ransomware situation; and make sure it all works at the time of recovery by conducting exercises and tests that validate the plans, capabilities and teams.

While there is no silver bullet when it comes to recovering data compromised by ransomware, by being prepared and applying the CIR-RM good practice framework outlined herein, it is possible to manage the changing face of data recovery effectively, and, ideally, before one's organisation is targeted by a cyber attacker.

References

(1) Cybersecurity & Infrastructure Security Agency (2021) 'Ransomware guidance and resources', available at: https://www.cisa.gov/stopransomware/ransomware-101 (accessed 22nd October, 2021).

(2) Verizon (May 2020) 'Data breach investigations report', available at: https://www.verizon.com/business/resources/reports/dbir/?CMP=OOH_SMB_OTH_22222_MC_20200501_NA_NM20200079_00001 (accessed 22nd October, 2021).

(3) Akshaya, A. (April 2020) 'Travelex paid $2.3 million to ransomware gang: report', BankInfoSecurity, available at: https://www.bankinfosecurity.com/travelex-paid-23-million-to-ransomware-attackers-report-a-14094 (accessed 22nd October, 2021).

(4) Soare, B. (December 2020) 'The year in ransomware', Heimdal Security, available at: https://community.spiceworks.com/topic/2300299-this-year-in-ransomware-payouts-2020-edition (accessed 22nd October, 2021).

(5) Cimpanu, C. (February 2021) 'Ransomware gangs made at least $350 million in 2020', ZDNET, available at: https://www.zdnet.com/article/ransomware-gangs-made-at-least-350-million-in-2020/ (accessed 22nd October, 2021).

(6) Bourne, V. (May 2020) 'The state of ransomware', Sophos, available at: https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf (accessed 22nd October, 2021).

(7) Chhabra, N. (2020) 'The State of Disaster Recovery Preparedness in 2020', available at: https://www.forrester.com/report/The-State-Of-Disaster-Recovery-Preparedness-In-2020/RES159676 (accessed 22nd October, 2021).

(8) Witty, R., Hoeck, M. and Gregory, D. (2021) 'How to prepare for and respond to business disruptions after aggressive cyber attacks', available at: https://www.gartner.com/en/documents/3956262/how-to-prepare-for-and-respond-to-business-disruptions-a (accessed 22nd October, 2021).

(9) Databarracks (2020) 'The Travelex ransomware attack: Are you prepared for extended downtime?, available at: https://www.databarracks.com/blog/the-travelex-ransomware-attack-are-you-prepared-for-extended-downtime (accessed 22nd October, 2021).

(10) Whitney, L. (February 2021) 'Ransomware threats to watch for in 2021 include crimeware-as-a-service', TechRepublic.com, available at: https://www.techrepublic.com/article/ransomware-threats-to-watch-for-in-2021-include-crimeware-as-a-service/ (accessed 22nd October, 2021).

(11) Emsisoft Malware Lab (July 2020) 'The chance of data being stolen in a ransomware attack is greater than

one in ten', Emisoft Blog, available at: https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/ (accessed 22nd October, 2021).
(12) Whitney, ref. 10 above.
(13) Holland, A. (April 2021) 'Nation states, cyberconflict and the web of profit', Threat Research, available at: https://threatresearch.ext.hp.com/web-of-profit-nation-state-report/ (accessed 22nd October, 2021).
(14) Muncaster, P. (April 2021) 'Global attacker dwell time drops to just 24 days', InfoSecurity, available at: https://www.infosecurity-magazine.com/news/global-attacker-dwell-time-drops/ (accessed 22nd October, 2021).