Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

How Tape Technology Can Be Used to Defeat Ransomware

A Key Tool to Enable Cyber-recovery

By Christophe Bertrand, Practice Director
and Monya Keane, Senior Research Analyst

April 2022

This ESG White Paper was commissioned by HPE
and is distributed under license from ESG.

Contents

Market Landscape and Key Trends

Concerns about ransomware have grown massively. According to ESG research, 82% of organizations are more concerned about ransomware today than they were two years ago, and conversations about ransomware have been escalated to the executive level in 67% of these organizations.[1]

The apprehension over ransomware is also unfolding against a backdrop of severe skills shortages. Forty-eight percent of respondents to an ESG research survey reported that their organizations had a shortage of cybersecurity skills, and cybersecurity spending tops all spending intentions at this point—69% of surveyed organizations expect their spending on cybersecurity to increase in 2022.[2] That willingness to invest highlights the reality and scope of this threat.

And it should be no surprise. Recent ESG research shows that an alarming 63% of organizations have been on the receiving end of attempted ransomware attacks in the past 12 months, with 36% experiencing ongoing attempts on a monthly basis or even more frequently. Alarmingly, nearly half (48%) of the respondents reported being the victim of a *successful* ransomware attack.[3] ESG expects that both the frequency and the success rate of these attacks will only accelerate moving into the future.

That problem is compounded further by the fact that at 82% of surveyed organizations, full-time employees have access to sensitive data,[4] which violates the principle of "least privilege access" (enforcing the lowest permission levels that still will allow users to perform their roles). It makes the need for cyber-resilient storage technology all the more urgent, and tape technology should be at the forefront of this effort.

Even when they have put protective measures in place (such as backups, primarily disk- or cloud-based), 43% of surveyed IT decision makers remain very concerned that their organization's "golden copies" (protected copies) could also become infected or corrupted by a ransomware attack.[5] That's why having backup copies that are either not easily accessible or not accessible at all through the network is key. *Offline copies of data augment cyber-resiliency.*

Implementing data recoverability capabilities has become a top-of-mind issue for IT decision makers, with 53% of respondents stating that their organizations currently have data recoverability capabilities in place to combat or mitigate ransomware attacks,[6] and is a priority investment area for 2022. Ransomware is now very visible to the top echelons of organizations. ESG research shows that ransomware readiness is the top priority for 22% of organizations and a top-five priority for another 46% (see Figure 1).[7]

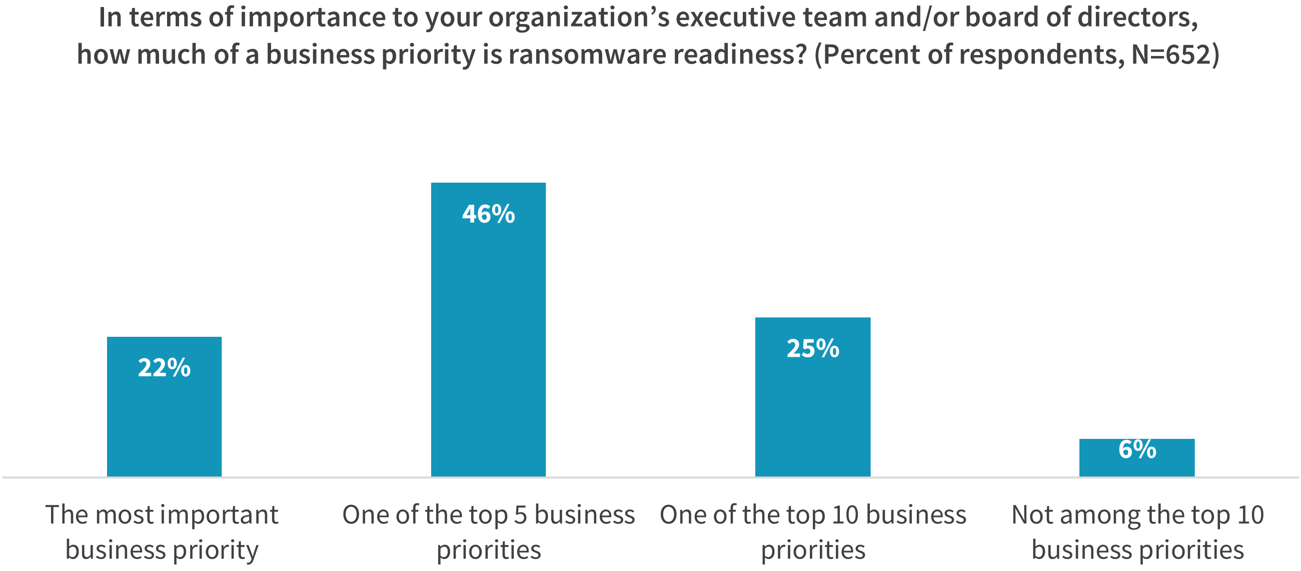
Cybercrime, including ransomware, is clearly rampant. It creates a significant data protection challenge for many organizations and the recovery processes they employ. Because attackers have become more sophisticated in targeting data *and backups*, organizations must put in place solutions that truly will protect data assets and ensure cyber-resilience.

That's where tape technology shines. Tape provides a scalable yet cost-effective answer to fending off attackers and significantly increasing the odds of recovery, even from frequent attacks. Thirty-five percent of organizations surveyed by ESG have deployed isolated recovery solutions and related storage. Tape allows air-gapping capabilities, and that's likely

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.
[2] Ibid.
[3] Ibid.
[4] Source: ESG Survey Results, *The State of Data Privacy, Compliance, and Data Security*, October 2021.
[5] Source: ESG Research Report, *Tape's Place in an Increasingly Cloud-based IT Landscape*, January 2021.
[6] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.
[7] Ibid.

why 61% of organizations leveraging isolated protection storage technologies are keeping production data on tape as a part of these solutions or will likely do so.[8]

Figure 1. Ransomware Readiness Is a Top Business Priority



Source: ESG, a division of TechTarget, Inc.

It's also worth noting that 85% of those organizations tell ESG that they have a high or very high degree of confidence in tape technology in the context of tape isolated recovery schemas.[9] Their vote of confidence for tape technology as a key component of a cyber-resilient strategy should inspire all organizations to consider or reconsider tape solutions for use themselves. After all, while other storage technology options do exist, they may still be susceptible to nefarious encryption. Let's explore this topic further.

The New Norms of Disaster Recovery

When a cybersecurity event occurs, it is expected that IT will leverage an incident response plan or methodology to take the steps necessary to identify, isolate, and remove the threat. That "first line of defense" may be successful, but considering the currently high frequency of attacks, it is not a matter of if but when an attack will eventually succeed.

This means the very nature of RTO and RPO changes in a cyber-attack situation. Traditionally with disaster recovery, a server has a critical malfunction, a database is lost, a flood occurs, etc. There is a linear set of actions that IT can perform to get back within SLAs to a point in time where data is again coherent to support business resumption.

But in a cyber-attack, organizations do not know whether they have the data to recover back to a normal situation. They don't know what's good, bad, incomplete … or where it has been moved.

In traditional disaster recovery, for example, after a server breaks down, most organizations might have an SLA requiring them to get back up and running within minutes. In the case of a cyber-attack, the question becomes, "Are we ever going to

[8] Source: ESG Research Report, *Tape's Place in an Increasingly Cloud-based IT Landscape*, January 2021.
[9] Ibid.

be able to get back? Are we ever going to be able to recover our now-encrypted data?" The traditional concept of RPO and what constitutes a disaster is now very challenging to navigate.

Essentially, disaster recovery is "over." We're in a different space now; everything is cyber-recovery. Why? Because if you can adapt and adjust to a cyber-event and recover in a certain timeframe, then other types of outages will likely be easier to fix. It's a different workflow or runbook … but it's a matter of when, not if. The bar is now raised.

Organizations should strive to recover and resume business as quickly as possible, but that can only be done with "good" unadulterated data. Therefore, a combination of technologies and strong processes is needed. (Some organizations favor the NIST framework to help them craft their processes and establish a successful recovery protocol.)

In general, a multi-layered strategy is needed, and tape technology will be an invaluable element of that strategy. It is ESG's opinion that tape should be included as part of a cyber-recovery plan.

Protecting What Matters with Tape

The Vulnerability of Disk- and Cloud-based Backups

Bad actors know they have a better chance of achieving their goal—i.e., receiving payment or else destroying the data—when their victims have no backup available for recovery.

A number of vulnerabilities exist with many current disk- and cloud-based backup solutions. That's because they were designed for accessibility to enable quick recoverability, not necessarily for security. Their main purpose is to provide an easy-to-reach copy of data for recovery purposes.

However, data and application backup systems themselves can become targets of attacks, encryption, and data leakage. That's why it is vital to revisit storage access-control lists, network exposures, and the locations of backups. Making backups extremely hard to access is why the case can easily be made that tape *must* be included in a recovery strategy. Tape will provide the golden copy. And with modern backup and tape solutions, assured-good backups can occur frequently throughout the day to optimize recoverability speed.

Protecting Vital Data with Tape

The ability to recover applications and associated data is predicated upon having all components of the infrastructure, all processes, and all people in place.

Remember that having only the application data itself back online won't suffice to resume operations. Protecting *every* key IT component is critical because those other components are just as vulnerable to being specifically targeted in an attack. For example, just think about how complex it would be to run your IT environment if all your administrator credentials were being held for ransom.

What vital data should be protected on tape? The following list and Table 1 offer a quick summary:

- Mission-critical application data with low RPOs (a few hours at most). This means investing in more frequent air-gapped backups for those applications. Of course, there are significant variations by vertical industry—in healthcare, for example, the focus is on electronic medical records, scheduling apps, medical imaging, payment systems, and similar workloads. In retail, the focus is on the point-of-sale application, logistics systems, employee scheduling, and so on.

- Infrastructure configuration data (Active Directory, networking configurations, and virtualization infrastructure). No business can resume operations without its back-end IT infrastructure in place. Bringing back critical data alone is not going to be enough.
- Intellectual property (long-term data, archives, etc.). This is an area where data destruction or data exfiltration (either by outsiders or unauthorized insiders) can be catastrophic.

Table 1. What to Protect on Tape

Type of Data	Specific Examples
Mission-critical Infrastructure Data	Authentication, Active Directory/LDAP, DNS dumps, certificates, event logs, physical and virtual platform builds, scripts, custom and third-party software, firmware, and operating systems.
Networking	Switch/router configurations, firewall settings, IP services, DNS mapping, and access control configurations.
Storage	DR or backup hardware configurations (e.g., appliances), SAN/array configurations, and firmware.
Intellectual Property	Source code, proprietary algorithms and documents, and test/dev libraries.
Documentation	IT asset lists, disaster recovery run books, and incident-response checklists.

Source: ESG, a division of TechTarget, Inc.

The bottom line is that tape enables organizations to ride out the worst-case scenario: one in which their infrastructure itself has been improperly accessed.

Leveraging Air Gapping with Tape

An “air gap” in IT terms means no direct or indirect physical connection exists between a computer or other IT system and the rest of the network (private, public, or internet network) to ensure maximum security. If the data can’t be reached, it can’t be corrupted or stolen.

Air gapping not only keeps an isolated copy of critical data off the network, but it also provides (ideally) multiple recovery points to guarantee that an uncompromised golden copy is always available for recovery.

Isolating and segregating the infrastructure and data is vital to accelerating incident response time and optimizing the effectiveness of that response. Remember that in a worst-case scenario, attackers will disable vital infrastructure components such as Active Directory or DNS mapping, rendering all related business operations inoperable.

Tape possesses a unique set of characteristics that support air gapping for all data and infrastructure components by design. Tape is more than an efficient and secure storage medium. It (and its management tools) also offer automation and security capabilities. These capabilities include encryption, WORM, physical management, access control (e.g., role-based authentication and multi-factor authentication), and vault or system partitioning. It’s not surprising that, as already mentioned, 85% of organizations surveyed by ESG have a high or very high degree of confidence in tape technology for isolated recovery.[10]

Limiting Data Leakage with Tape

Another great advantage of tape is overcoming data leakage events. Have hackers been trying to steal your data from the cloud? That's almost impossible to do with tape. The hacker would need to be physically where the tapes are and have all the right access permissions. But if the data is in a cloud service, then it's easier for someone to export a few gigabytes and put it up for ransom.

The Strategic Relevance of Tape

Tape has a long, reliable history with IT professionals, and it continues to be a storage technology used extensively by many organizations and service providers, including hyperscalers. Tape is truly experiencing a renaissance—due in large part to its reliability, capacity, extremely competitive cost profile, inherent cyber-friendly features, and very favorable sustainability/green profile.

But recoverability is the key. While there may be a lot of interest in what cloud providers and object storage vendors market as "immutable storage" and "software-based air gapping," those solutions do not and cannot deliver the capabilities of a physical offline backup to tape.

Similarly, technologies such as continuous data protection are great for rolling back data within minutes in a traditional DR scenario. That may not work in a worst-case cyber-attack scenario in which admin credentials are compromised and infrastructure components become unusable.

Your cyber-resilience will be put to the test sooner or later. Having the best technology on your side is going to be incredibly important. Tape technology must be part of the arsenal available for you to leverage to support your cyber-resilience and, ultimately, your cyber-recovery.

The Bigger Truth

Attack vectors for ransomware are numerous. It's unlikely that any IT organization can completely seal every single one. It's not a question of if but when you will be targeted. Organizations now understand that cybersecurity is a business issue that requires all their attention and focused IT investment.

Different solutions bring different strengths to the table, and tape offers many compelling advantages in the realm of cyber-resilience. The majority of tape users are continuing to place their bets on tape, with 61% of organizations reporting to ESG that they are going to continue to invest further in tape, while 26% will maintain their current investment.[11]

Depending solely on other solutions is not good enough anymore. Businesses demand recoverability in a timely fashion, with full data integrity. To accomplish that feat, all business-critical data (and applications, infrastructure configurations, etc.) must simply be put out of the reach of the criminals trying to get their hands on it.

It is ESG's strongly held position that tape is incredibly relevant and useful for defending digital data against the threat of ransomware and related cyber-attacks. In short, tape should be a part of the arsenal of any modern IT organization.

[10] Ibid.
[11] Ibid.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com

contact@esg-global.com

508.482.0188