ESG SHOWCASE

Leveraging Tape to Combat Ransomware

Date: April 2020 **Author:** Christophe Bertrand, Senior Analyst

ABSTRACT: Cybercrime, including ransomware, is rampant and creates a significant challenge for protecting data across many organizations and recovery processes. Traditional backup and recovery is not enough to fend off the evolving threat and minimize production network exposures, the ensuing business impact, or inherent risk. Air gapping and tape technology offer a perfect combination to deliver proven and scalable advanced ransomware protection.

Market Overview

Cybercrime, including ransomware, is rampant and creates a significant challenge for protecting data across many organizations and recovery processes. ESG's recent research shows that 60% of organizations report experiencing at least one attempted ransomware attack in the last 12 months. This is making investments in security a top priority: 62% expect to increase cybersecurity spending in 2020. Not surprisingly, improved cybersecurity is the top business driver for tech spending in 2020, and security is still the most common IT investment justification metric (36%).[1]

Ransomware is a business-interruption event that affects data and application uptime and thus comes with significant consequences across the board. Business and technology leaders are naturally very concerned about the risks associated with destroying mission-critical data assets that can't be easily or economically recreated. In addition to the data loss risk, direct and indirect consequences on service and system unavailability can significantly affect an organization. Organizations must make mitigating risks associated with ransomware a major IT and business priority.

In many ways, ransomware attacks are akin to "logical data disasters," or events in which data becomes corrupted, unusable, or lost. Reversing the effects of data loss is the traditional role of backup and recovery mechanisms. Our research shows that recovery is both the top mandate and the top challenge of IT professionals.[2] Recoverability is critical, and while it must meet recovery time metrics to support the business, it is also fundamental that backup data be uncorrupted, or what is traditionally called a "golden copy."

In recent years, a new set of risks associated with backup copies themselves has emerged, generating a significant amount of concern among data protection IT professionals (see Figure 1).[3]

---

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[2] Source: ESG Master Survey Results, *2018 Data Protection Landscape Survey*, November 2018.
[3] ibid.

Figure 1. Cyber Attacks Affect Confidence in Protection Copies

Generally speaking, aside from the impact malware infections and ransomware events could have on production data and operations, how concerned are you that your organization's protection copies of data (backup/snapshot/replication) could also become infected or corrupted by these types of attacks? (Percent of respondents, N=320)
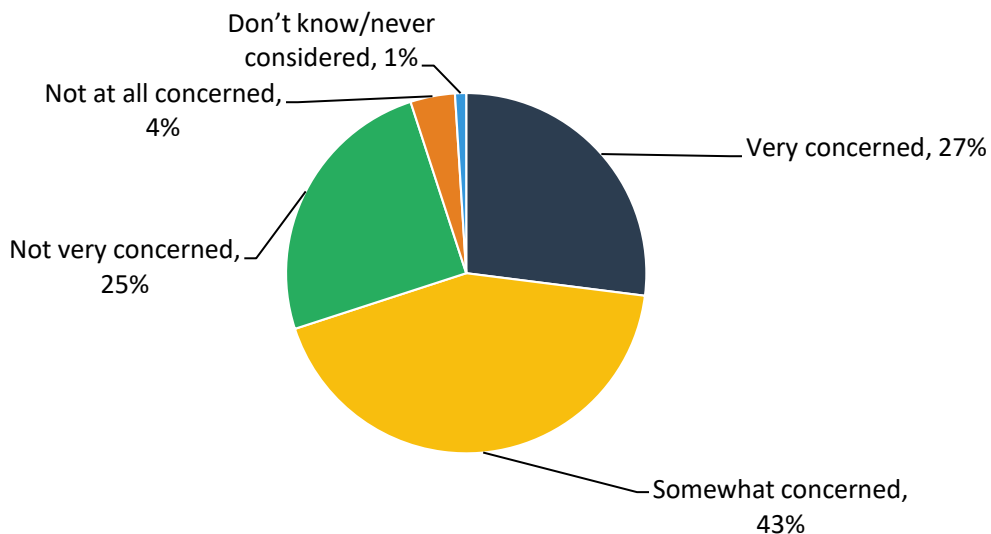
Source: Enterprise Strategy Group

As cyber-criminals become more proficient and mount attacks on the backup infrastructure, IT leaders must install strong mechanisms and technologies to fend them off. It has become key to "protect the protector"—i.e., protect the backup data and solutions. This is where having backup copies that are not easily accessible, or not accessible through the network at all, can help. Businesses need offline copies of data to augment cyber resiliency.

Augmenting Backups with Air Gapping and Tape Isolated Recovery

Traditional backup and recovery can be performed and stored locally or in cloud environments; many topology variations exist. They serve the primary purpose of having an easy-to-reach copy of the data for recovery purposes. The easier the access to the files, the better.

In contrast, what we will call a "cyber-resilient" copy of data must *meet much more stringent requirements* in order to not be affected or infected by ransomware. This is where "air gapping" and tape technology come into play.

This section will cover the need to leverage a topology that air gaps the backup data.

Air Gapping

An "air gap" in IT terms means that there is no direct or indirect connection between a computer or system and a network (such as private, public, and internet networks) in order to ensure maximum security. If the data can't be reached, it can't be corrupted or stolen. Our research shows that 41% of surveyed organizations have deployed isolated recovery solutions, while 47% are interested or engaged in the process of planning or testing them.[4]

---

[4] Source: ESG Master Survey Results, *2018 Data Protection Landscape Survey*, November 2018.

Air gapping keeps an isolated copy of critical data off the network, with no direct network connection and ideally multiple recovery points, to guarantee that an uncompromised "golden copy" is always available for recovery. Isolating and segregating the infrastructure and the data is critical to optimizing incident response time and effectiveness. This is what defines "isolated recovery."

Automation and policy management capabilities are another important aspect to consider as protection and recovery workflows can be complex and prone to errors when left to manual interventions.

This set of requirements makes tape an ideal medium because of its capacity, performance, automation, durability, vendor ecosystem integration, and, last but not least, cost characteristics.

Tape to the Rescue

Tape has a long history with IT professionals and remains a significant storage technology used by many organizations and service providers, including hyperscalers. It is truly experiencing a renaissance due to its capacity and extremely competitive cost profile.

In fact, among those who have an isolated recovery solution in place, 49% implement or will implement a tape-based solution. In the context of backup, recovery, and archiving, 28% of IT professionals indicate that they will continue to invest in tape and increase their current footprint, while 35% will maintain their current footprint. In the data center, onsite and offsite tape represents a steady 21% of the total volume of backup data in enterprises, a number that is projected to remain stable through 2020.[5]

ESG has identified many benefits for users of the most common current tape technology known as LTO-8.[6] LTO-8 technology builds on the inherent reliability and low costs of tape media, enabling organizations to lower hardware costs in their storage infrastructure. The higher capacity of LTO-8 media can decrease operational expense, as more data can be stored on fewer tapes. There is also decreased operational expense, including administration, support, maintenance, infrastructure, and data migration. Since an organization can leverage higher-capacity cartridges, less space is consumed in the data center. Also, compared with disk-based systems, LTO-8 tape's reliability and high transfer rates can help businesses gain timely access to tape-stored data, more reliably, as data is less at risk of being lost while tape is less prone to failure.

Many types of tape systems exist, ranging from small one-tape autoloaders to very large capacity libraries. One of the great benefits of tape storage is its compelling and sophisticated use of automation, which simplifies the deployment of the technology at large scales. This in turn offers a strong alternative to other approaches that can quickly become costly at scale such as disk-based object storage. For the best cost profile and high scalability, tape rules.

The Bigger Truth

Cyber-attacks have become a serious concern for IT leaders in many organizations, and it has become clear that these will keep intensifying in the future. Daily news unfortunately provides a constant reminder that no one is immune to ransomware. It is a technical and business risk that just can't be ignored and must be addressed with education, prevention, and remediation processes and proven technologies. Testing and evaluating new and innovative approaches is important to further IT efficiency, but when it comes to cyber-resilience, proven approaches prevail because newer approaches can require significant investments and may not scale.

---

[5] ibid.
[6] Source: ESG Economic Validation Summary Report, *Quantifying the Benefits of LTO-8 Technology*, August 2018.

Leveraging an air gapped topology that is based on proven and efficient technology is part of the solution to mitigate the impact of cyber-attacks. Tape systems provide a great set of options to deliver isolated recovery capabilities at scale, and hyperscale, with a cost profile that cannot be matched by disk-based technologies.

With all the characteristics highlighted, a very desirable cost profile, and virtually unlimited scale, tape is poised to continue its "rebirth." Its inherent strengths become more vital in contemporary IT, rather than less.

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