Enterprise Strategy Group by TechTarget

storcom EVOLVE TO THE CLOUD

WHITE PAPER

Defeating Ransomware With IBM Storage Defender

By Christophe Bertrand, Practice Director
Enterprise Strategy Group

January 2024

Contents

Market Overview

Ransomware Is Pervasive

The prevalence of ransomware is a growing concern for businesses of all sizes. Whether or not an attack is successful, the fact remains that it's not a matter of *if* but rather *when* an organization will experience such an incident. Recent research demonstrates that 75% of respondents have reported falling victim to ransomware within the past year.[1]

Unfortunately, the current situation is far from ideal, as only a small percentage of victims can fully recover their data. This is due to the complexity of the recovery process and the fact that ransomware attacks are becoming increasingly sophisticated and more difficult to detect. Also, 6 in 10 organizations have not thoroughly tested their incident response strategy. As a result, organizations must take proactive measures to secure their systems and minimize the risk of falling victim to such attacks.

Overall, massive amounts of data—often in the petabyte range—are affected by these attacks. At this scale, it is easy to see how much disruption can be caused and how recoverability will be made more complex.

Cybercriminals target various types of data sources. Research by TechTarget's Enterprise Strategy Group (ESG) indicates that regulated data, such as personally identifiable information (PII), is the most favored target (cited by 58% of respondents). However, it's not just sensitive production or mission-critical data (cited by 40%) that is vulnerable; sensitive infrastructure data comes in second to PII (55%). This implies that cyberattackers will explore multiple avenues to impact operations and advance their ransom or extortion schemes.

There are many ways cybercriminals can affect data, applications, and infrastructure. The initial point of compromise for successful ransomware attacks includes application software vulnerabilities, systems software vulnerabilities, the software supply chain, and misconfigurations. It should also be noted that 24% of respondents surveyed by ESG indicated that ransomware had been re-injected from an old backup. This should be a focal point for the IT and security operations team: What good is a backup that is not "clean" and perpetuates the problem by letting ransomware back in post-recovery?

Ransomware Is a Business Issue

Ransomware is a severe threat that has the potential to cripple organizations completely. It is alarming to note that a whopping 65% of respondents consider it one of the top three most severe threats to their organization's viability.

This is a fundamental problem for many organizations because ransomware can inflict significant data, operational, and financial disruption. Leading the long list of impacts are data exposure (cited by 53% of respondents), data loss (51%), and operational disruption (46%) (see Figure 1).

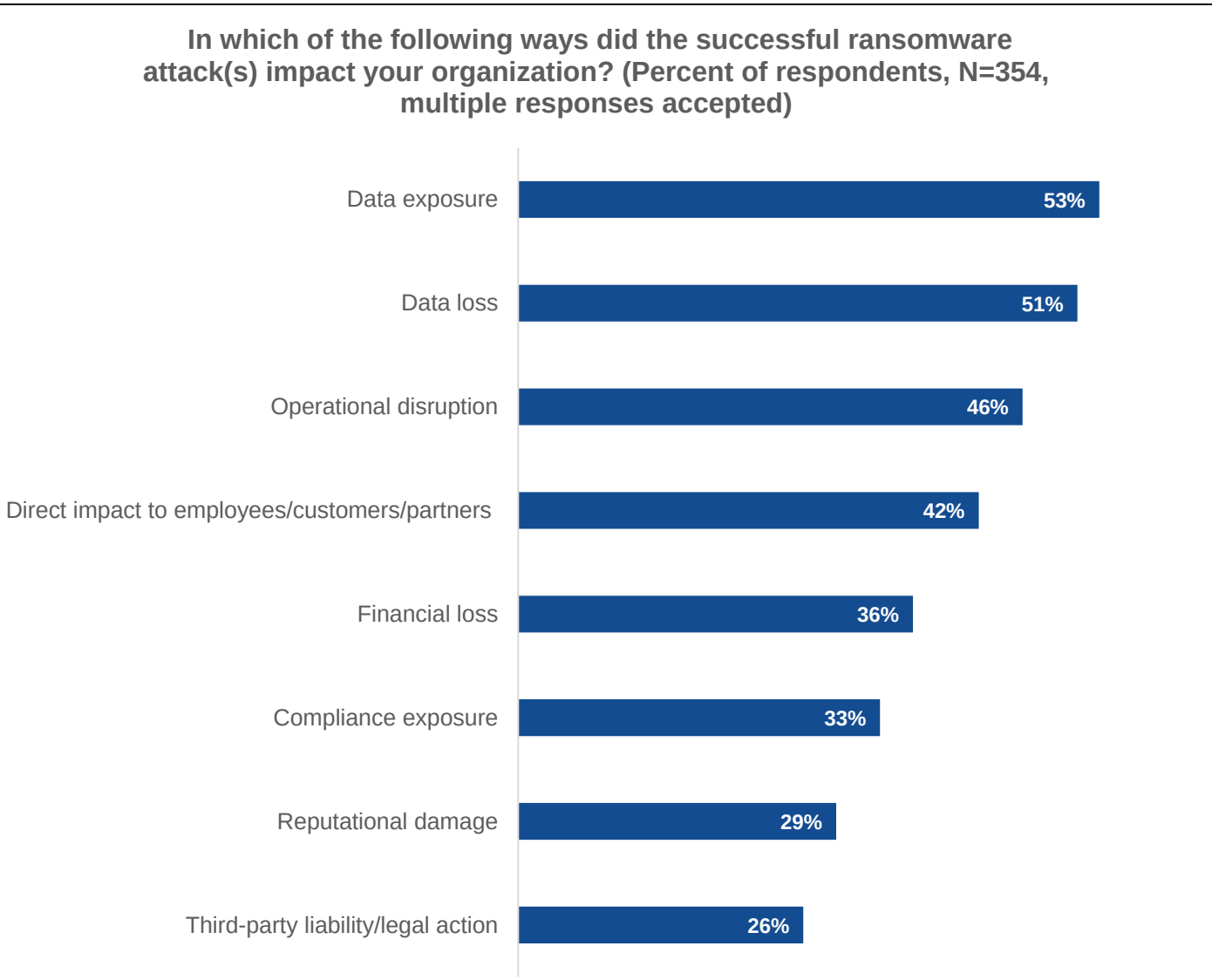
In addition, 23% percent of IT professionals indicated that successful attacks have had an extensive impact on their organization, affecting multiple business functions and involving a significant amount of data, applications, users, and/or systems.

Ransomware attacks are, therefore, a severe threat to any organization, and once a system is infiltrated, the consequences *can* be devastating. The primary objective in such a scenario is to recover lost data and prevent further damage. The reason for this is twofold: First, data losses can lead to noncompliance, resulting in hefty fines and legal issues. Secondly, losing important business transactions can have long-lasting implications for the organization's growth and reputation.

[1] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023. All references and charts in this white paper are from this report unless otherwise noted.

In our opinion—considering the estimates government agencies worldwide have provided, showing global costs in the hundreds of billions—ransomware has become an "industry" in itself. The dark web offers ransomware services as a pathway for fueling the growth of attacks. In other words, the barriers to entry for cybercriminals have been lowered, also opening the door for insider attacks.

Figure 1. Impact of Ransomware



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Protecting Mission-critical Applications and Systems

Ensuring the protection of mission-critical applications is of utmost importance. However, it is unfortunate that many organizations cannot meet this requirement. Only 25% of organizations are confident in their ability to recover more than 80% of their mission-critical data and applications, while just 15% can protect over 90% of such applications. Ideally, this number should be much higher. The disconnect between the actual numbers and the ideal numbers is the reason why ransomware and cyberattacks can have such a devastating impact on the data and application

infrastructure. But this is also an opportunity for organizations to revisit and improve their recovery technology and strategies.

It's essential to acknowledge that infrastructure data, including backup data, can be vulnerable to cyberthreats. Data recovery may become impossible if backups are compromised or deleted. Consequently, attackers may attempt to target these valuable workloads. A significant number of IT leaders (around 29%) have expressed concerns regarding the security of their backup and recovery infrastructure.

To address these concerns, it's essential to prioritize the protection of backups. Currently, 40% of organizations take additional measures to secure all their backup copies, while 44% do so for most of their backups.

Solution Requirements

Beyond Traditional Disaster Recovery

According to 69% of IT professionals, recovering from ransomware attacks is significantly different from other types of disasters for a number of reasons: 56% of survey respondents reported that successful cyber-recovery requires different technologies and features, and 53% of respondents said they believe different workflows must be leveraged for that purpose. For 53% of respondents, cyber-recovery is more complex than traditional disaster recovery, and according to 50% of respondents, it requires different personnel and skill sets.

Therefore, traditional technology approaches must be reconsidered, and new, more comprehensive solutions are needed to tackle ransomware's complexity, scale, and impact. Enterprise Strategy Group research identifies the critical capabilities expected by IT leaders today.

Top Requirements for Ransomware Recovery Solutions

When considering the technology and features currently needed in the market, it is apparent that any solutions implemented must have a wide range of capabilities across many disciplines.

It's crucial to understand that no single vendor can provide a complete ransomware recovery solution. Instead, a range of technologies and vendors must collaborate to create integrated solutions that cater to the diverse requirements of organizations. Therefore, a comprehensive ransomware recovery solution should incorporate a broad spectrum of capabilities provided by multiple vendors.

A variety of factors or capabilities are essential considerations in the selection of a ransomware recovery solution, among which are data encryption (at rest and/or in flight) and the ability to protect many data sources, including SaaS products, VMs, endpoints, and the backup workloads themselves. The ability to detect ransomware in data copies and backups is in the top three on the list of requirements, with 34% of respondents selecting it as a must-have.

In this context of protecting critical data and backup assets, air-gapping technologies are critical, according to IT leaders. Of those surveyed, 27% report already deploying this type of solution, while a majority (52%) are interested or already engaged in investing in an air-gapped platform.

Our research also shows that IT leaders expect their data protection and ransomware recovery vendors to form partnerships and integrations to help tackle the broad nature of cyberattacks and establish a cyber- and data-resilient infrastructure.

Among key partnerships are those with vendors in the areas of cloud security, network security, data loss prevention, endpoint security, managed detection and response, managed security services providers, security platform providers, and extended detection and response vendors. Organizations essentially must enable layers of detection using different technologies.

IBM Storage Defender for Data Resilience

Solution Overview

IBM believes that data resiliency is a comprehensive approach to safeguarding data and ensuring its accuracy and integrity. It involves distinguishing between primary and secondary workloads and addressing targeted recoveries that are critical for restoring operations. IBM Storage Defender is a powerful tool that provides end-to-end visibility for data resilience across primary and secondary workloads. It brings together the necessary capabilities for enterprises to achieve real data resilience beyond just data protection.

Defender provides a range of capabilities essential for meeting organizations' data resiliency requirements. IBM Storage Defender, for instance, is equipped with intelligent software that helps identify threats such as ransomware, and exfiltration. With this tool, organizations can quickly determine the safest recovery points and integrate their existing security operations tools and processes to recover their company as soon as possible.

IBM Storage Defender can detect threats and anomalies across primary and secondary workloads by leveraging sensors from backup metadata, array snapshots, and other relevant indicators. Using IBM Storage Defender, customers can detect events earlier and recover faster by knowing the location of their latest clean copy.

IBM Storage Defender is optimized for personas based on their specific roles across storage, backup, and SecOps. It can bring the right groups together to converge on the recovery plan. Also, IBM's licensing model allows clients to pay for specific Storage Defender services based on usage, providing a more flexible approach that can help fill data resiliency gaps and avoid payment for capabilities already in place.

Key Solution Capabilities

IBM Storage Defender comprises various components that provide a comprehensive view of data impacts and a coordinated response. It also seamlessly integrates with SIEM and security orchestration, automation, and response (SOAR) tools to ensure that security consoles have complete visibility into threats, from the networks to the stored data.

Capabilities that Storage Defender provides include:

- Backups and data protection.
- Replication.
- High availability.
- Air-gap (logical and physical).
- Immutable copies.
- Isolation.
- Encryption.
- Data reduction rate monitoring.
- Anomaly detection for hardware snapshots.
- Anomaly and malware detection for VM backups.
- Anomaly and malware detection in near real time for VMs.
- Primary storage.

- Backup recovery.
- Archive recovery.
- Snapshot and immutable copy management (crash-consistent and application-consistent).
- Recovery testing (integration with partner solution).
- Primary storage clean room (integration with partner solution).
- Backup clean room (integration with partner solution).
- Tape and S3 Cloud integration.
- IBM Qradar SIEM integration.
- Performance and capacity monitoring (primary).
- Subscription licensing.
- Resource unit licensing model.
- Single buying experience.
- Consolidated support experience.

A Modern Management Experience

The IBM Storage Defender portal is the landing page for users accessing all current and future IBM Storage Defender services. Each IBM Storage Defender customer has a tenant to connect to. User identity is managed through IBM Security Verify.

IBM Storage Defender provides a platform for future data-resiliency services. Defender includes cloud-based and on-premises services and solutions that the customer selects and enables based on their specific needs.

Metadata and some cataloging data will be stored in the cloud, but backup and storage data will only be moved to the cloud if the desired solution specifically requires it. The solution also offers threat detection aggregation and simple recovery orchestration.

Protecting Your Investments in Existing Technologies

IBM is not the only company that values data resilience and believes it cannot be achieved through a single vendor's solution. Data resilience requires a collaborative effort, and IBM's Storage Defender offers a solution that can enhance the capabilities of an existing system. This also means the Storage Defender platform does not require a complete system overhaul to improve resilience. Storage Defender, in conjunction with its partner solutions, can provide a customized solution that meets the specific requirements of each customer's environment.

The capabilities offered by IBM Storage Defender provide a wide range of options to achieve data resilience efficiently and effectively while leveraging an ecosystem of complementary technologies. With its ability to eliminate the need for multiple solutions and integrate seamlessly into existing infrastructure, it presents a valuable solution for ensuring the sustainability of data for the long term.

Conclusion

The threat of ransomware attacks has grown exponentially in recent years, posing a significant challenge for organizations. These malicious attacks often result in data breaches, financial losses, and company reputation damage. Therefore, organizations must take a proactive approach to address this challenge and ensure they have the necessary measures to safeguard their operations and protect against cyberthreats. By doing so, organizations can enhance their cyber and business resilience as well as minimize the impact of any future ransomware attacks.

The research is clear: Ransomware attacks can fundamentally impact business processes and operations, leading to significant compliance exposure, reputation damage, and financial loss. Cybercriminals constantly evolve tactics to target valuable or regulated data and infrastructure, making data recovery even more challenging.

While restoring all data is a challenge that many organizations face, it is essential to understand the far-reaching impacts of ransomware attacks, beyond data-related issues such as data exposure and loss.

The threat of ransomware attacks has become a fundamental concern for businesses worldwide. IT leaders understand the need for proactive measures to protect their businesses against these threats. They are searching for practical solutions that can address the complexity and pervasiveness of this issue. IBM's Storage Defender platform is an excellent option that can provide comprehensive protection against ransomware attacks. Its advanced features can help businesses stay ahead of the curve and avoid the devastating consequences of ransomware attacks.

IBM Storage offers a comprehensive set of data-resiliency capabilities alongside a robust ecosystem, highlighted by IBM Storage Defender, which provides a proactive solution to detect attacks efficiently, recover data and business operations quickly, simplify data protection, and seamlessly integrate with cybersecurity tools to ensure end-to-end cyber resilience. By leveraging IBM Storage's extensive data resiliency ecosystem, organizations can manage data recovery more efficiently, mitigate the risks of ransomware attacks, and enable business continuity in the face of cyberthreats.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com