Enterprise Strategy Group™
by TechTarget

WHITE PAPER

Storage’s Role in Addressing the Challenges of Ensuring Cyber Resilience

By Scott Sinclair, Practice Director and Senior Analyst
and Monya Keane, Senior Research Analyst

December 2022

This Enterprise Strategy Group White Paper was commissioned by IBM
and is distributed under license from TechTarget, Inc.

Contents

Executive Summary 3

Introduction 3

The Rising Threat of Cyberattacks and Ransomware 3

The Role of Data Storage in Cyber Resiliency 5

Data Storage and Data Protection: Knowing Where to Focus to Minimize Ransomware Risk 6

Shifting from Cybersecurity to Cyber Resilience with IBM 6

- Building a Cyber Resilience Foundation with IBM Safeguarded Copy 7
- Cyber Resilience with IBM Cyber Vault 8

The Bigger Truth 9

Executive Summary

Data's role as a transformational business asset continues to grow. Thanks to increasing investments in application development; modern DevOps practices; and heightened business intelligence, analytics, and machine learning demands, nearly all businesses are accelerating data creation and usage. They are also scaling the number of locations that leverage data. This proliferation of data combined with mounting pressure to accelerate operations has led to an increase in the complexity of both IT infrastructure and IT operations.

Such factors put organizations and their infrastructures at great risk of experiencing malicious attacks, human error, and negligent behavior. Unfortunately, legacy strategies cannot adequately ensure that business operations will continue during and after these types of incidents. Companies can try to weave together capabilities in an attempt to prevent attacks and other breaches, but functional gaps, poor integration, and management complexity make meeting security objectives time-consuming and difficult.

Changing organizational mindsets from prevention to incident preparation—e.g., implementing storage solutions with built-in cyber resilience—is key to safeguarding critical data assets and being able to quickly respond to and recover from ransomware and other cyberattacks.

Introduction

IT faces new challenges. Over half (53%) of survey respondents to research by TechTarget's Enterprise Strategy Group (ESG) say IT is more complex today than it was two years ago. This increase in complexity may be the result of ongoing digital transformation initiatives (cited by 33%), higher data volumes (34%), the rapid evolution of the cybersecurity landscape (35%), and/or efforts to adhere to new data security and privacy regulations (34%).[1]

Simultaneously, organizations are struggling to address a problematic shortage of critical IT skills. In fact, 45% of surveyed organizations report they don't have enough cybersecurity specialists—it was the most often-cited shortage area. Additionally, these organizations are dealing with application, device, and remote/mobile worker sprawl, which are increasing the size and scope of the security perimeter that IT is tasked with protecting.[2]

Given the complexity of modern IT, proliferating data, and ever-growing cyberattack threats, IT teams often struggle to keep pace. Trying to address complexity with internal personnel alone is a losing battle. Success requires modernizing the underlying infrastructure itself. However, when doing so, IT decision makers must look for technologies that don't just meet application needs or simplify operations. Achieving true success means finding technology that can achieve those goals and improve the cyber-resiliency posture of the application environment as well.

The Rising Threat of Cyberattacks and Ransomware

Organizations face increasing cybersecurity threats, likely fueled by increasing financial incentives for cybercriminals. For example, complaints from the American public in 2020 to the FBI's Internet Crime Complaint Center (IC3) increased 69% from 2019, with reported losses exceeding $4.1 billion.[3] Additionally, over the past five years, the IC3 reports a combined $13.3 billion in total losses.[4] As of the fourth quarter of 2020 in the U.S., the average length of interruption after ransomware attacks on businesses was 21 days.[5] Clearly, ransomware's negative impact on business operations is substantial.

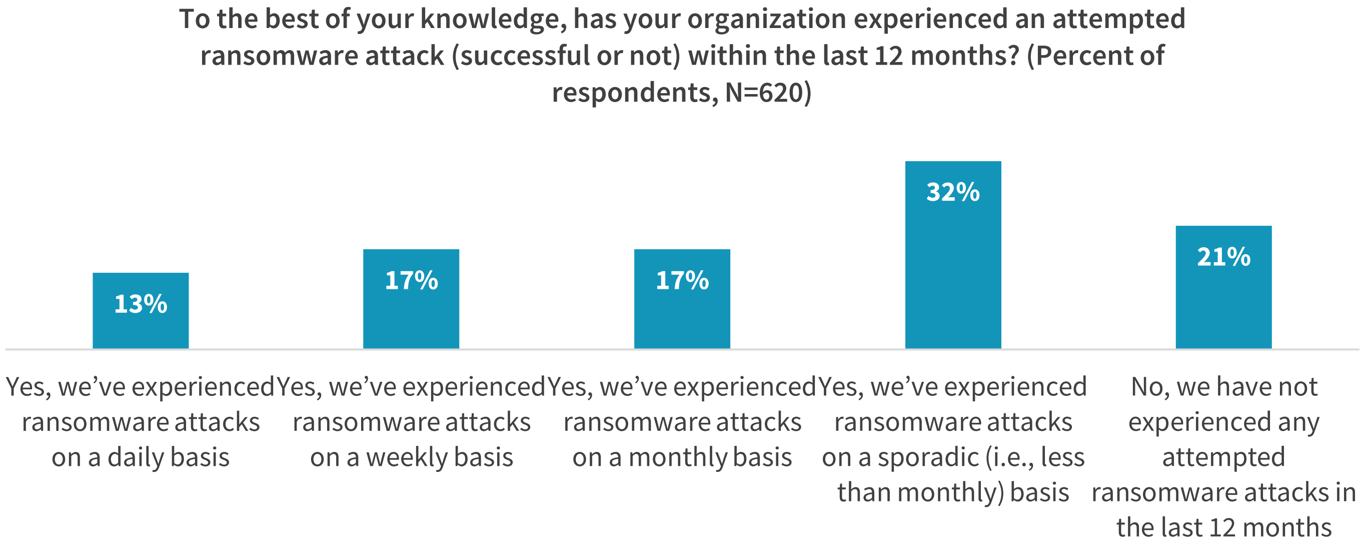
[1] Source: Enterprise Strategy Group Complete Survey Results, *2023 Technology Spending Intentions Survey*, November 2022.
[2] Ibid.
[3] Source: Federal Bureau of Investigation Internet Crime Complaint Center, *Internet Crime Report 2020*.
[4] Ibid.
[5] Source: Coveware Blog, *Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands,* February 2021.

A strong correlation exists between IT complexity and cyberattack vulnerability. As IT grows more complex, cyberattacks will increase in frequency and come at a higher cost.

Ransomware is a pervasive threat and one that attacks a business's most valuable asset—its data. The IC3 identified 2,474 reported ransomware incidents in 2020, and Enterprise Strategy Group (ESG) found that 63% of the organizations it surveyed experienced ransomware attacks in the past year. In fact, 13% experienced ransomware attacks on a daily basis (see Figure 1).[6]

Ransomware protection requires a technology strategy that expands beyond the realm of traditional cybersecurity—it should leverage advances in data storage and data protection as well.

Figure 1. Seventy-nine Percent Experienced Ransomware Attacks in the Last 12 Months



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

Among those respondent organizations that experienced a ransomware attack, 73% identified that at least one attack was successful. In response to a follow up question to the victims of a successful ransomware attack, more than half (56%) identified that their organization paid the ransom.

Paying the ransom, however, was not often an effective strategy. ESG found that among those organizations that paid a ransom, 87% faced additional extortion attempts to pay additional fees beyond the original demand, and only 14% identified that they got 100% of their data back after paying the ransom.

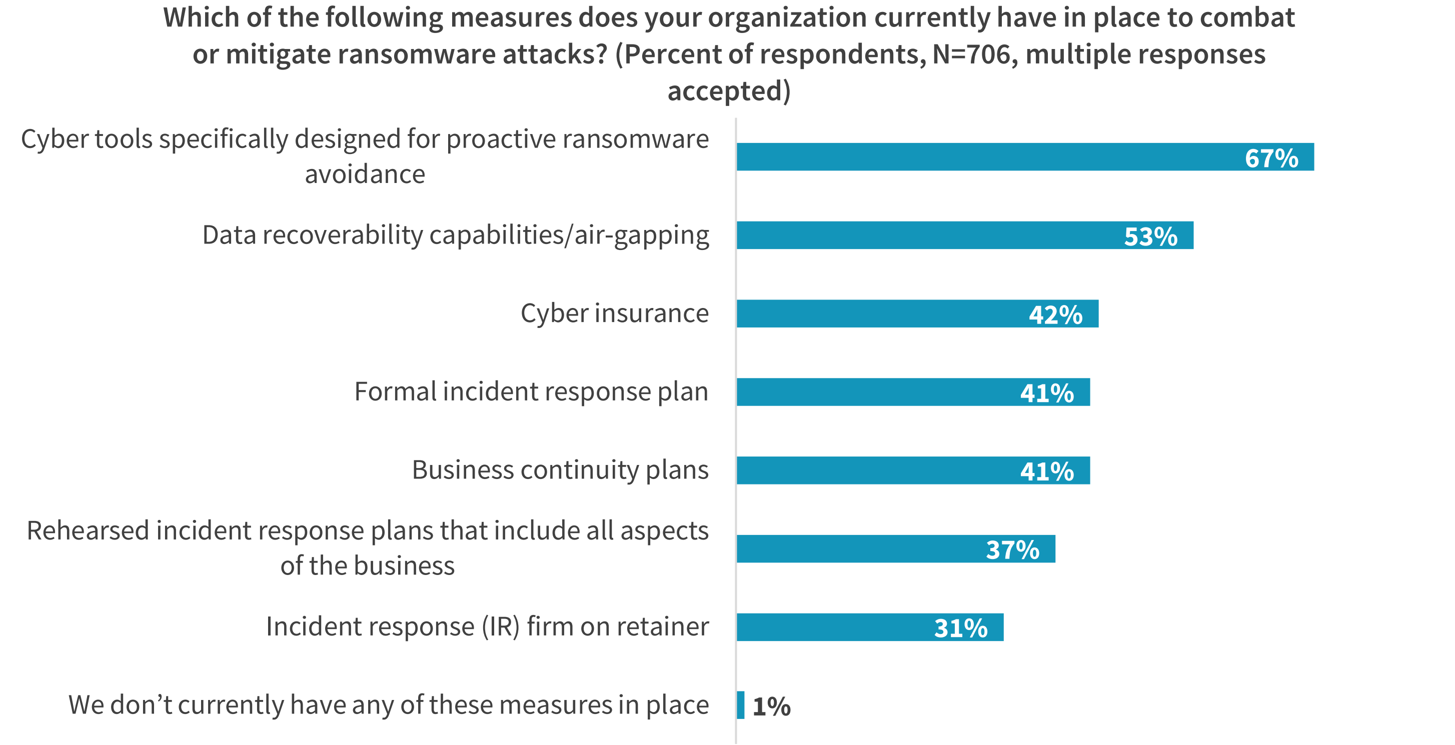
[6] Source: Enterprise Strategy Group Complete Survey Results: *The Long Road Ahead to Ransomware Preparedness*, June 2022.

The Role of Data Storage in Cyber Resiliency

When Enterprise Strategy Group asked IT decision makers which measures their organizations have in place to combat or mitigate ransomware attacks, 67% of the respondents reported using cyber tools for proactive ransomware avoidance, and 53% identified data recoverability capabilities such as air-gapping.

Storage systems and storage administrators both play a big role in protecting against ransomware. When Enterprise Strategy Group (ESG) asked IT decision makers which measures their organizations have in place to combat or mitigate ransomware attacks, 67% of the respondents reported using cyber tools for proactive ransomware avoidance, and 53% identified data recoverability capabilities such as air-gapping (see Figure 2).[7] Those two commonly identified responses highlight the importance of not only implementing measures to avoid an attack, but also investing in solutions to ensure the business is prepared to recover when an attack inevitably occurs. It's important to avoid simply setting up policies to combat or mitigate ransomware, and then stop. This "partial" approach creates a false sense of security because, while effort is made to mitigate attacks, little or no effort is actually made to establish an effective data recovery plan *before* it's needed.

Figure 2. Common Measures in Place to Combat or Mitigate Ransomware



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

It's important to remember that combating an attack is quite different from traditional data recovery. Typically, organizations almost always want to recover their data by using the most recent copy. But with ransomware, IT typically doesn't know which "good" copy to use; hence, recovery is often riskier and can take much longer. Some ransomware attacks not only target data, but also target the backup infrastructure itself. This is why advanced storage capabilities are foundational for effective ransomware recovery.

[7] Source: Enterprise Strategy Group Research Report, 2022 Technology Spending Intentions Survey, November 2021.

Organizations should shift from asking "*How do we protect?*" to "*If we're hit by ransomware, how fast can we recover? How quickly can our business return to normal?*"

While adopting the measures identified in Figure 2 is smart and needs to increase, organizations must understand that no single defense is 100% effective for ransomware recovery. While it is important to consider tools that specialize in identifying and avoiding ransomware as well as recovering data, that is just part of the effort. Even with the best defense, it's possible an attack might get through. Organizations must prepare for that eventuality and assess how they can minimize the business impact by recovering as quickly as possible. To minimize overall ransomware exposure, organizations should look for ways to accelerate how soon they can identify attacks, how quickly they can mitigate any damage, and how fast they can recover with a known-good copy.

This is where strong cyber resiliency strategies come into play, taking into consideration *all data-handling components*, i.e., hardware, software, people, and process. When developing a cyber resilience posture, organizations should shift from asking "*How do we protect*?" to "*If we're hit by ransomware, how fast can we recover*? *How quickly can our business return to normal*?"

Data Storage and Data Protection: Knowing Where to Focus to Minimize Ransomware Risk

Ransomware recovery is a form of disaster recovery, but the effects of ransomware are quite different from those of a fire or a flood. After all, you can generally tell when a fire is fully extinguished. Ransomware is more like a hidden spark inside a wall that could potentially reignite at any time. Storage admins need to focus on certain areas to help reduce the risks associated with ransomware. Because speed is essential, they should determine how quickly their organization can:

- Identify a risk.
- Quantify the damage that was done.
- Mitigate the damage by identifying a known-good copy, recovering using that known-good copy, and ultimately restoring operations.

Taking a "this won't happen to us" approach is risky at best. Organizations must be proactive, and put in place an effective data storage and protection solution—before they actually need it.

Shifting from Cybersecurity to Cyber Resilience with IBM

With its extensive experience in cybersecurity and risk management, IBM is a recognized leader in cyber resilience and offers a comprehensive suite of advanced storage and data protection solutions, including:

- IBM FlashSystem and DS8000, which are primary storage solutions that come with data immutability and encryption features that can be automated or can be subscribed to as a service.
- IBM Storage Scale, IBM Storage Scale System, and IBM Storage Ceph, which are file and object storage solutions with data immutability and encryption features that can be automated or can be subscribed to as a service.
- IBM Tape Storage, which also supports data immutability and encryption and provides protection through air-gapping.

- IBM Spectrum Sentinel, which is a prebuilt solution designed to help organizations simplify and improve their ransomware detection and recovery by integrating scheduling, scanning, and identifying potential recovery copies. Spectrum Sentinel is currently available for SAP HANA and for Epic Healthcare Systems.

- IBM Spectrum Copy Data Management software manages and protects copies of data.

- IBM Spectrum Protect Suite for additional protection. Spectrum Protect software-defined storage can place data on flash, disk, object storage, and physical or virtual tape. It then detects malware and ransomware activity by identifying large deviations from normal access patterns.

- IBM QRadar and IBM Storage Insights solutions help accelerate detection of potential threats using AI-enhanced capabilities.

Building a Cyber Resilience Foundation with IBM Safeguarded Copy

IBM Safeguarded Copy allows users to create granular point-in time copies of active production data that are immutable protected copies and cannot be altered or deleted. Users must have the right privilege access to modify the Safeguarded Copy expiration settings supporting a separating of duties approach to operations and management. Lastly, Safeguarded Copy leverages existing Copy Management software for testing and ease of recovery of copies. Figure 3 offers additional details on IBM Safeguarded Copy.

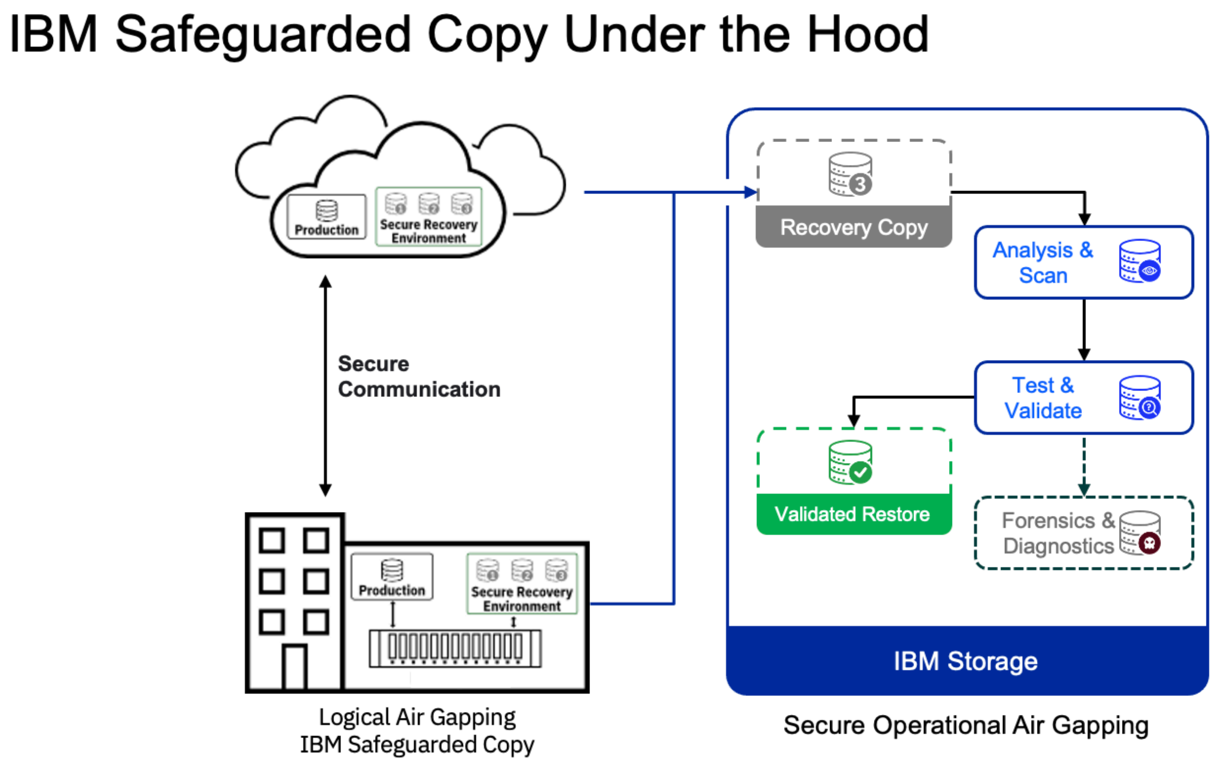
In summary, IBM Safeguarded Copy offers:

- Protected copies of the data that deliver a higher level of security while meeting industry and business regulations. Safeguarded Copy backups are immutable, which means they are hidden, non-addressable, cannot be altered or deleted, and only usable after recovery.

- Automation to set and manage policies, such as the number of copies or the retention period, to simplify and accelerate management and restoration.

- Separation of duties. Traditional backup and restore capabilities normally do not protect against intentional (e.g., rogue employee) or non-intentional attacks. By preventing access to Safeguarded Copy expiration settings, backups are provided increased protection against internal attacks.

Figure 3. IBM Safeguarded Copy



Source: IBM

Cyber Resilience with IBM Cyber Vault

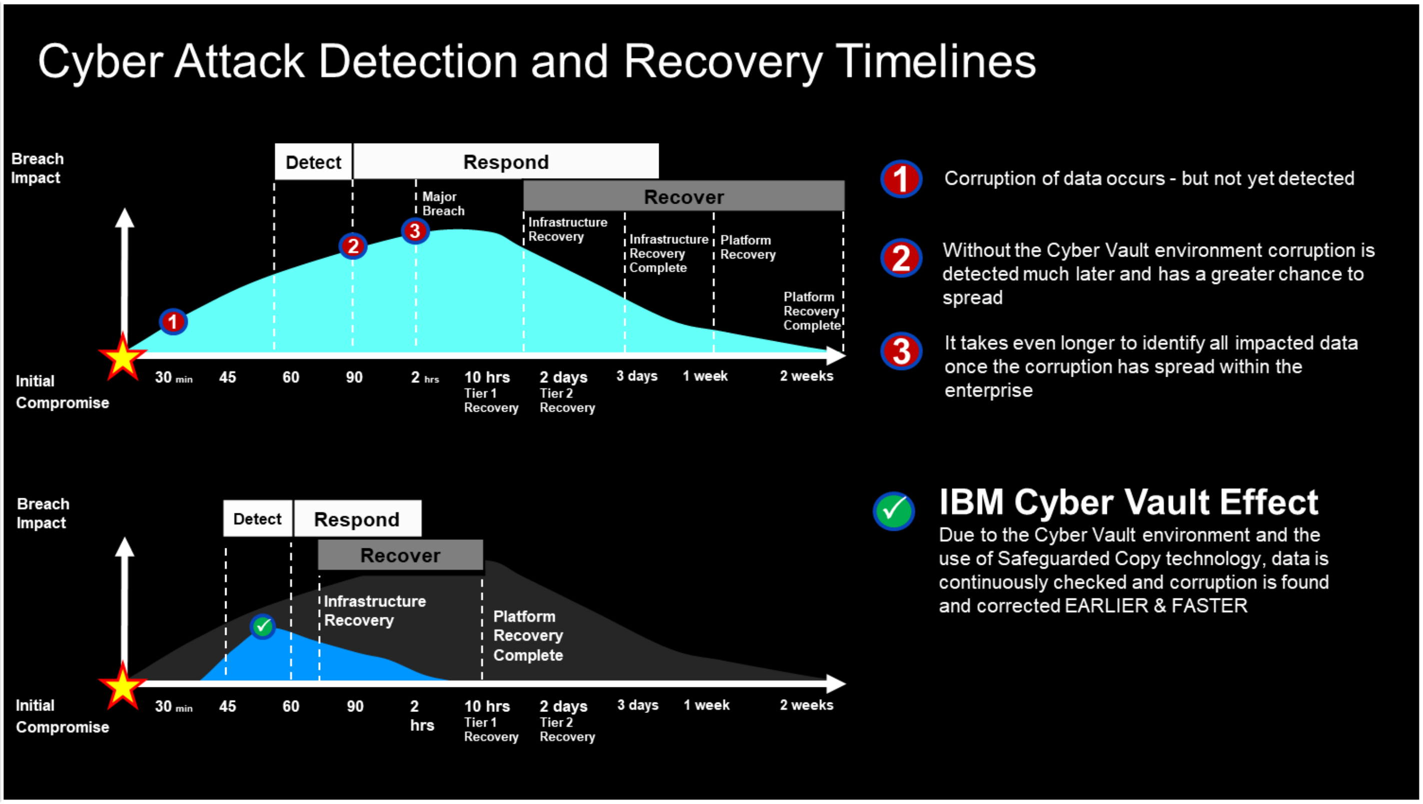
It is hard to overemphasize storage’s role in protecting against ransomware. The storage software is seeing the changes made to primary data, and because it is seeing those changes, it’s in a great position to identify when an attack is starting. It is the technology that is taking and protecting secondary copies, too—which makes storage critically important to help with recovery. With these facts in mind, perhaps one of the most useful tools of all in IBM’s cyber resiliency toolbox is IBM Cyber Vault.

IBM Cyber Vault is a security methodology for rapid recovery from a cyberattack. It is built on top of IBM Safeguarded Copy, a technology for regularly creating isolated, immutable snapshots. Cyber Vault analyzes these snapshots, looking for potentially malicious changes that could indicate the presence of ransomware. IBM Cyber Vault also integrates with IBM QRadar and IBM Storage Insights for even faster detection. Its validation of immutable copies allow admins to quickly identify a good copy, test it, and then restore from it.

In terms of enhancing speed in particular, IBM Cyber Vault helps storage administrators accelerate:

- Identification—The integration of QRadar and Storage Insights offers enhanced detection and monitoring.
- Mitigating and quantifying damage—This is an automated process. Early, automatic detection of attacks obviously enables faster recovery from them.
- Identification of a known-good copy—Automation of immutable copies of data occurs if a threat is detected.
- Restoration of operations—Rapid recovery is possible within hours, instead of days or weeks (see Figure 4).

Figure 4. How IBM Cyber Vault Accelerates Cyber Recovery



Cyber Attack Detection and Recovery Timelines

1 Corruption of data occurs - but not yet detected

2 Without the Cyber Vault environment corruption is detected much later and has a greater chance to spread

3 It takes even longer to identify all impacted data once the corruption has spread within the enterprise

✓ IBM Cyber Vault Effect

Due to the Cyber Vault environment and the use of Safeguarded Copy technology, data is continuously checked and corruption is found and corrected EARLIER & FASTER

Source: IBM

IBM Cyber Vault is available to users as an IBM service offering, where experts from IBM work with organizations to tailor the solution to suit the needs of their specific application environment. For select application environments, such as SAP HANA or EPIC Healthcare Systems, IBM offers Spectrum Sentinel, which delivers IBM Cyber Vault capabilities in a pre-architected turnkey implementation designed to simplify and accelerate deployment.

The Bigger Truth

IT infrastructures are continuing to become more complex, increasing the opportunity for human error, system failures, or negligence to occur. Simultaneously, malicious actors—both inside and outside the organization—are relentless in their efforts to search for and exploit weak links.

Without a doubt, security incidents will happen. This fact should compel a change in the organizational mindset from reactive to proactive—from fervently attempting to prevent an attack to preparing for and responding to security failures *when* they happen. This is the transformation organizations must undertake as they travel from cybersecurity to cyber resilience.

Many organizations are modeling their cyber resilience strategies after the guidance provided by the NIST Cybersecurity Framework, which recommends that organizations identify critical resources, protect those resources, detect failures and breaches, and plan for response and recovery from cyber incidents. Leading organizations are paying special attention to IT infrastructure capabilities that can enhance their cyber resilience through capabilities such as data discovery, copy management, encryption, access control, and immutable storage, while maintaining multiple data recovery options.

For IT and business leaders, cyber resilience is all about making the right technology decisions and the right business decisions—with the goal of keeping the business operational.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com

contact@esg-global.com

508.482.0188