CISO

POINT OF VIEW

Analysis of Storage & Backup Security in the Financial Services & Banking Sector

Survey Report

CONTINUITY

INTRODUCTION

When organizational data is compromised, the last line of defense lies in the storage and backup environments. Recent years have witnessed an alarming growth in the number and sophistication of data-centered attacks – primarily ransomware[1].

The fact that so many victims eventually choose to pay the ransom gives rise to serious concerns about the market's storage and backup security maturity. Fueled by the expansive media coverage and dramatic financial repercussions of data-centered crimes, organizations, vendors, and regulators alike are in a race to identify and close the gap.

In search of structured analysis of the market maturity, challenges, and gaps – we were surprised and intrigued to discover that very little work has been done.

This extensive study – the first of its kind – is aimed at addressing the gap. This survey was conducted between June and August 2021. Our research included 200 financial services firms and banks from 45 countries – the results of which are presented below.

KEY FINDINGS

- More than two-thirds of the respondents believe an attack on their storage environment will have 'significant' or 'catastrophic' impact
- Almost 60% of the respondents are not confident in their ability to recover from a ransomware attack
- The significance of securing storage and backup systems is widely recognized by Infosec and GRC teams alike, and over two thirds of the respondents mentioned it has been specifically addressed in recent external audits
- And yet, storage and backup systems are the two lowest focus areas of organizations' vulnerability management programs
- Continuously changing priorities, organizational silos, and lack of skilled personals were chosen to be the most prominent challenges to achieving effective storage and backup security

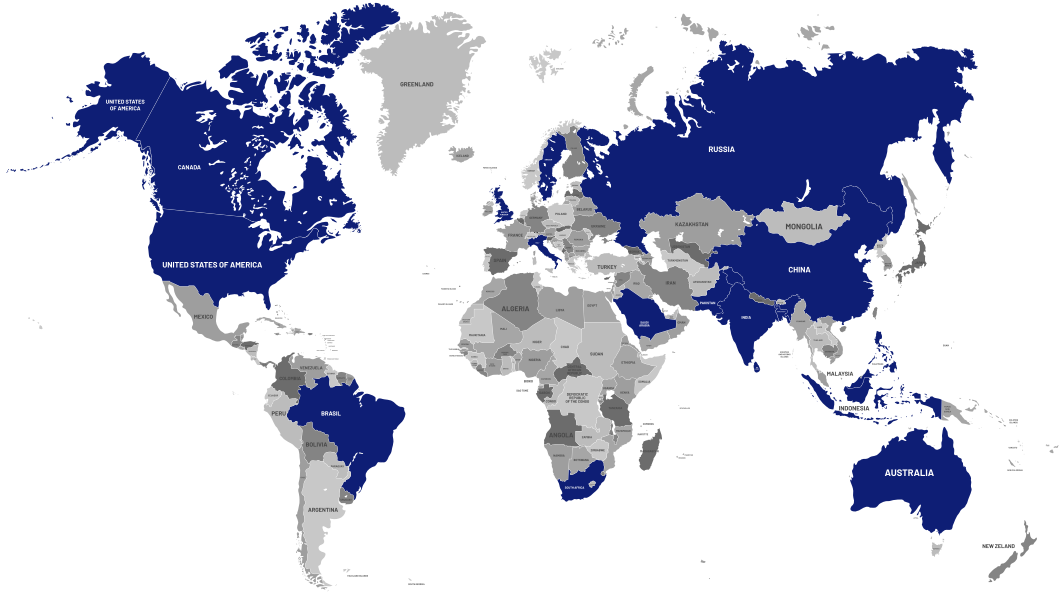
[1] Closely followed by data theft. Additional risks, that get less media coverage, yet carry grave implications to the victims, include data destruction, and malicious data tampering – sometimes aimed at attacking the victims' entire eco-system (e.g., attacks on ISVs and ISPs)

METHODOLOGY

This report is based on the results of an online survey conducted between June 10 to August 10, 2021. Among the areas covered:

- Scope and focus of organizational vulnerability management,
- Impact of storage attacks,
- Confidence level in the ability to recover from ransomware attacks, and in the security of storage and backup systems,
- What is being protected?
- How security configuration and vulnerabilities are being assessed and measured?
- Top challenges to securing storage and backup
- How mature are the organizational security configuration baselines?

The 200 validated respondents represent a cross-section of organizations from 45 countries, including USA, UK, China, Singapore, Canada, Australia, Bangladesh, Brazil, Egypt, India, Indonesia, Israel, Italy, Kenya, Malaysia, Mexico, Pakistan, Philippines, Portugal, Russia, Saudi Arabia, South Africa, Sri Lanka, Sweden, and the UAE.



Responses were grouped by topics, and the results of related questions were inspected for consistency. Some incongruities were observed that we believe could shed more light on security specialist thought processes and priorities.

Throughout this document, we have rounded up percentage values to the nearest whole number.

The survey aims to showcase how security experts in the banking (45% of the respondents) and financial services sector (55% of the respondents) view the current state of storage security. It also brings to light the challenges and opportunities and the roles and responsibilities of a security professional in the industry.

DETAILED ANALYSIS AND FINDINGS

In the following sections are more detailed analysis of key aspects of storage and backup security management, including review of participant responses and discussion of findings, as well as observations and conclusions derived from cross-referencing results, and analyzing anomalies and incongruities.

CONFIDENCE LEVEL IN STORAGE SECURITY & RECOVERABILITY

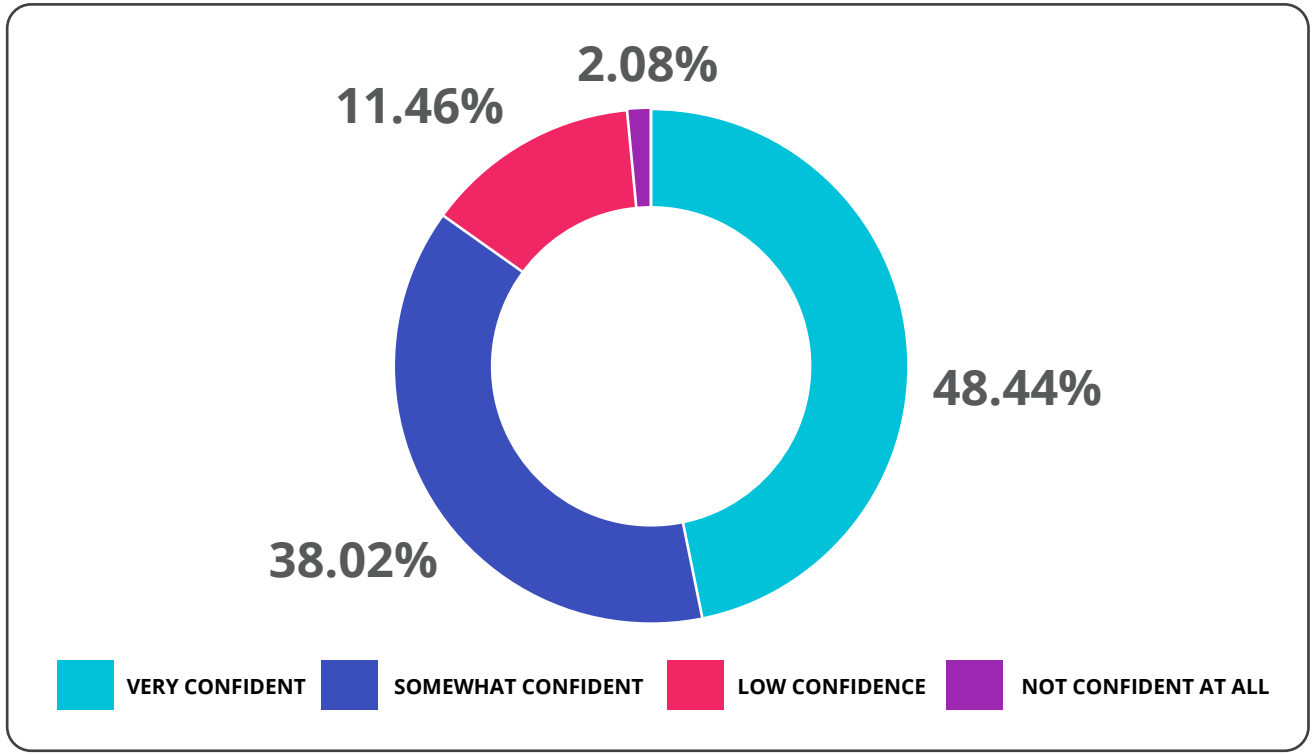
Confidence among business leaders and security staff is associated with factors such as technical capability, availability of resources and infrastructure, existing skill-sets, internal and external testing results, visibility and measurement, proven compliance with industry standards, external audit track-record, etc.

WE ASKED

How confident are you that the storage and backup systems of your organization are well-secured?

WE LEARNED

Around 52% of the respondents are not strongly confident about their storage and backup security, with a quarter of which that are significantly concerned (low or no confidence). It is interesting to note the slight incongruity with the response to the next question;

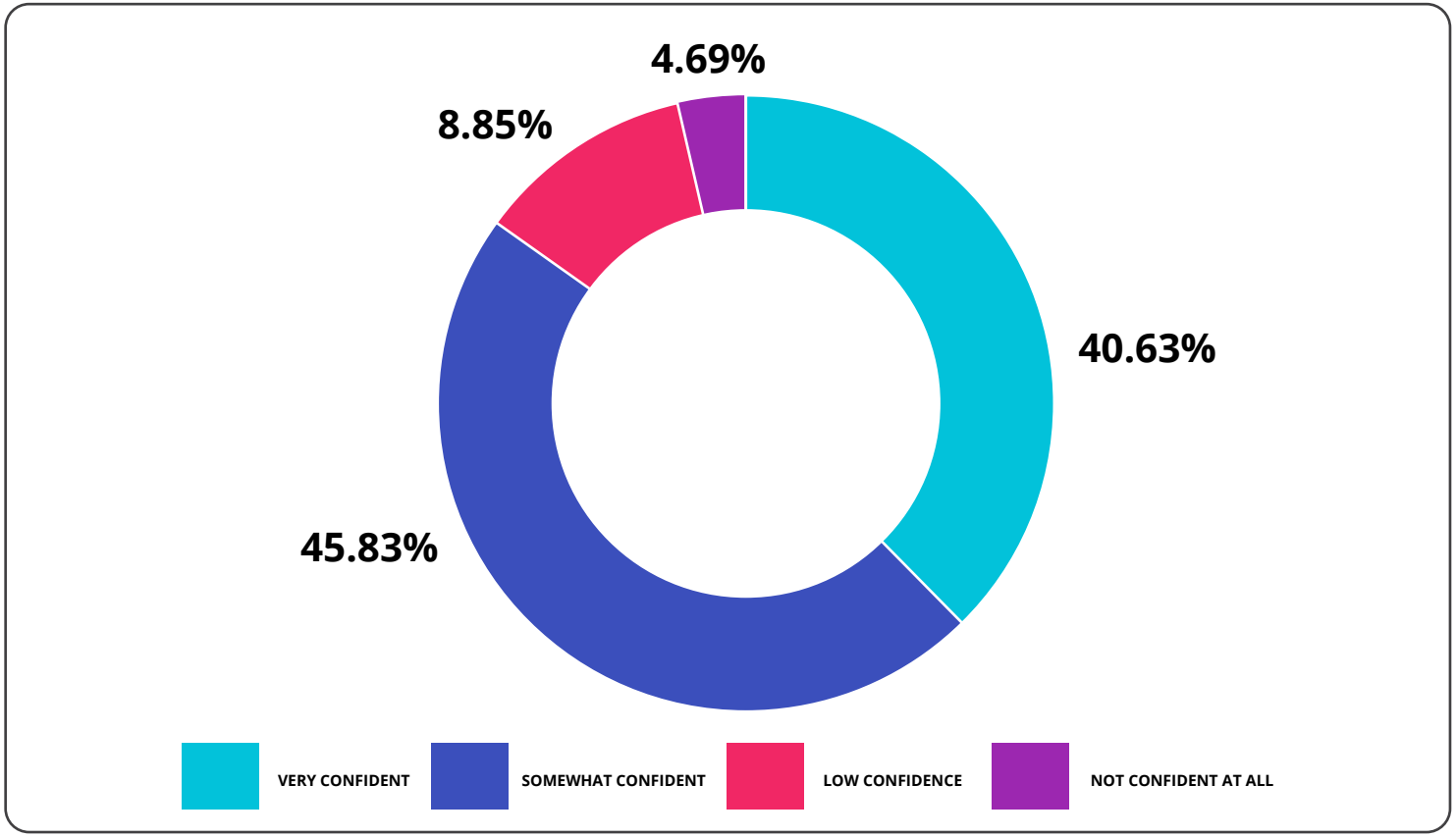


WE ASKED

What is the level of confidence you have in the organization's ability to recover data in the event of a ransomware attack?

WE LEARNED

Slightly more than 59% of the respondents are not confident they can recover from a ransomware attack. As mentioned above, it is interesting to compare this response to the overall confidence in storage and backup security. One would expect the results to be quite similar, especially since recovery from ransomware is the ultimate test of storage and backup. Yet the 20% difference in certainty suggests that the overall level of confidence in storage and backup security might be even lower than organizations are willing to admit.



IMPACT OF STORAGE ATTACKS

Data breaches, if occurred, irrespective of the vector or mode utilized, have a tremendous impact on organizations – in the form of financial loss, reputational damage, operational downtime, legal action, loss of sensitive data, etc.

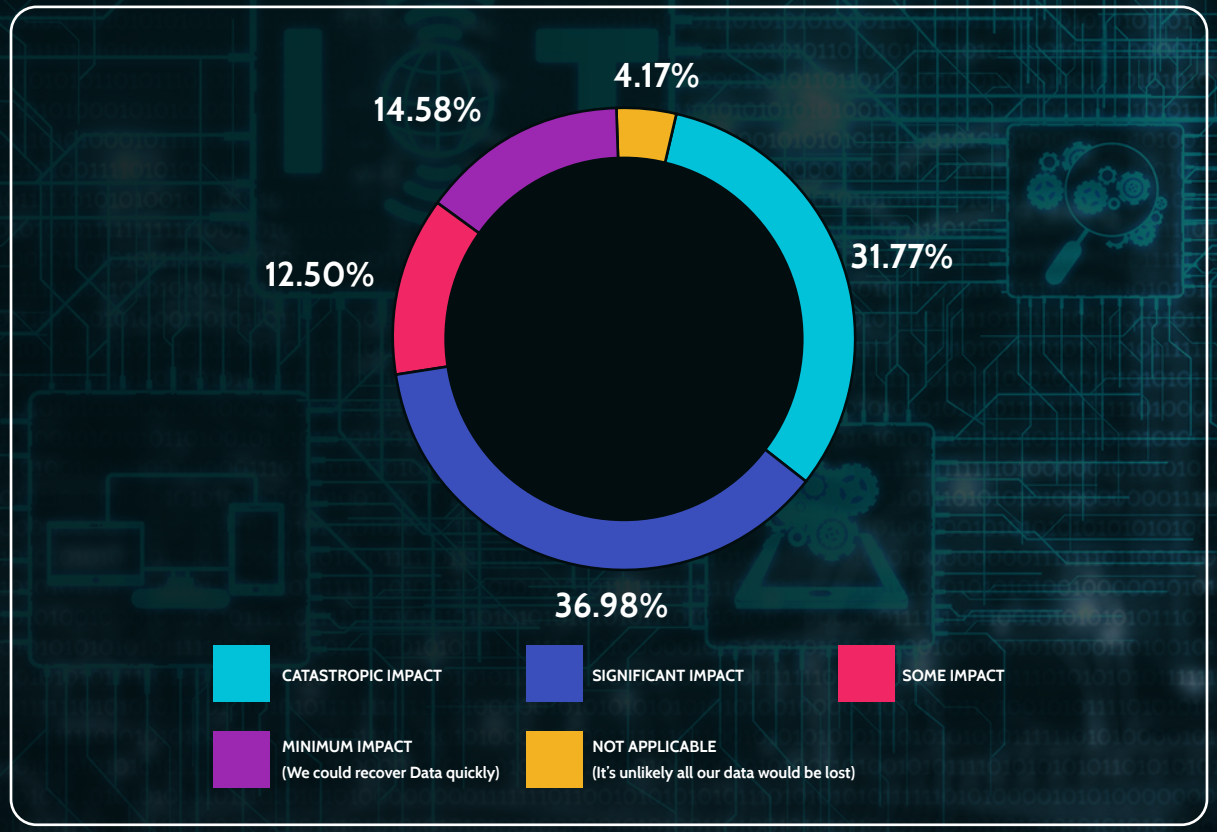
For financial and banking organizations in particular, the business value of digital data may be so high, that a well-orchestrated attack on both storage and backup could wipe away a significant amount of the organization's value – potentially affecting entire economies.

WE ASKED

What impact/ severity level would an attack on your central storage and backup systems have on your organization?

WE LEARNED

Around 69% of respondents believe that any kind of security breach on storage and backup will have a significant to catastrophic impact on their organization.



SCOPE AND FOCUS OF ORGANIZATIONAL VULNERABILITY MANAGEMENT

Storage security could be defined as the operations and procedures involved in making the storage and backup resources available to users accessing it in a secure way.

These parameters are applicable to both hardware and software components, and this survey analyzes it from a wide angle, including elements related to access control, secure communications protocols, organizational policy, data privacy, vulnerability management, configuration management, and other security aspects.

Apart from minimizing the potential security gaps through actions such as vulnerability scanning, the scope of vulnerability management should include disassembling unnecessary services, updating the operating system (including storage arrays and storage networking devices' OS), redundant storage solutions, establishing and informing principles and policies implemented in governing the network use, etc.

Cloud environments must also be part of the vulnerability management program, in order to prevent data loss and threat to information security. The scope of any vulnerability assessment and management architecture includes asset discovery, scanning for common vulnerability and exposure (CVE), establishing security baselines, prioritizing known vulnerability, threat detection, incident response plans, and complying with information security standards and regulations.

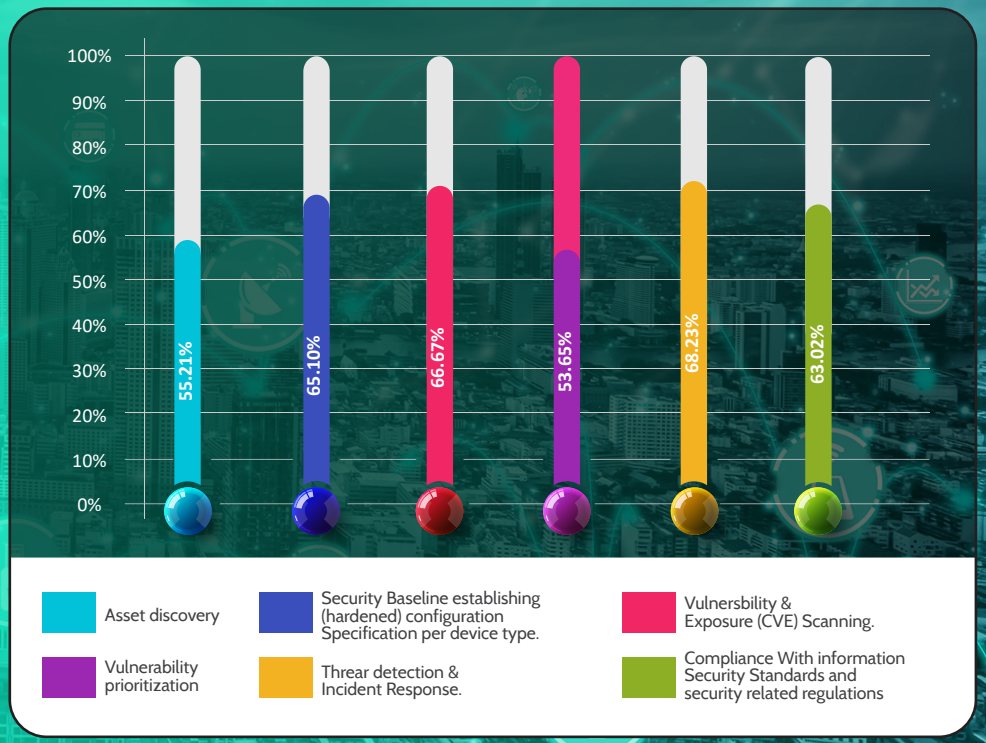
WE ASKED

What does your Vulnerability Management program include (directly or indirectly)?

WE LEARNED

Threat detection and incident response are the most widely mentioned parts of organizations' Vulnerability Management program (68% of the respondents), followed by CVE scanning (67%), and establishing a security baseline (65%).
It is interesting that asset discovery and vulnerability prioritization are the two least covered areas. With already overworked infosec and IT infrastructure teams, the constant struggle to keep track of dynamic environment changes, and the flood of identified vulnerabilities, present a tremendous challenge.
Realizing that it's not possible to address 100% of the detected issues, the lack of clear prioritization could significantly increase the chances of dangerous vulnerabilities falling in between the cracks.

[3]I.e., over a secured network with strict access controls, permitting only secured/trusted users or devices, with sufficient logging, with comprehensive change management controls, etc.



Similarly, establishing a focus area for vulnerability assessment and management process is an effective step taken towards strengthening your organization's Information Security. This process tends to provide a clear picture of existing vulnerabilities and is focused on assets such as endpoint devices, servers (such as email servers and file servers), network and associated services, databases, storage, backup, applications, etc.

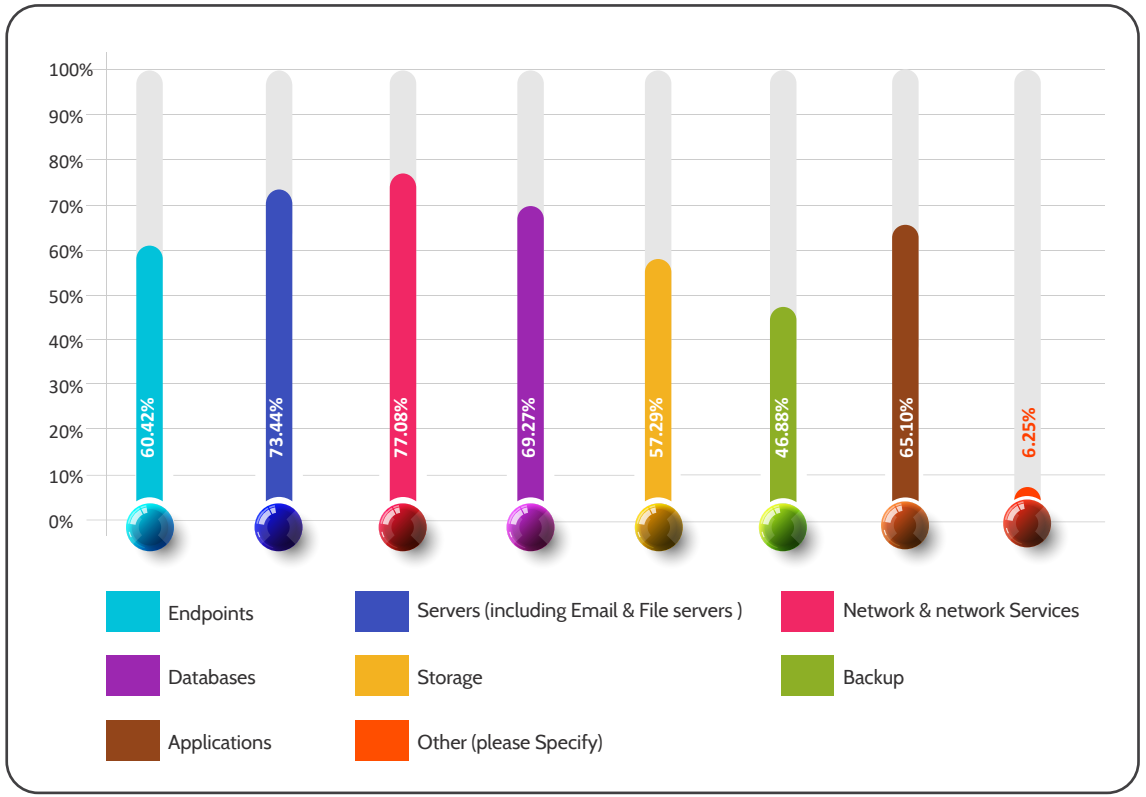
WE ASKED

What are the focus areas of your organization's Vulnerability Management program?

WE LEARNED

The top three focus areas, unsurprisingly, remain network & network services (77%), Servers (73%), and Databases (69%).

Given the criticality of Storage and backup Systems, as analyzed below (see Impact of storage attacks, and Confidence level in storage security and recoverability below), we were surprised to find storage and backup as the two least areas of focus.



CONFIGURATION AND VULNERABILITIES: HOW THEY ARE BEING ASSESSED AND MEASURED?

Data breaches, if occurred, irrespective of the vector or mode utilized, have a tremendous impact on organizations – in the form of financial loss, reputational damage, operational downtime, legal action, loss of sensitive data, etc.

For financial and banking organizations in particular, the business value of digital data may be so high, that a well-orchestrated attack on both storage and backup could wipe away a significant amount of the organization's value – potentially affecting entire economies.

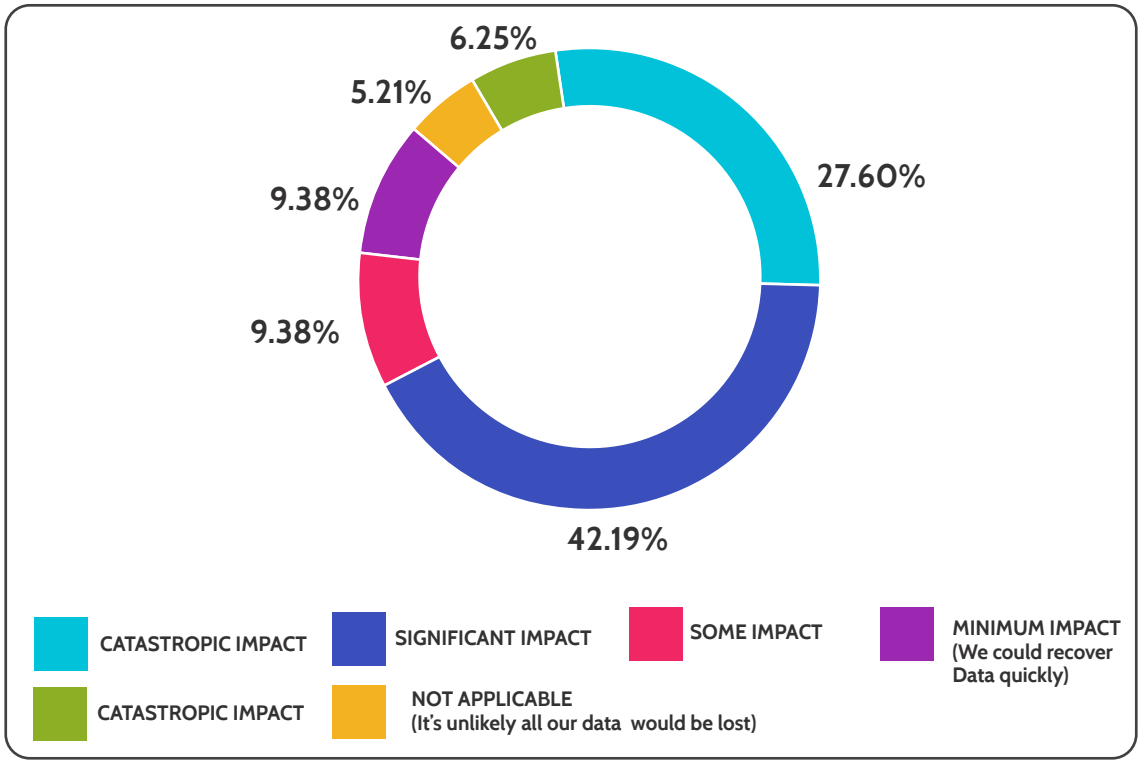
WE ASKED

What are you doing today to secure your storage and backup systems?

WE LEARNED

Continuous scanning of storage is carried out by only 42% of the respondents, and an additional 27% scan storage periodically.

The rest - 30% - rely on unstructured processes: most (around two thirds) do not currently scan storage, or cann0t tell how storage is being assessed, and the rest (around a third) relies exclusively on the IT operations teams to solve the problem, without the supervision of InfoSec or GRC.



When it comes to implementing storage and backup security, many organizations are implementing it across various elements such as block storage, object storage, file storage, server-based storage, Fibre-Channel storage networks, storage management software, storage virtualization solutions, data protection systems, backup software, and solutions, public cloud storage, etc.

WE ASKED

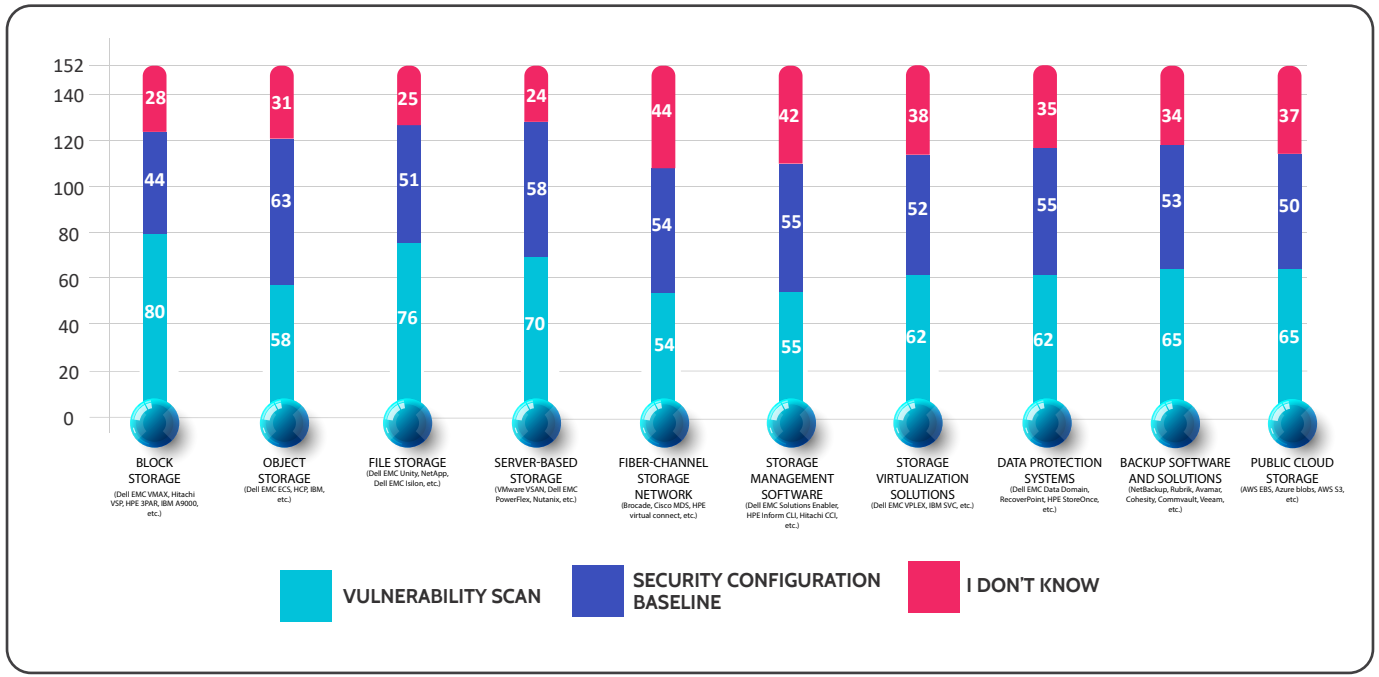
What type of storage and backup systems are covered by your infosec program?

WE LEARNED

Block and File storage, closely followed by server-based storage are the most closely inspected areas.

It is of particular interest to note that Fibre-Channel network elements, and Storage Management solutions are the two least covered areas. Not many organizations realize that gaps in the protection of those two elements could allow adversaries to easily circumvent most existing security controls! For example, it is possible to clone your core servers and export both their OS, software and data (unnoticed by virtually all IDS and DLP implementations), or even tamper with the content of key financial transaction databases, without tripping any wires at the OS or database engine level.

There is a relatively high percentage (24-44%) of respondents for each question that did not know the details of storage security vulnerability management and baseline coverage. In all other questions included in this survey, the percentage of respondents that were not familiar with the details ranged between 5-6%.



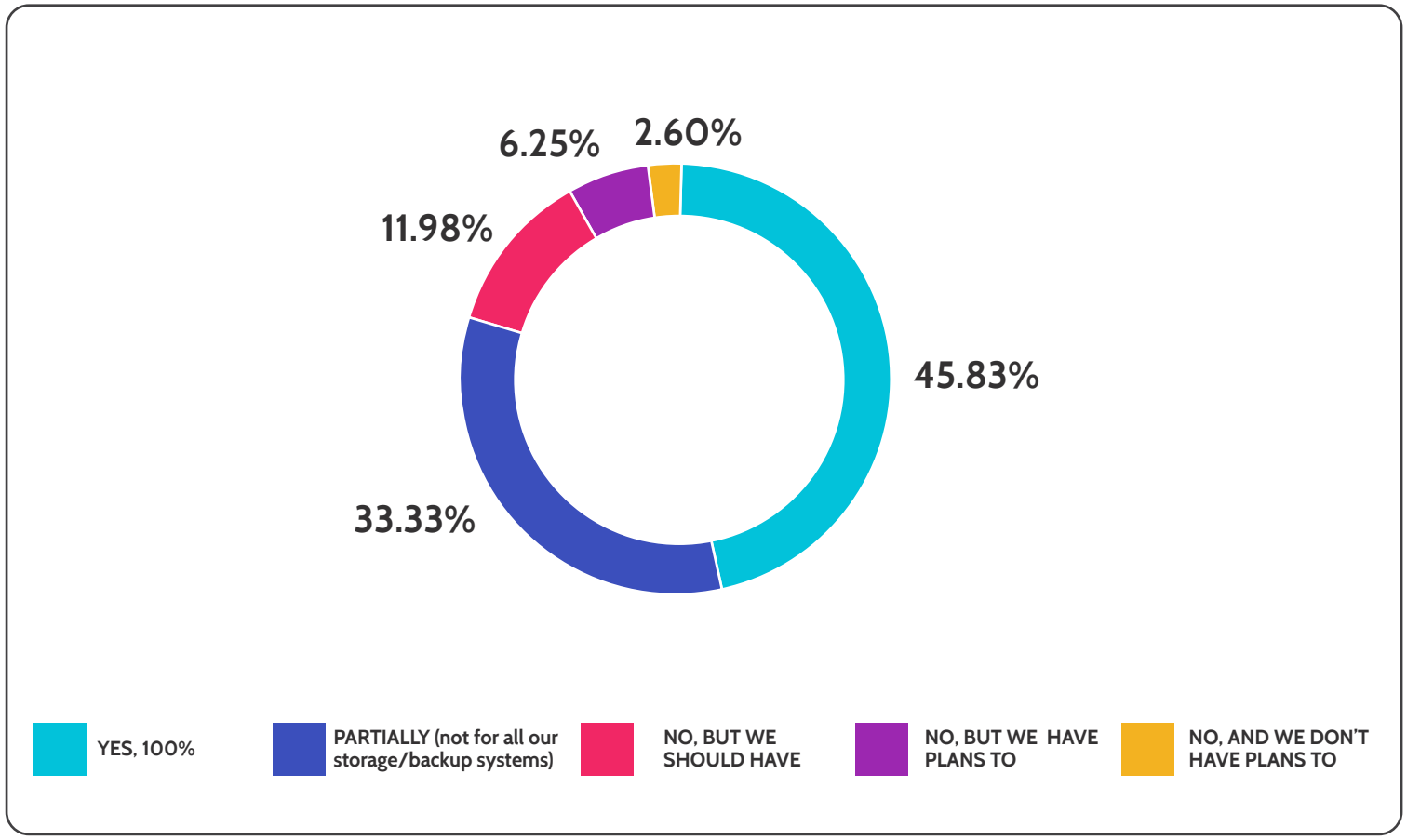
The last aspect we were interested in investigating is the comprehensiveness of organizations' security baselines, whose importance cannot be overestimated. Lack of sufficiently detailed security baselines in any given area creates a significant blind-spot that not only increases the attack surface and extends the window of opportunity for exploitation, but also leads the organization to a false sense of security.

WE ASKED

Does your organization have security configuration baseline and implementation documents defining the minimal security settings required for each data storage and backup solution in use?

WE LEARNED

Only 46% believe they have carried out a comprehensive job. Around 21% (!) do not have any form of security baselines in place, and the rest have only partial coverage.



SECURITY AUDITING

A security audit is a process used to evaluate the effectiveness of the security risk management program and to determine how well it meets industry and regulatory standards.

Financial Services is one of the most heavily regulated industries. Audits are performed both internally and externally – and tend to evolve year-over-year based on advances in technology, industry regulation changes, and shifts in the threat landscape.

Encompassing storage infrastructure into these audits involves developing storage security assessment and audit procedure as a separate initiative, which is later integrated with regular security practices. If in the past, IT audits had little explicit reference to storage and backup systems. Evidence now shows that governments and international standards organizations are paying closer attention to these fields.

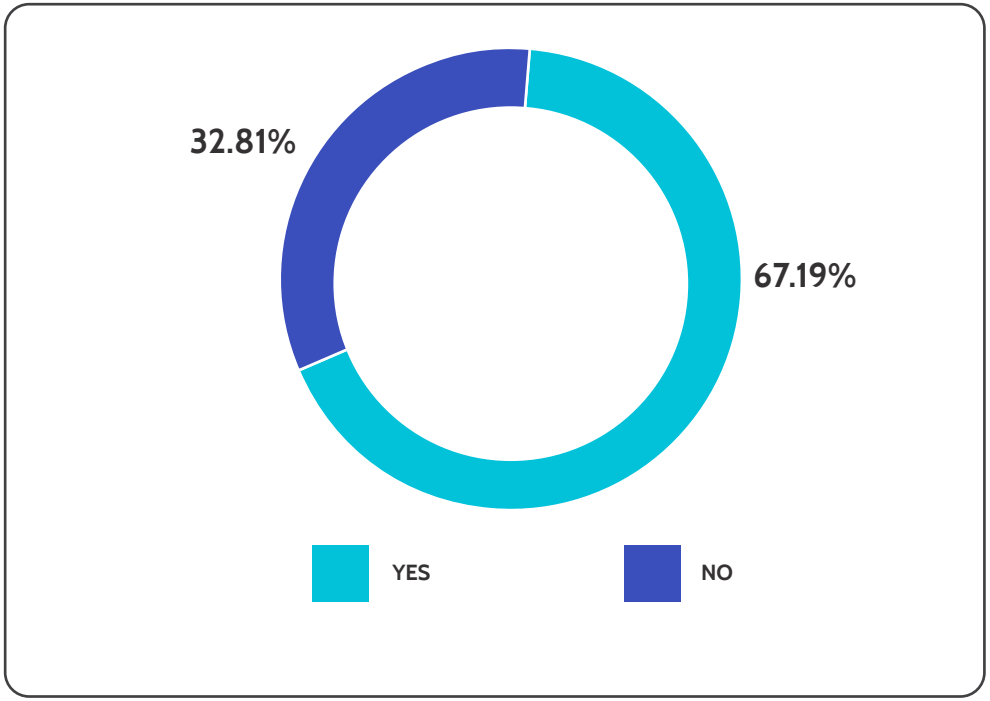
We were interested to learn how pervasive storage and backup security controls have become as part of IT auditing.

WE ASKED

Within the last 18 months, did your organization participate in any security audits explicitly addressing your storage and backup?

WE LEARNED

The majority of the respondents (67.19%) indicated that storage and backup security has been included in recent audits.



TOP CHALLENGES TO SECURING STORAGE AND BACKUP

Data storage, backup, and recovery management have always been demanding tasks, requiring detailed planning, implementation, testing and tuning.

Traditionally, little attention has been paid to storage and backup security; InfoSec teams witnessed relatively little focus from "regular" cyber-criminals (only nation-states had the means to directly attack storage infrastructure), while storage admins have held the (relatively grounded in facts) belief that adding security to storage increases management overhead and gravely impacts performance.

Both these assumptions have long become irrelevant.

Storage and backup compromise are at the heart of all current ransomware kits, and modern storage infrastructure allows tremendous amount of hardening with virtually no performance impact and with far less complexity than in the past.

Yet, as many assume (and as this report clearly demonstrates)– most organizations, especially those in the financial services & banking sector, have not yet reached sufficient maturity in terms of storage and backup security. We wanted to understand what was holding them back.

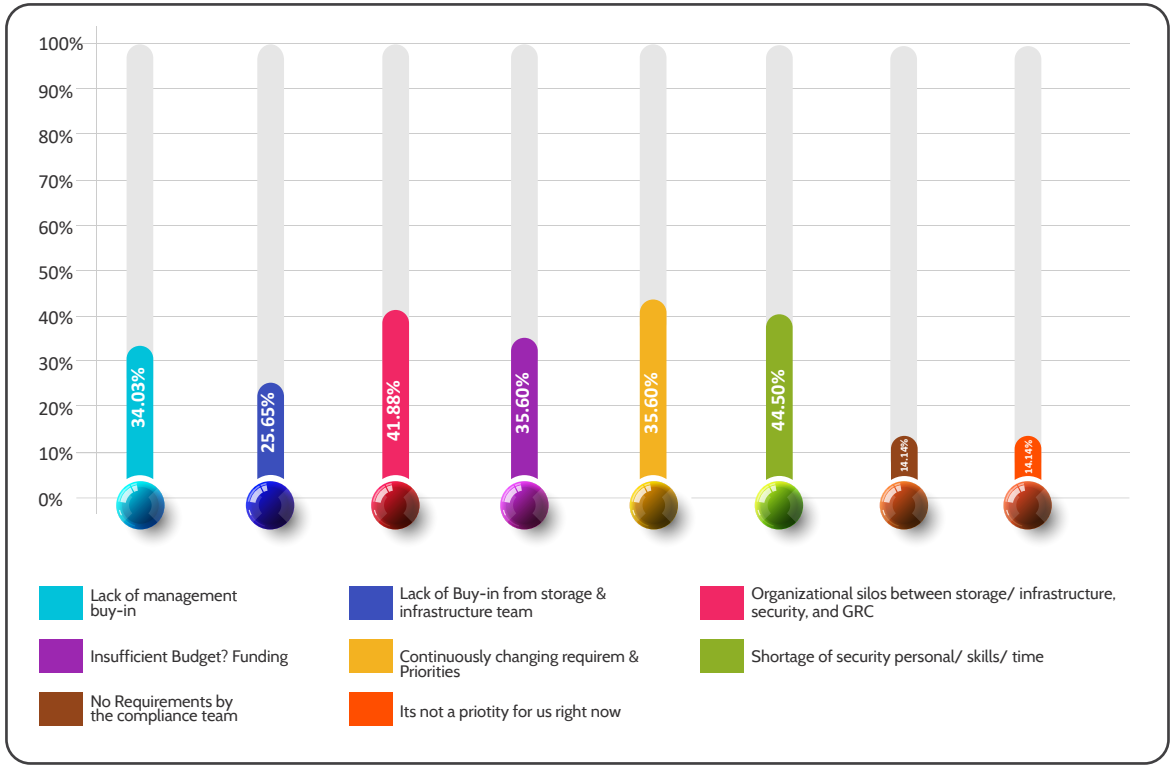
WE ASKED

What are your top challenges (e.g., barriers) in securing your storage and backup?

WE LEARNED

The top factors that slow down storage and backup security evolution include: continually changing requirements, silos within the organization (infosec, IT infrastructure, GRC), and shortage of knowledge and skills[4].

It is interesting to note that very few organizations believe that adopting storage and backup security is of low priority, or is not required by GRC groups.



[4]This is reflected not only by being the items most frequently picked up from the multi-choice list – but were also flagged by an overwhelming number of responders. Some of the lower-rating items were flagged by far fewer participants.

CONCLUSION

Storage and backup security is an evolving practice. Given how lucrative organizational data has become – and its growing business values, it is important to realize that we are all in an arms-race with cyber criminals.

The fact that so many recent data-centered attacks succeed, and the alarming percentage of organizations that have elected to pay to get their data back – rather than rely on their own capabilities, illustrates the gravity of the hour.

The honest feedback provided by participants of this survey show that there is much to be desired. Most financial services firms and banks have not yet reached a satisfactory level of storage and backup maturity.

KEY OPPORTUNITIES FOR IMPROVEMENT INCLUDE:

- Assigning higher priority to improving the security of storage and backup
- Building up knowledge and skill sets – and improving collaboration between Infosec and IT infrastructure teams
- Defining comprehensive security baselines for all components of storage and backup
- Using automation to reduce exposure to risk, and allow much more agility in adapting to changing priorities
- Applying much stricter controls and more comprehensive testing of storage security and the ability to recover from an attack. This will not only improve confidence, but will also help identify key data assets that might not meet the required level of data protection
- All aspects of storage and backup management should be covered, including often overlooked key components such as Fibre-Channel network devices, management consoles, etc.

ABOUT THE AUTHOR

CONTINUITY

With the rise in cybersecurity threats, Continuity is the only solution provider that helps enterprises protect their data by securing their storage systems – both on-premises and in the cloud. Continuity's StorageGuard complements existing data-protection and vulnerability management solutions, by adding a layer of security that prevents attackers from penetrating storage and backup systems which can result in gaining control over practically all of an enterprise's critical data.

Among Continuity's customers are the world's largest financial services firms and Fortune 500 enterprises, including six of the top 10 US banks. For more information, please visit