THE STORAGE SECURITY HANDBOOK

CONTINUITY

With all the news around data storage hacks, ransomware attacks, and immutable storage erased, it's not surprising that cyber-protected storage is getting much more attention.

One storage array is equivalent to about one thousand servers. So, protecting storage is now considered the single most important layer of defense against ransomware.

While storage is one of the most critical areas for security teams, it also happens to be one of the least understood.

This handbook provides CISOs and their information security teams with an overview of the evolution of the storage technology landscape, current security threats, and a set of practical recommendations.

CHAPTER 1

Building the Need; The Reasons for Storage Security

Vulnerabilities from within and without are plaguing data storage. Storage hardening is a low priority even as infosec professionals are in high demand and low supply. Security managers task the talent they have with OS and network hardening, leaving storage technologies vulnerable.

Security managers are under the assumption that central storage and backup systems are far too deep in their datacenter core to reach and far too obscure to pose a meaningful attack surface. This assumption has now been proven wrong by cybercriminals and insider threats. And so it's time for CISOs to close the gap.

Meanwhile, legacy perimeter security has evaporated. Mobile and remote working employees are the new perimeter. New and traditional storage technologies don't live inside the new perimeter and must do without its protections.

EACH STORAGE TECHNOLOGY COMES WITH ITS HAZARDS.

> A quick Google search will show you the open Amazon S3 buckets; there are millions of them, and the risk is dramatic.
>
> DICK WILKINSON
> Former CISO
> New Mexico Supreme Court

Cloud storage misconfigurations like these are commonplace, regularly starring in stories of significant data exposures.

Storage arrays have Operating Systems (OS), and OS vulnerabilities are routine. SAN technologies risk flaws in open-source software, vulnerable programming languages such as Java, and virtualization technologies such as software containers. Ransomware encrypts on-premise storage and backups, leaving enterprises with no alternative but to pay the ransom.

Complexity always increases vulnerabilities. Data storage is more complicated than you think. According to NIST Special Publication 800-209, Security Guidelines for Storage Infrastructure, data storage management complexities have multiplied due to a blend of traditional storage services such as block, file, and object storage and advanced storage architectures such as storage virtualization, storage architectures for virtualized servers, and cloud storage. The greater the complexities, the more the configuration errors and security threats.

Now storage teams must return to fix errant configurations and manage realized risks from security threats. They can't do it alone.

You care about your organization's most precious data, safeguarding it in transit and use. Networks, applications, and devices remain secure because of you. But the same data lives at rest, too, in largely undefended storage systems.
Storage may seem relatively minor in your IT stack, but there are other ways to consider its size.

The world's data reached about 59 zettabytes last year, according to Statista. Storage will grow to meet demand as data multiplies exponentially. Statista expects global spending on data storage units to exceed 78 billion U.S. dollars this year.

Size isn't the best measure of the criticality of storage. Let's compare storage to the human heart. The heart is modest in size but pumps life-giving blood throughout the body. So, storage houses critical high-risk data that feeds your applications and devices. Just as shooters aim for the heart, so criminal hackers target data where it lives. If you let cybercriminals leak data from storage, they can sell it or give it away. Ransomware encrypts data in storage, cloud storage, and backups, which could kill the company.

IT'S TIME TO STOP PUSHING STORAGE SECURITY OFF AS SOMEONE ELSE'S RESPONSIBILITY.

> There are gaps in the roles and responsibilities between the security and storage/infrastructure teams. Storage has been a grey area; nobody owns it.
>
> SUNIL VARKEY
> Former Global Head of
> Cyber Security Assessments
>
> HSBC

Someone has to own storage. IT security can't account for all security if no one on the team owns storage security.

CHAPTER 2

Defining the Risks: Where Hackers Get In

In chapter 1 of this handbook, we discussed the importance of securing storage and backup infrastructure. In this chapter, we will further analyze the risk, show how storage attacks can happen, and discuss the lagging industry maturity - most organizations do not do enough to secure their storage.

Your organization's data is a lucrative target for hackers. Whether to exfiltrate sensitive information, to demand ransom, to commit fraud, or simply to cause harm – a successful attack could be extremely damaging.

> You have to remind your board, that it can take 20 years to build a strong reputation in your industry. It can take five minutes of a cybersecurity event - and enough press - to tear it all down.
>
> **ENDRÉ JARRAUX WALLS**
> CISO
>
> Customers Bank

Unlike traditional data-centered attacks that target endpoints and servers in order to compromise files; modern attacks also focus on storage and backup infrastructure – which many organizations do not secure properly.

A successful compromise of those layers will enable attackers to not only inflict more severe damage, but to do so completely "under the radar". Among the risks of such attacks are:

- The ability to duplicate sensitive environments (e.g., Active Directory, protected databases, your source code repositories), investigating them for weaknesses and performing reconnaissance - in isolation, without tripping any wires
- The ability to destroy not only data, but also its backup copies – to completely prevent recovery
- The ability to commit fraud by directly manipulating the storage plane, without the need to compromise operating systems or database servers, thereby leaving no trail
- The ability to bypass software supply chain (internal or external)

A new research report about the state of storage security portrays a grim picture. Most organizations do not do enough to secure their storage infrastructure, and the average storage device or service (e.g., a storage array, a Fibre Channel Switch. or Virtual SAN) has 15 security misconfigurations, out of which 3 are of high or critical severity.

The report outlines both the most common issues, as well as ones which are less prevalent, but nonetheless particularly lethal. As it turns out, the storage attack surface is much wider and deeper than most organizations expect.

It is tempting to think that storage security concerns could be solved by patching the clients (Host Operating Systems), and making sure there's a backup solution in place.

Regretfully, this is just the tip of the iceberg. Storage infrastructure could be breached in a wide array of exotic ways:

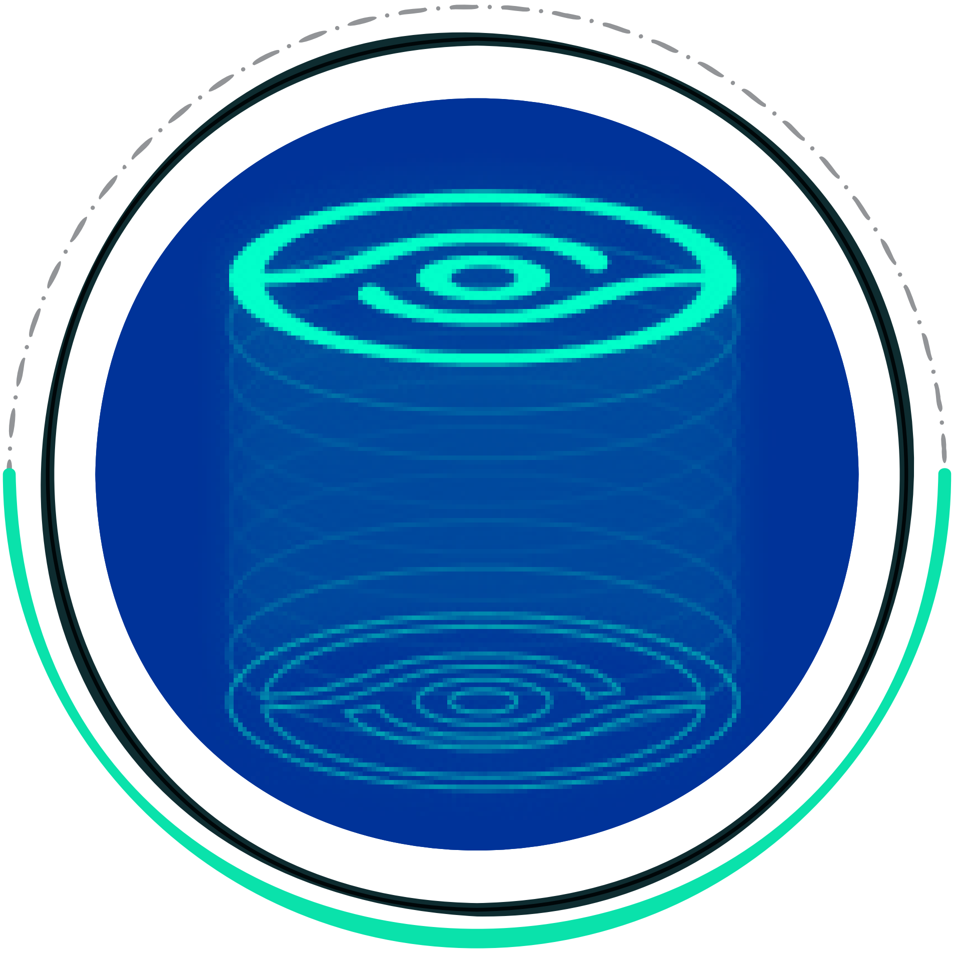
- Through the protocols used by clients and storage devices
- Through management consoles
- Through local admin APIs or control endpoints each device provides (which are often not hardened)
- By taking advantage of weak storage security hygiene:

- Not closing default device accounts, using local accounts instead of centrally managed ones
- Not restricting access to sensitive data (such restrictions should be done end-to-end: at the storage device, the network, and client level, using strong authentication)
- Not securing admin sessions
- Poorly configured (or completely overlooked) encryption
- And so much more

NIST's Special Publication (SP) 800-209 "Security Guidelines for Storage Infrastructure" is a great place to start learning more about storage security.

Here are a just a few examples of how criminal hackers can exploit poorly secured storage and backup environments:

- Finding a weak spot in your environment to discover the IP address of your Domain Controllers or DNS servers. If your storage is not hardened, they can utilize storage APIs (or hijack insecure admin sessions, exploit unpatched storage CVEs, etc.) to find out which storage objects (e.g., LUNs, Shares) are used by those services, and then further use the APIs to create a copy. Copies can be mounted on unmonitored development servers, or even "smuggled" outside of the organization in a variety of ways (e.g., OneDrive, public S3 buckets, …)
- They can find out how data is backed up, and – if administration planes are not sufficiently segregated – destroy the backups (e.g., array-based snapshots, disk and tape copies, etc.) before encrypting your data for ransom.
- Even if your backups are secured (and that's a big "if" – as the research report indicates) – without sufficient isolation of duties, they can "poison" any future backup (e.g., modify the backup job, remap backed up LUNs, etc.)
- They can map volumes used by critical servers (e.g., source code, databases. build environments) to additional compromised servers, and read or modify content (e.g., financial data, personal information) "out of band" without tripping any alarms
- They can "kill" an entire storage array (including its snapshots) crippling hundreds of servers for days



CHAPTER 3

Six Tips To Secure Your Storage Now

In chapter 1 of this handbook, we discussed the importance of securing storage and backup infrastructure. In chapter 2, we analyzed the risks, watched storage attacks progress, and discussed lagging industry maturity. Most organizations do not do enough to secure their storage. In this chapter, we'll provide practical guidance for improving storage security.

The cost of a data storage breach could overwhelmingly exceed the investment in a storage security framework and controls (we will cover financials in more detail in part 4). Data-centered attacks are growing more frequent and intense. You can expand your framework to encompass storage assets and add controls specific to your unique needs. The more you define and enforce detailed security policies, the more you reduce your risk.

> The hackers are after our crown jewels: our data. In a bank, data is money. This is why I'm a big believer in securing storage.
>
> ERDAL OZKAYA
> Former Regional CISO
>
> Standard Chartered

If you're taking your first steps, we urgently recommend getting to know prominent storage security guidelines and frameworks. Examples include the NIST Security Guidelines for Storage Infrastructure (published 2020), ISO 27040 (published 2015), and SNIA's storage security publications.

Here are 6 actions you can take now to protect data in storage and backup:

1. Steer a culture that breaks the silos between security and storage teams. Security teams often lack a good understanding of storage capabilities, protocols, and the attack surface. Storage teams often adopt a naïve approach to security. They assume it complicates storage management (somewhat true) and that security and performance are contradictory (valid years ago, much less so now). A good first step could be to perform a one-time joint audit for storage security.

2. Build safeguards into your storage security processes and practices. Start by creating secure storage designs, implementations, and management procedures. Walk yourselves through the storage lifecycle from technology inception through security updates and patches to retiring storage devices.

3. Raise your security baseline to include identity and access management controls that separate administration within and between different data-planes (such as primary storage, backup, and DR), business functions, and environments (such as production, development, and testing). You can bake security baselines, guidelines, and quality controls into your IT management DNA and apply them with every new storage initiative.

4. Deploy and inventory storage in adherence with your baseline security.

5. Monitor and measure change against your baselines 24/7 to make sure you neve deviate from them.

6 Expand your incident response and recovery plan to cover storage, using metrics on the likelihood and severity of incidents as they apply to your business. (Use available data to benchmark your environment against other organizations for reference.) Run tabletop exercises to decide how to recover from scenarios such as these:

- An attack wipes out a large storage array supporting thousands of servers, VMs, and operating system instances. The onslaught has erased your data and storage configurations. You must rebuild the array, create the LUNs, and remap them to those servers and data stores.
- A criminal hacker deletes your SAN settings, including zoning and masking. It took years to design and roll out those configurations. Now you must fall back on your documentation and backups. Do you have automation in place to recover quickly?
- An unidentified strain of ransomware targeting a zero-day vulnerability in SAN storage software has hit your storage plane. The ransomware targets primary storage and backups. You need to keep secure backups so you can recover once you stop the attack. You must defuse the malicious software as soon as possible.

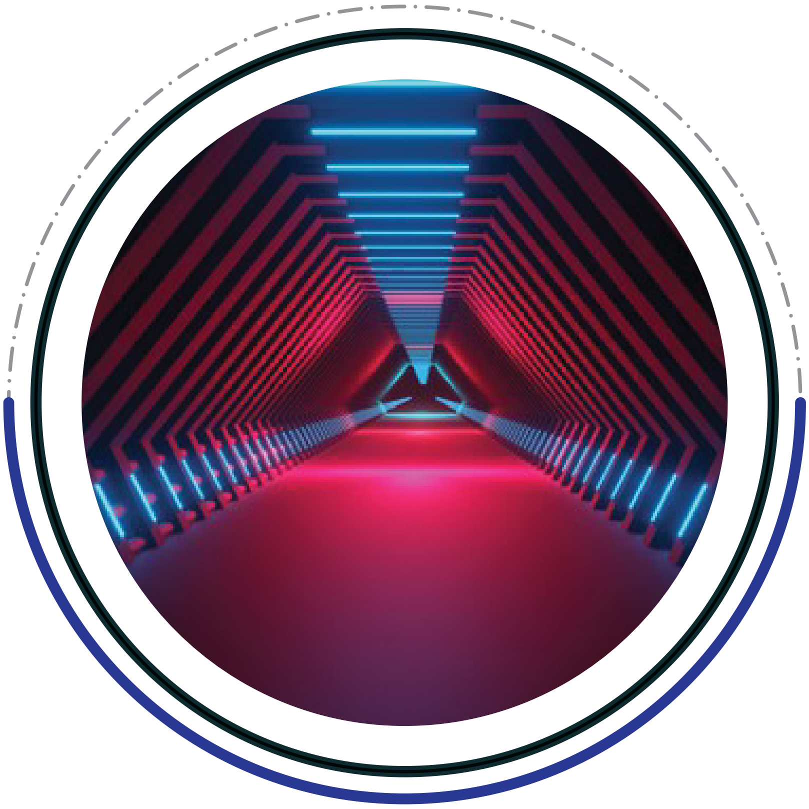
NOW'S THE TIME TO GET ON THE STORAGE SECURITY FAST TRACK!

> You need to have governance and an active program to secure your storage management layer
>
> MARC ASHWORTH
> CISO

FIRST BANK
Member FDIC

If you need help, reach out to consultants who can find your gaps. They can map your infrastructure and conduct a one-time audit to get you on your way.

Understand that automation is your best friend for curtailing errors, costs, and person-hours. It's best to bake automation into provisioning, validation, and auditing. Consider automation that validates your configurations against your security baselines.



CHAPTER 4

Making the Business Case for Securing Storage and Backup

In chapter 1 of this handbook, we discussed the need to protect storage and backup systems. In chapter 2, we provided more details on the risk and showed how hackers can get in. In chapter 3, we talked about improving your storage and backup security posture. In this final chapter, we'll cover the economics of storage security.

Now that you know costly storage attacks happen in the wild, I'm sure you realize that the risks are significant. Criminal hackers can invade storage and do whatever damage they want to your data and systems if you don't secure them sufficiently. But there is much that you can do to plug the holes and safeguard your most valuable asset: your data.

It takes an investment of time and money to reach storage security nirvana. To justify the price tag to yourselves, the CFO, and the CIO, you must do the following:

- Do your due diligence to calculate the storage security price tag or price range and
- Measure the price against the costs that come with breaches and the likelihood of a storage attack. Here are some of the many disconcerting risks:

The death of your business when you lose your core data and your backups with no way to restore them

The costs of extensive breach notifications and public awareness of your failing

Reputational damage

Falling stock prices

Loss of customer confidence, customers taking their business elsewhere

Costs for premium credit and identity theft protection for affected consumers

Fines and penalties:

- From the SEC, the PCI Council, Health and Human Services, and other regulators for non-compliance on PII, PHI/HIPAA-HITECH regulations, the GDPR, the CCPA, and financial data.
- From regulators and merchant banks enforcing SOX, PCI-DSS, and other financial services requirements
- Joint, cross-state, HIPAA lawsuits in federal court
- Lawsuits from consumers and business customers
- Financial judgments and civil penalties

> Storage is where our core data is stored. And so, vulnerability management, configuration management, and ensuring a strong policy around the governance of all storage devices are absolutely critical.
>
> **SUNIL VARKEY**
> Former Global Head of Cyber Security Assessments
>
> HSBC

You're lucky or living with blinders if you believe you never had a breach and never could. Let's say that you're right. There are costs for neglecting storage security as it comes up in your next audit. Many organizations report that auditors are asking tough questions – and that failing to provide convincing answers can result in severe penalties. These questions include:

- Can you produce an inventory of your storage devices?
- Can you show me your evaluation of the requirements to secure storage devices and backups? Auditors request details about storage protocol vulnerabilities (IP and Fibre Channel), encryption, CVE management, protection of backup copies, utilization of ransomware and DoS prevention features, and more.
- Can you show me the decisions you made based on your evaluation?
- Can you share your storage security plan and actuals?
- What are your controls for storage system authentication and authorization?
- Do you know who may access what systems with what rights and privileges?
- Does your incident response plan cover in detail how you recover from storage-related attacks?

> Securing central storage is an area that I personally have been harping on about quite a bit, and I've been telling people that just aren't aware of how much risk exits in storage environments. It's your responsibility. You, the CISO,have to take some responsibility here. I get really emphatic about it. And then I just give them a few of the horror stories.
>
> DICK WILKINSON
> Former CISO
> New Mexico Supreme Court

Up to 30 percent of financial services organizations are aware and concerned about new audits that include storage security requirements.

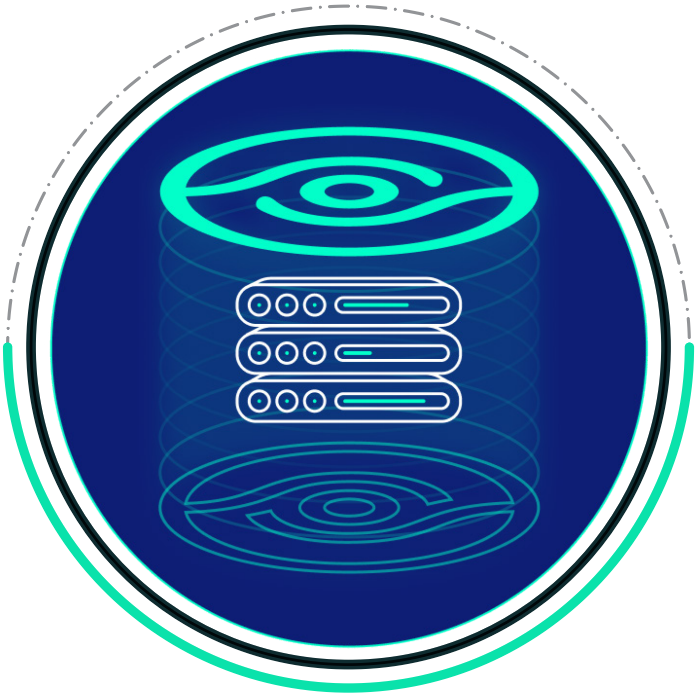
CFOs and CIOs find financial costs, opportunity costs, and ROI relevant. Share your new list of breach costs. Present the audit failure costs. Show your numbers in big-picture expenses and have the subtler details ready when they ask you for them. Underline the differences between paying for security now and paying all these other costs plus the cost of security later.

There is ROI in the CFO's peace of mind for not sticking their head in the sand and pretending there are no storage threats or penalties. There is measurable ROI in the competitive advantages you gain by marketing your security savvy as a selling point, along with your organization's products and services.

You have your storage security intelligence. You can justify the investment. Now's the time to take this business case to your CIO and CFO. Enable your enterprise to protect itself and prosper!

See how secure your storage systems are with this one-time assessment. And get recommendations on resolving any risks that are identified.

Book your Storage Risk Assessment



CONTINUITY