5 CRITICAL STEPS TO IMPROVE YOUR ORGANIZATION'S CYBER RESILIENCE

COHESITY

RESILIENCE EVERYWHERE

INTRODUCTION

The rise in ransomware attacks and their increasingly severe impacts reveal an uncomfortable truth. Even with substantial investments in prevention, these measures alone aren't enough to counter today's threats.

Like it or not (and we don't), cyberattacks aren't going away. And they'll never stay the same—not in frequency, severity, or scale.

So that's the bad news.

Now for the good news. There's a proven playbook to improve cyber resilience, and organizations like yours are using it to rethink their approach and enjoy better outcomes.

In this eBook, we present this playbook as a five-step progression towards cyber resilience. By taking concrete actions across all five steps, you'll align with best practices in cyber response and recovery. You'll also see substantial benefits in terms of security, cost savings, and reduced risk.

SOME QUICK BACKGROUND

Despite greater awareness of cyber threats like ransomware, cyberattacks continue to cause tremendous operational, financial, and reputational damage. In fact, they're the number one threat to businesses globally.

The financial toll is real:

$540,000
lost for each hour of downtime[1]

US$1B+
in ransomware payments annually[2]

The State of Ransomware 2024 from Sophos[3] includes equally sobering statistics:

Of the 59% of organizations surveyed that were hit by ransomware in the last year, **94% said attackers targeted their backups,** and **57% of those backup compromise attempts were successful.**

Plus:

- **70% of attacks resulted in data encryption**
- **$2M on average was demanded in ransom**
- **34% of organizations took more than a month to recover**

The time for new and more effective strategies, capabilities, and solutions is now.

[1] Splunk, The Hidden Costs of Downtime: The $400B problem facing the Global 2000: https://www.splunk.com/en_us/pdfs/gated/ebooks/the-hidden-costs-of-downtime.pdf

[2] Chainalysis, Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline, 2/7/24: https://www.chainalysis.com/blog/ransomware-2024/

[3] Sophos, The State of Ransomware 2024: https://www.sophos.com/en-us/content/state-of-ransomware

TWO REASONS CYBER RESILIENCE CAN BE ESPECIALLY CHALLENGING:

1. Cyber recovery is not like disaster recovery.

Even if your organization has solid disaster recovery processes in place, you can't rely on these same processes to recover from cyberattacks.

In a disaster, whether a fire, flood, power outage, or even a misconfiguration, you can quickly do a root cause analysis to figure out what went wrong. In a cyberattack, hundreds of things may have transpired that will require thorough investigation and remediation—plus, you have an adversary actively undermining your recovery efforts and pressuring you to pay ransom.

2. Even savvy organizations and experts may underestimate how destructive a ransomware attack might be.

You may assume that trusted systems can help you get back online or be counting on data and evidence to help you know what happened.

But in a cyberattack, the very systems you rely on to investigate the incident may be down—or they may have been evaded or compromised. When good data intermingles with bad, the road to recovery will be longer and more difficult. That's why we see lots of smart organizations still struggling with fast, clean, and confident recovery.

LET'S LOOK AT THE **5 CRITICAL STEPS** TO IMPROVE CYBER RESILIENCE

Think of this as a practical blueprint where each step you take gets you further along the progression.

STEP ONE

PROTECT ALL DATA WITH GLOBAL GOVERNANCE.

It may sound simple, but plenty of organizations still don't take this crucial first step—and data sprawl is likely to blame.

Organic data growth has led to fragmentation and silos, significantly widening the attack surface and leaving organizations more exposed than ever. At the same time, managing and securing data at scale places a growing strain on operational efficiency.

This combination—more data in more places, with less ability to manage it efficiently—has created the perfect conditions for attackers to wreak havoc.

NOTABLE BENEFITS OF STEP ONE

- ☑ **Enhanced security**
- ☑ **Reduced risk**
- ☑ **Improved compliance and governance**
- ☑ **Lower costs and improved ROI**
- ☑ **Increased IT efficiency**

KEY ACTIONS TO IMPLEMENT STEP ONE

1. Adopt a modern data platform that supports 1000+ data sources, including:

- Virtual machines (VMs)
- SaaS applications
- Databases
- NAS environments (unstructured data)

2. Make sure your platform runs across on-premises, cloud, and SaaS environments.

Because you have data all over the place, your platform should have flexible deployment models unified by a common UI and APIs.

3. Simplify operations with an intuitive UI.

When your UI is easy to use, you can have a relatively small team running a giant estate—and running it well. Our customers enjoy superior operational efficiencies with a single UI and set of APIs for automating workflows on our platform.

4. Get strong storage compression.

You'll want to use a platform with strong data compression. This will yield substantial savings when running at petabyte scale. We have a unique file system that's the industry standard. Really strong storage compression gives a lower TCO.

STEP TWO

ENSURE BACKUPS ARE ALWAYS RECOVERABLE.

Attackers target backups. They know if they can impact this last line of defense, you'll be far likelier to pay ransom as your organization will have no other recourse.

And while it might be nice to assume a modern platform guarantees recoverable backups out of the box, this isn't quite true.

You need to take several actions to make it more difficult for attackers to get access, and for your organization to recover clean backups if they do.

NOTABLE BENEFITS OF STEP TWO

- ☑ **Faster and more secure recovery**
- ☑ **Stronger protection against attacks**
- ☑ **Audit readiness**
- ☑ **Zero trust alignment**

KEY ACTIONS TO IMPLEMENT STEP TWO

1. **Harden your platform by configuring powerful features like:**

- Multifactor authentication (MFA)
- Immutability (so data can't be altered or deleted)
- Role-based access control (RBAC)
- Separation of duties (dividing critical tasks among different individuals)

2. **Implement a cyber vault**

With an air-gapped copy of your most important data and adherence to the **3-2-1-1 backup rule** (three copies of data, two different media, one offsite, and one immutable), you'll always have a copy of your data available in case of emergency.

We at Cohesity also provide an advanced key management system, so we can still give our customers access to their data in an attack.

This access ensures backups are always recoverable.

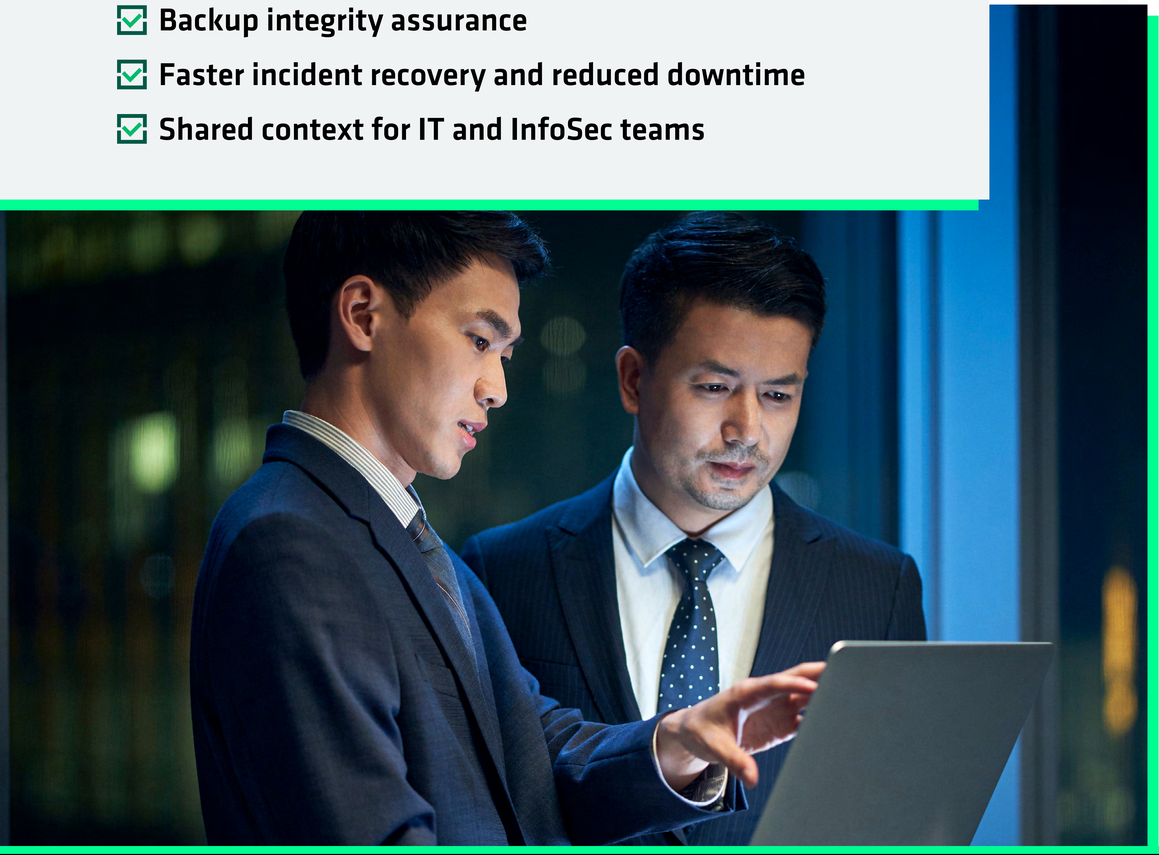
STEP THREE

DETECT AND INVESTIGATE THREATS.

This step relates to the combined power of threat scanning and threat hunting capabilities.

NOTABLE BENEFITS OF STEP THREE

- ☑ **Early threat detection and mitigation**
- ☑ **Backup integrity assurance**
- ☑ **Faster incident recovery and reduced downtime**
- ☑ **Shared context for IT and InfoSec teams**



KEY ACTIONS TO IMPLEMENT STEP THREE

1. Be proactive by regularly scanning for threats in your backups. Think of this proactive **threat scanning** like practicing consistent hygiene. It'll help you:

- Root out any changes as quickly as possible
- Identify malware or other vulnerabilities

2. Initiate **threat hunting** capabilities when seeking specific threats. Our curated threat feeds and integrations with the security ecosystem vendors in our Data Security Alliance, including CrowdStrike, Palo Alto Networks, Cisco, and more—means you get the combined benefit of their collective wisdom with the data we can bring to these systems.

Your InfoSec and IT teams will also operate with the same set of information.

As we've helped customers recover from cyberattacks over the years, native threat scanning and threat hunting capabilities must be part of your data platform.

Why? Because other security systems may be disabled or otherwise offline when you're under attack.

STEP FOUR

PREPARE, PRACTICE, AND RECOVER FROM INCIDENTS.

When it comes to "prepare," you're already in good shape if you've done steps 1-3 above. You've gotten your platform stood up, gotten it hardened, and extended your deployment with a cyber vault.

You've also had some good practice with regular threat scanning and threat hunting. Well done!

Here in step four, you take preparation to the next level by practicing your response and recovery processes. After all, you don't want to be doing this for the first time in an actual attack when your systems are down and the pressure is on.

You may be thinking, "Bringing everything back online is a time-consuming process. How can I regularly test and still do my day job?"

NOTABLE BENEFITS OF STEP FOUR

- ☑ **Faster and safer recovery**
- ☑ **Improved RTO**
- ☑ **Lower risk of reinfection**
- ☑ **Reduced disruption and financial risk**

This is where orchestration comes into play.

With orchestration, you can automate response and recovery workflows and start to "rehearse" bringing your systems back online after an attack. These rehearsals will help you get good at response and recovery, and orchestration can help you fine-tune those practices with less manual effort.

One key example of automation at work: Our clean room solution allows you to spin up a separate environment where you can conduct forensic analysis and dive deep into infected bits of data, understand what transpired, and then eradicate the attack artifact so you can be sure your systems are safe to recover. This approach offers a unique blend of speed, automation, and powerful forensics to help incident responders collaborate with IT teams. The result: faster cyber response and recovery.

In this step, you'll also work with Cohesity CERT (Cyber Event Response Team). These experts will help you respond to and handle incidents, from sophisticated ransomware and data breaches to targeted attacks. You'll never have to go it alone.

KEY ACTIONS TO IMPLEMENT STEP FOUR

1. Practice with orchestration and rehearsals
- Automate your response and recovery processes
- Conduct recovery rehearsals to refine your response plans

2. Use a clean room
- Spin up a separate, secure environment for forensic analysis
- Identify and eradicate threats before restoring your systems

3. Get expert support
- Contact Cohesity CERT when you're under attack

STEP FIVE

REDUCE YOUR RISK FROM DATA THEFT.

In addition to ransomware gangs getting worse, you simply have more data to manage—on-prem, SaaS, cloud, edge—than ever before. Everyone's always thinking, "Hmm, what do I have in that unsecured S3 bucket that no one knows about or is keeping tabs on?"

In addition to unsecured S3 buckets, hidden risks may also include orphaned databases, exposed credentials, and more.

Proactive measures like Data Security Posture Management (DSPM) and data classification can help reduce these risks.

NOTABLE BENEFITS OF STEP FIVE

- ☑ **Enhanced data visibility and classification**
- ☑ **Proactive risk identification and mitigation**

KEY ACTIONS TO IMPLEMENT STEP FIVE

1. **Find out what data is where**

- Scan your environment and assess what data is where and what protection level it has. The whole class of tools with DSPM makes this possible.
- Understand what may be in your backup estate and make sure it's protected the right way with our full featured integrations with some of the best vendors in the industry, including Cyera and BigID.

2. **Assess what may have been impacted in a breach or what may have happened in a case of data exfiltration**

- Get the right coverage you need and reduce your risk with the data classification built into our products.
- Answer quickly when there's an incident and lawyers ask: What data was impacted? How sensitive is it? What's our risk? How many customers were impacted? What types of records were affected?

CONCLUSION

You now understand the 5 critical steps to improve your organization's cyber resilience—and have the practical information needed to implement these steps in your environment.

We at Cohesity are uniquely positioned to guide you along this progression so you can have the strongest cyber resilience possible.

For further reading on recovering from ransomware securely and rapidly, we recommend:

"HOW TO FORMULATE A WARTIME RESPONSE TO DESTRUCTIVE CYBERATTACKS"

COHESITY

RESILIENCE EVERYWHERE