cristie
PROTECTING DATA SINCE 1969

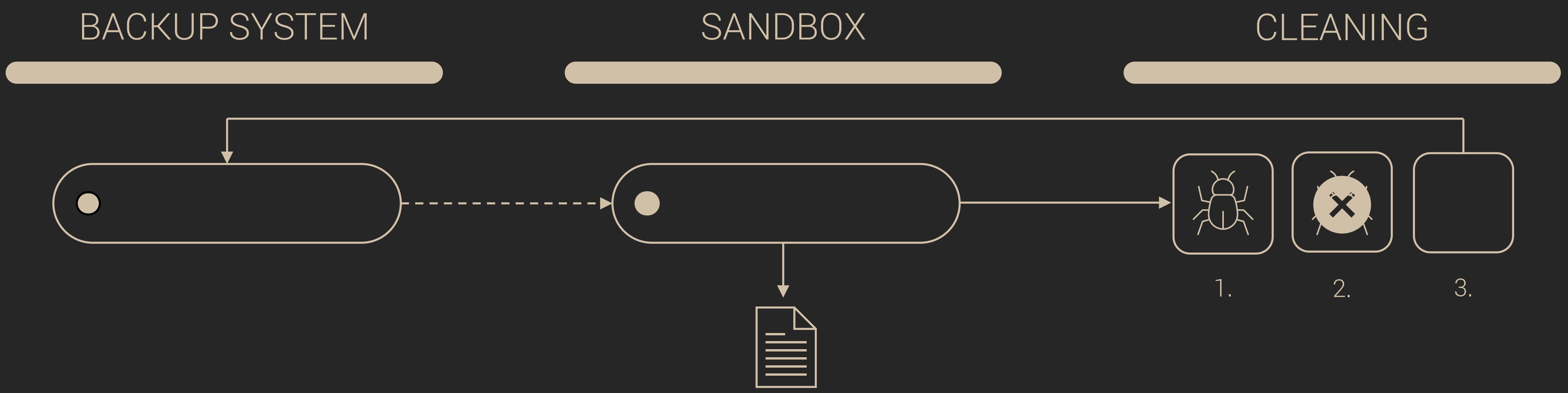
CLOSE YOUR CYBER RECOVERY GAP IN 4 STEPS

A guide to achieving data resiliency for enterprise security leaders.

The guide is produced by Predatar and provided by Cristie, a Predatar APEX Partner

APEX PARTNER. POWERED BY PREDATAR

OVERVIEW



BACKUP SYSTEM

SANDBOX

CLEANING

- COHESITY
- IBM
- RUBRIK
- VEEAM

- TEST AUTOMATION
- THREAT DETECTION
- REPORT & ALERT

1. THREAT DETECTED
2. THREAT CLEANED
3. CLEAN RESTORE

cristie
PROTECTING DATA SINCE 1969

> "Today,
> many organisations will be unable to recover all of their critical data and IT systems following a cyber attack.
>
> This ebook is designed to help you understand the risks associated with cyber recovery, and help you close the gap between where you are today and where you need to be."

CONTENT

- Section 1: Understanding the cyber recovery gap
- Section 2: Closing your cyber recovery gap
- Section 3: Conclusion & next steps

01010101101011010110011010110010101 1 010101 01011010110011010110010101 1
0101010110101101010101110110101100110101100101011 0101010110101101010101110110101100110101100101011
010 01101011010110010101011 01010101101011010110010101 1

APEX PARTNER. POWERED BY PREDATAR

UNDERSTANDING THE GAP

WHAT IS A CYBER RECOVERY GAP?

Almost every business, big or small, takes precautions against cyber threats. They do their best to keep cyber criminals out of their networks with cyber security tools such as firewalls, antivirus, and access controls. And they take regular backups or snapshots, so if the worst happens they can recover their important data and systems.

But... the startling fact is that most recoveries following a cyber attack fail, because the underlying storage infrastructure and processes weren't designed for a world full of cyber threats

8% of data fails to fully recover when needed.

Statistics based on data from monitoring enterprise storage environments totalling more than 978PB by Predatar

An inability to recover will cause your organization significant financial and reputational damage, and in a ransomware scenario will put you at the mercy of the criminals.

As a security leader you will already know that you can't stop every attack. Sooner or later it is inevitable that your defences will be breached. But how much do you understand about your organisation's ability to recover from a cyber attack?

Your organisation's cyber recovery gap is the delta between it's ability to recovery from an attack, and where it needs to be to ensure operational continuity. Perhaps, most worrying of all is that many organsiations have a misplaced confidence and don't understand the complexities and risks associated with recovering from a cyber attack.

UNDERSTANDING THE GAP

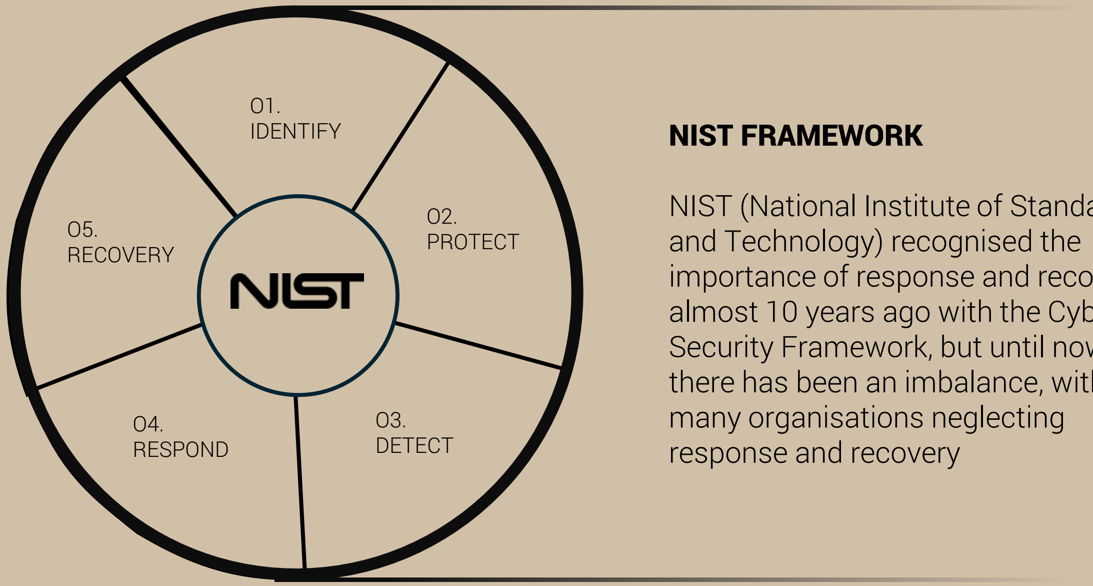
CYBER RESILIENCY VS CYBER SECURITY

So, why has this recovery gap emerged in many businesses? In recent years, most organisations have responded to the increasing threat landscape by investing in defence. i.e. preventing breaches by keeping cyber criminals out of their networks. This is cyber security.

Today, analysts and industry experts agree that it's simply not possible to prevent every malicious attack.

A cyber resilient organisation is one that is prepared to mount a fast and effective recovery in the face of a cyber-related crisis.

> To make a real difference to the impact of cybersecurity incidents, priorities must shift from defensive strategies to the management of disruption through resilience.
>
> Gartner, Maverick Research
> Embrace the breach.



NIST FRAMEWORK

NIST (National Institute of Standards and Technology) recognised the importance of response and recovery almost 10 years ago with the Cyber Security Framework, but until now there has been an imbalance, with many organisations neglecting response and recovery

cristie
PROTECTING DATA SINCE 1969

UNDERSTANDING THE GAP

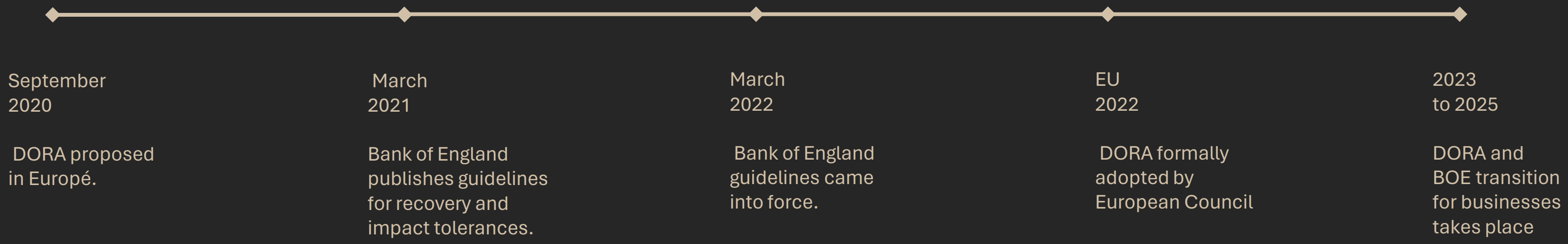
CYBER RESILIENCY REGULATIONS

Ensuring your business has operational resiliency is not only a wise strategy, but for many organisations, it will soon be mandatory.

Significant new regulations are coming into force for financial services institutions in Europe, US and UK.

The DORA (EU), Bank of England PRA/FCA (UK), and Sound Practices (US) regulations all require financial services organisations to prove their ability to recover critical data and systems quickly. It’s only a matter of time before regulatory bodies in other industries follow suit

OPERATIONAL RESILIENCE TIMELINE



September 2020

DORA proposed in Europé.

March 2021

Bank of England publishes guidelines for recovery and impact tolerances.

March 2022

Bank of England guidelines came into force.

EU 2022

DORA formally adopted by European Council

2023 to 2025

DORA and BOE transition for businesses takes place

APEX PARTNER.
POWERED BY PREDATAR

CLOSING THE GAP

CLOSE YOUR RECOVERY GAP

We have identified 4 key steps to help you close your cyber recovery gap and boost operational resiliency in your organisation.

The following pages will help you understand what is involved and what best practice looks like for each of these steps.

STEP 1 – Identify your team

STEP 2 - Define your KPIs

STEP 3 - Ensure your data integrity

STEP 4 - Optimise your recovery speed

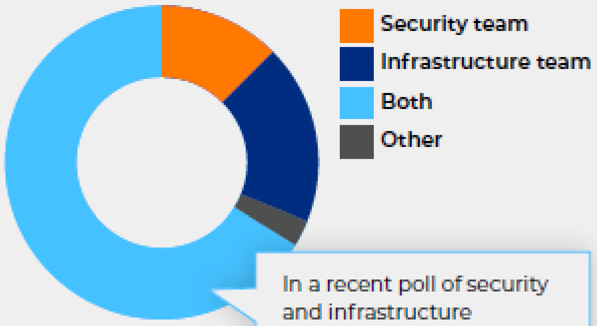
STEP 1 – Identify your team

Before we look at ways to close the recovery gap, we must first look at organisational structure and lines of responsibility.

One of the major contributing factors of cyber recovery gap is a lack of visibility and coordination between security teams and infrastructure/storage teams.

While security teams have been focusing on preventing data breaches in an ever-evolving threat landscape, infrastructure teams have been focussed on managing storage environments which are growing exponentially in size and complexity every day. As a result, responsibility for cyber recovery has often been overlooked.

Who is responsible for cyber resiliency?

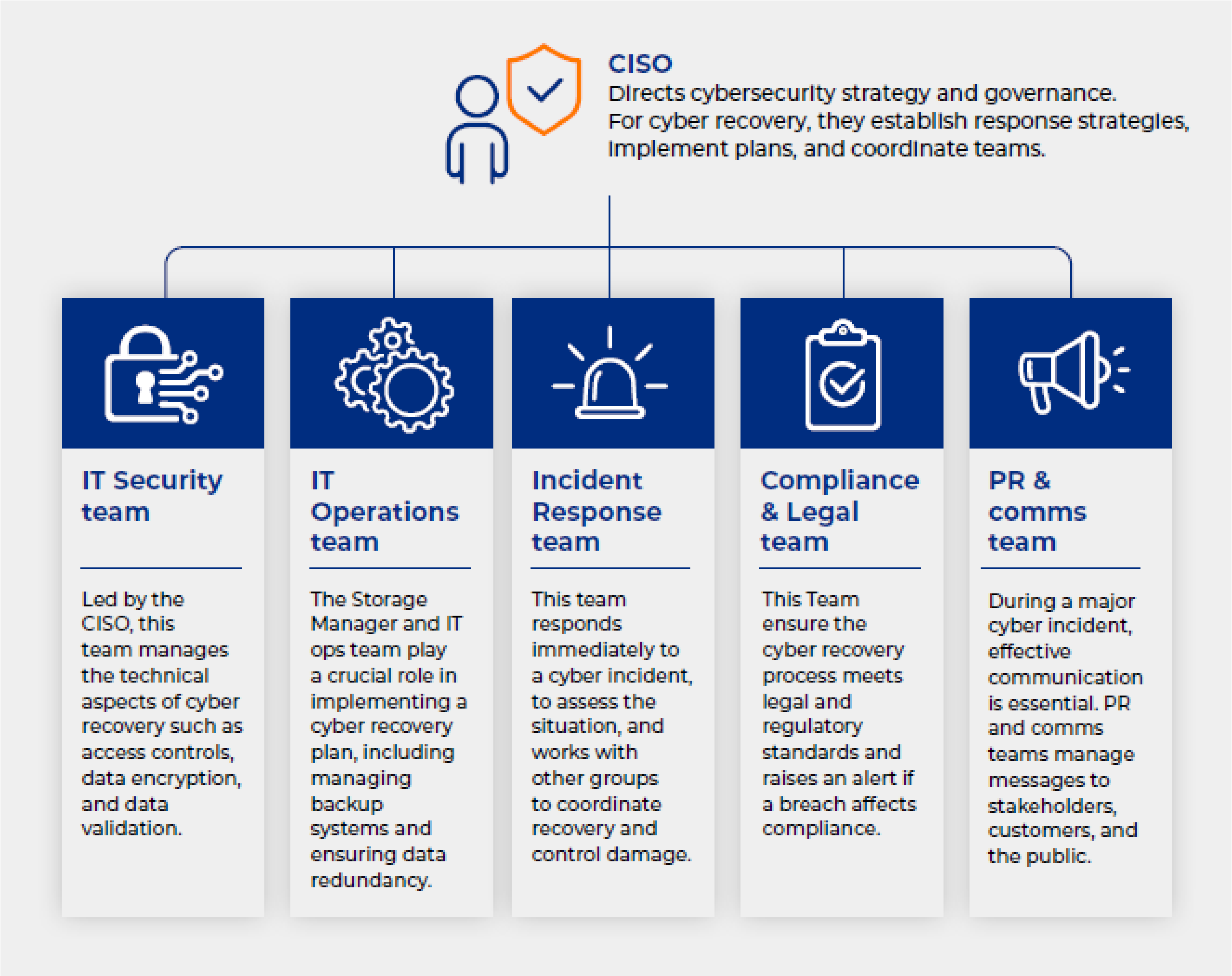


In a recent poll of security and infrastructure professionals 68% agreed that resiliency is a shared responsibility.

CISO's need to know...

#1

Ask your CTO or CIO what steps are being taken to ensure safe and effective data recovery is possible following a cyber attack?



CISO
Directs cybersecurity strategy and governance.
For cyber recovery, they establish response strategies, implement plans, and coordinate teams.

IT Security team

Led by the CISO, this team manages the technical aspects of cyber recovery such as access controls, data encryption, and data validation.

IT Operations team

The Storage Manager and IT ops team play a crucial role in implementing a cyber recovery plan, including managing backup systems and ensuring data redundancy.

Incident Response team

This team responds immediately to a cyber incident, to assess the situation, and works with other groups to coordinate recovery and control damage.

Compliance & Legal team

This Team ensure the cyber recovery process meets legal and regulatory standards and raises an alert if a breach affects compliance.

PR & comms team

During a major cyber incident, effective communication is essential. PR and comms teams manage messages to stakeholders, customers, and the public.

STEP 1 – Identify your team

Every organisation is different, but it's important that someone takes a responsibility for leading the evolution.

Often the CISO is best placed to lead and coordinate the efforts.

Disciplined cyber security teams track and measure everything in dynamic reports – servers patched, incidents raised, mean time to fix and many more.

The metrics monitored by storage managers and IT Operations teams lean towards systems availability and minimising downtime.

We know this based on data collected by Predatar, firms on average recover less than 1% of their data in any given year. In addition, one in fourteen backup recoveries are compromised in some way.

These metrics highlight the gap that exists between firms' cyber security and cyber resilience operations.

1 in 12
Nodes fail to recover when needed

0.8%
of nodes are recovery tested

<0.1%
of test recoveries are checked for malware

CISO's need to know...

#2
Ask your CTO or CIO to outline the recovery testing process and the measures of success in your organisation.

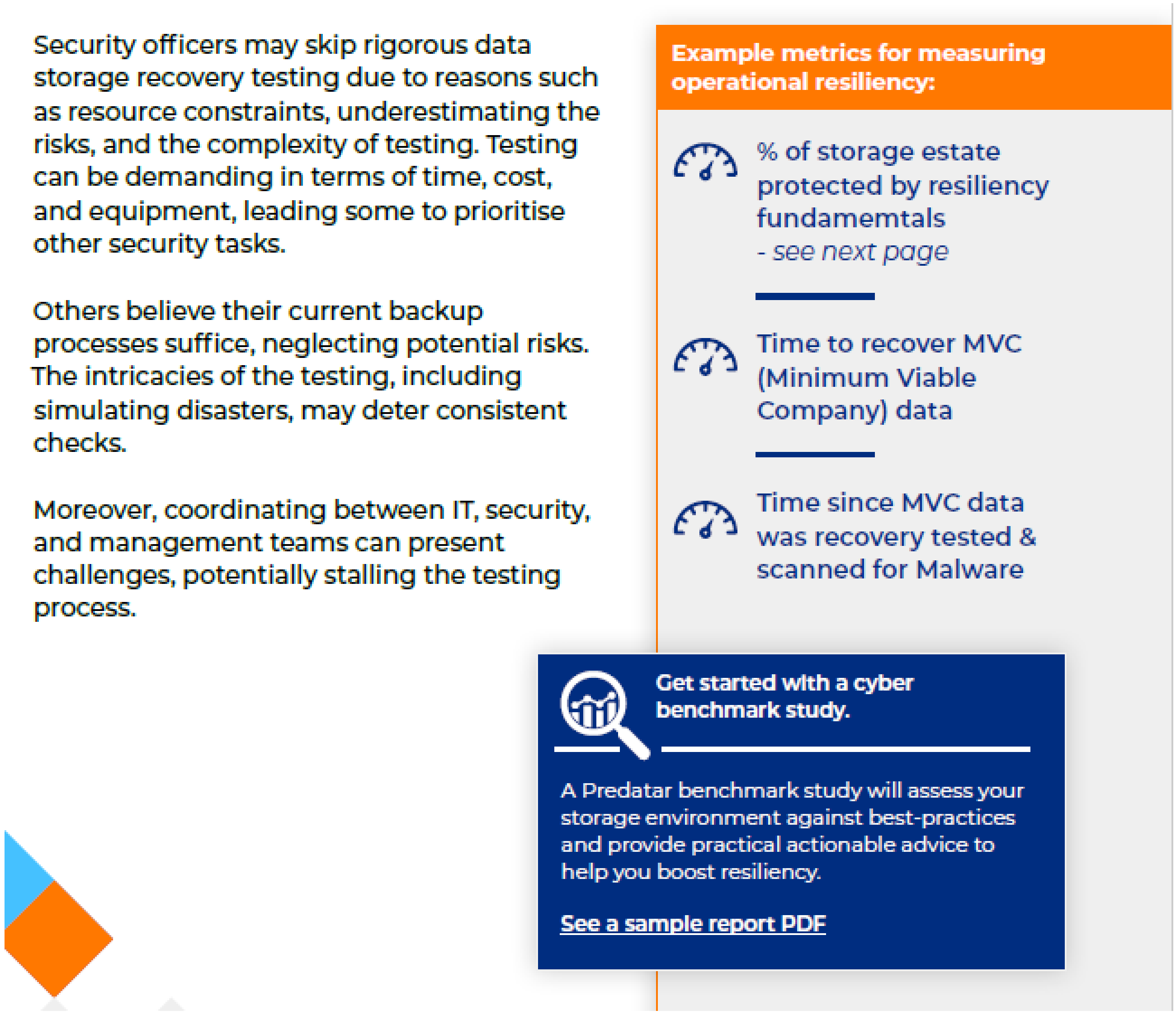
Statistics based on data from monitoring enterprise storage environments totalling more than 978PB by Predatar

STEP 1 – Identify your team

STEP 2 - Define your KPIs

Security teams and IT teams are typically data driven and reporting on key metrics is an important part of both functions.

However, few businesses track data recovery metrics.



Security officers may skip rigorous data storage recovery testing due to reasons such as resource constraints, underestimating the risks, and the complexity of testing. Testing can be demanding in terms of time, cost, and equipment, leading some to prioritise other security tasks.

Others believe their current backup processes suffice, neglecting potential risks. The intricacies of the testing, including simulating disasters, may deter consistent checks.

Moreover, coordinating between IT, security, and management teams can present challenges, potentially stalling the testing process.

Example metrics for measuring operational resiliency:

- % of storage estate protected by resiliency fundamemtals
  - *see next page*
- Time to recover MVC (Minimum Viable Company) data
- Time since MVC data was recovery tested & scanned for Malware

Get started with a cyber benchmark study.

A Predatar benchmark study will assess your storage environment against best-practices and provide practical actionable advice to help you boost resiliency.

See a sample report PDF

cristie
PROTECTING DATA SINCE 1969

STEP 1 – Identify your team

STEP 2 - Define your KPIs

Organisations must define processes to validate the recoverability of their data AND the metrics they use to measure success.

APEX PARTNER.
POWERED BY PREDATAR

Storage Design

The design of your storage infrastructure is critical for ensuring that the data that your organisation stores can't be tampered with by bad-actors - this could include employees within your business. There are 5 fundamental principles of cyber resilient storage design:

1. **Data Encryption:** While it won't halt malware spread, if data is taken off the network, its worth to attackers diminishes.

2. **Access Controls:** Use features like multi-factor authentication, command approvals, and strong passwords in storage systems.

3. **Multiple Copies:** Originally, the 3-2-1 rule advised having 3 data copies on 2 media types with 1 off-site.

4. **Immutability:** Available for various storage types, it ensures data accuracy and deters tampering. It's valuable but has costs.

5. **Air-Gap:** Initially used to guard against physical threats, it's now also effective against malware spread.

For more detail on these key storage concepts, please read the Predatar 5 Fundamentals eBook here.

CISO's need to know...

#3

Ask your CTO or CIO, how many of these fundamentals are in place in your organisation?

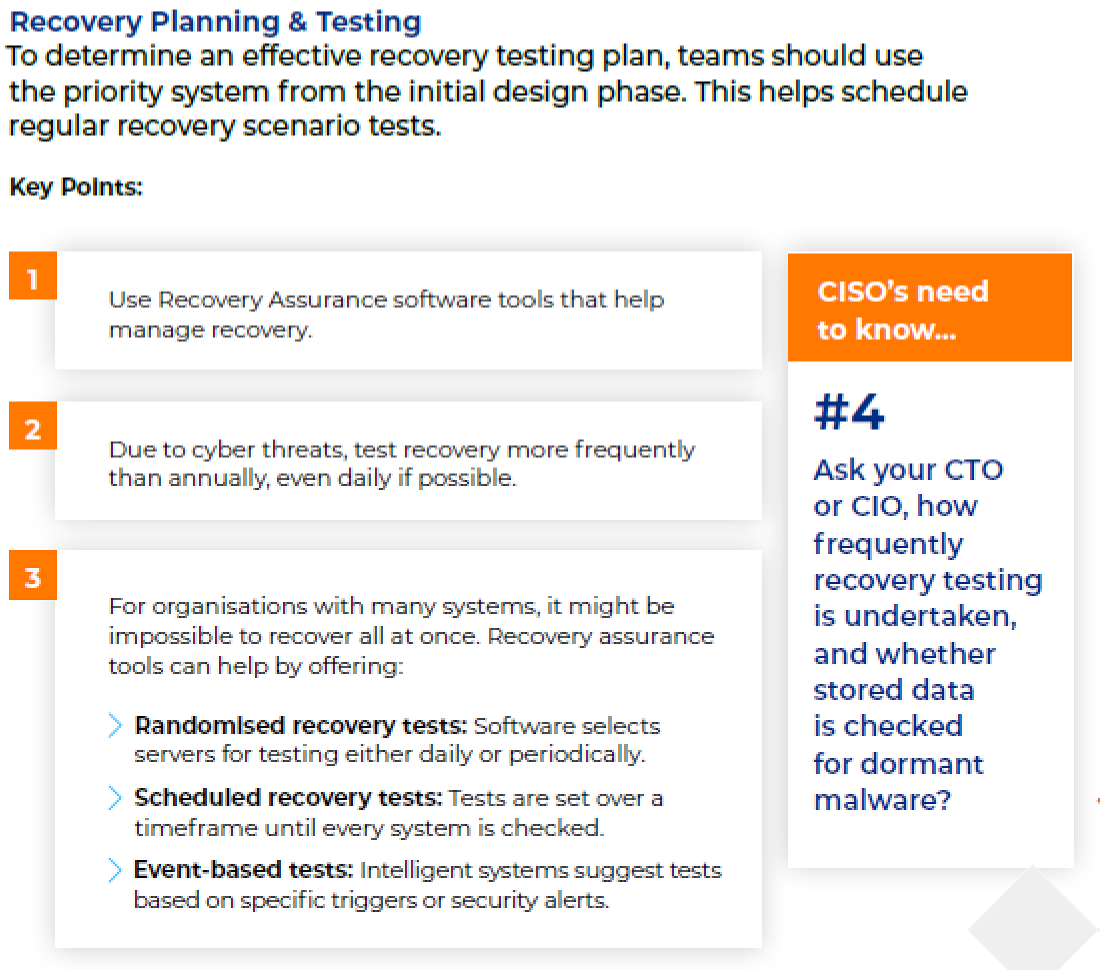
STEP 1 – Identify your team

STEP 2 - Define your KPIs

STEP 3 - Ensure your data integrity

Storage architects, prioritise availability, balancing cost and speed.

A comprehensive cyber resilience strategy should integrate both primary and secondary storage with top-tier cybersecurity.



Recovery Planning & Testing

To determine an effective recovery testing plan, teams should use the priority system from the initial design phase. This helps schedule regular recovery scenario tests.

Key Points:

1 Use Recovery Assurance software tools that help manage recovery.

2 Due to cyber threats, test recovery more frequently than annually, even daily if possible.

3 For organisations with many systems, it might be impossible to recover all at once. Recovery assurance tools can help by offering:

- **Randomised recovery tests:** Software selects servers for testing either daily or periodically.
- **Scheduled recovery tests:** Tests are set over a timeframe until every system is checked.
- **Event-based tests:** Intelligent systems suggest tests based on specific triggers or security alerts.

CISO's need to know...

#4

Ask your CTO or CIO, how frequently recovery testing is undertaken, and whether stored data is checked for dormant malware?

STEP 1 – Identify your team

STEP 2 - Define your KPIs

STEP 3 - Ensure your data integrity

Even with all of the storage fundamentals in place it is still important to validate the recoverability cleanliness of your data with continuous and rigorous testing.

Optimising your recovery speed can dramatically reduce inconvenience for staff and customers, not-to-mention the financial and reputational damage.

Early Detection

The sooner you know your organsiation is under attack, the faster you can act. That's why fast recovery begins with early detection.

Security teams and storage teams are already using tools to detect danger signals and raise alerts.

Emerging technology can connect these security and storage tools, to supercharge AI-powered threat detection and raise alerts faster than ever before.

Prioritisation

Most large organisations already prioritise the recovery of their most critical systems in business continuity management plans.

This documentation can be used to programme automated recovery assurance tools, to make sure the data and systems your organisation needs to remain operational are continually validated for clean and complete recovery.

Storage Method

Storage isn't just about holding data; it's a balance of cost and speed. Faster access costs more. Companies use varied storage from different suppliers.

Utilising both primary and backup storage is vital because:

- Primary storage might not protect everything.
- Backup storage offers different protection levels.
- Think of backup storage as a safety net; test its recovery.
- Checking backups for malware is unobtrusive to users.

CISO's need to know...

#5

Ask your CTO or CIO, if you have a comprehensive and prioritised recovery plan in place to recover the whole business?

STEP 1 – Identify your team

STEP 2 - Define your KPIs

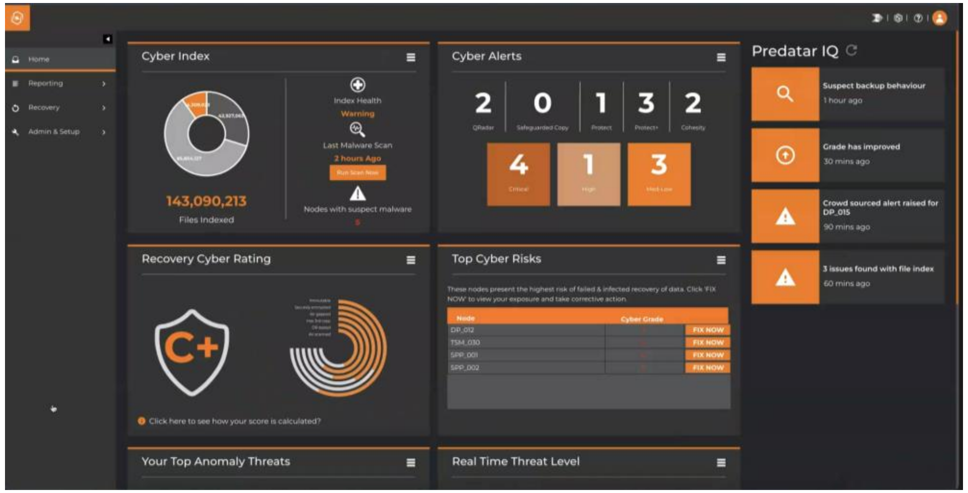
STEP 3 - Ensure your data integrity

STEP 4 - Optimise your recovery speed

Every minute your critical systems and data are offline following a cyber attack will have a negative impact on your business.

CONCLUSIONS AND NEXT STEPS

CYBER RECOVERY ASSURANCE TECHNOLOGY



These nodes present the highest risk of failed & infected recovery of data. Click 'FIX NOW' to view your exposure and take corrective action.

Node	Cyber Grade	
DP_012	[illegible]	FIX NOW
TSM_030	[illegible]	FIX NOW
SPP_001	[illegible]	FIX NOW
SPP_002	[illegible]	FIX NOW

The growing recognition amongst businesses that they need to boost resiliency, not to mention the influx of regulations demanding proof of operational resiliency in the event of a cyber attack has triggered a wave of innovation to help solve the challenge.

Predatar is at the forefront of this wave. Our Recovery Assurance Software is already being used by enterprises around the world to give them confidence in their ability to mount a fast and effective recovery - whenever they need to.

Reporting is key for ongoing cyber resilience. Regularly updated reports let you assess your organisation's status and find areas to improve. Common reports include Risk, Vulnerability, Penetration Testing, Incident Responses, Training Metrics, Patch Management, Backups, and Downtime Metrics.

Additionally, consider introducing a Cyber Resilience Index, a combined metric to monitor progress and convey your cyber stance to stakeholders.

CONCLUSIONS AND NEXT STEPS

5 QUESTIONS

As we have discussed in this ebook, in order to maintain a robust and resilient security posture, it's vital to not only implement safeguards but also regularly question and refine them.

We have suggested some questions throughout the ebook which you can use to help you understand the state of resiliency in your business.

Along with these five additional questions, any security leader can begin to identify the gaps that exist.

These queries delve deep into areas of encryption, access control, data recovery, data segregation, and cyber resilience metrics.

By addressing these critical domains, organisations can fortify their defenses, ensuring not just prevention, but also swift recovery and adaptability in the face of cyber security threats.

1 **Encryption and Security:** How do we manage encryption for our data, both at rest and in transit, and which methods and key management systems are in place?

2 **Access Control:** How are user permissions structured within our organisation, and what measures, such as multi-factor authentication, do we employ to ensure the security of sensitive data and prevent unauthorised escalations?

3 **Data Recovery:** What protocols and strategies are in place for data recovery, and how frequently do we test and scan our backup data?

4 **Data Segregation:** How does our organisation segregate data based on sensitivity, and what precautions do we take to prevent leaks or breaches between different datasets?

5 **Cyber Resilience Metrics:** Beyond traditional metrics like backup rates and patching, what comprehensive resilience metrics do we employ to measure and enhance our cybersecurity posture?

cristie
PROTECTING DATA SINCE 1969

CONCLUSIONS AND NEXT STEPS

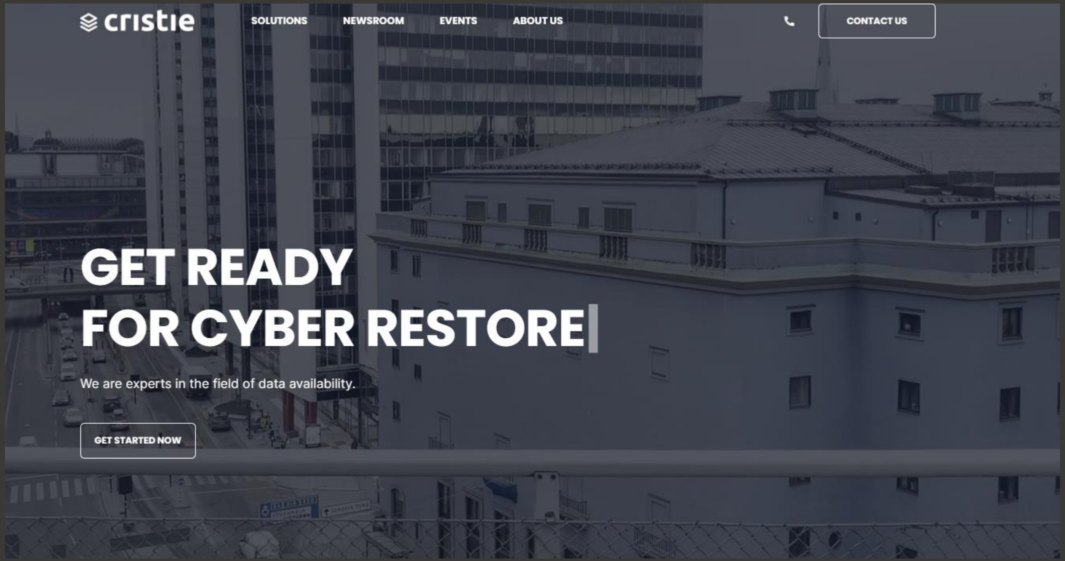
CONCLUSION

The digital landscape makes it evident that merely focusing on cybersecurity isn't enough. "Closing your Cyber Gap" highlights the need to prioritize cyber resilience alongside prevention. Breaches are inevitable, so having an efficient recovery mechanism is vital. This means a collaborative effort among teams, led by the CISO, using advanced technologies like A.I. for improved threat detection.

Regular testing, monitoring, and reporting are paramount for proactive cyber resilience. With global regulations leaning towards recovery, resilience is no longer optional but a necessity.

As security leaders chart this terrain, the key questions outlined in the book offer essential guidance, ensuring ongoing adaptation and collaboration.

CONTACT FOR A TALK



GET READY
FOR CYBER RESTORE

We are experts in the field of data availability.

www.cristienordic.com

APEX PARTNER.
POWERED BY PREDATAR

cristie

PROTECTING DATA SINCE 1969

www.cristienordic.com
www.cristie.de