2024 SINGAPORE I.T & DATA RESILIENCE READINESS REPORT

Published by:

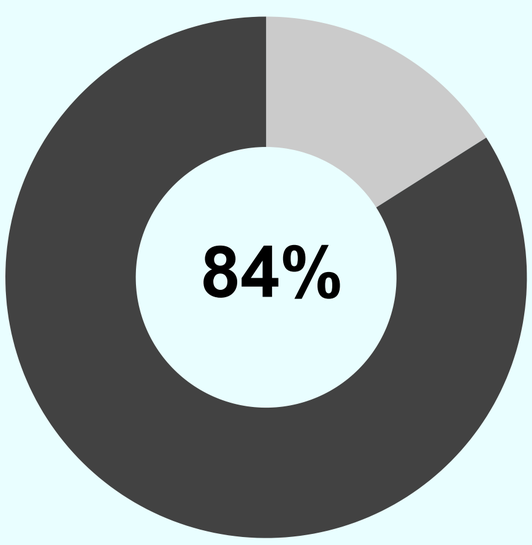
Spark

In Partnership with:

veeam

www.wahspark.com

OVERVIEW



84%[1] of businesses in Asia plan a full cloud migration by 2024.

Increasing Cost of Data Breach in S.E.A

$3.05M

$3.05M[2] USD is the average cost of data breach in S.E.A.

$4.18M
FINANCIAL SERVICES

$3.60M
ENERGY & UTILITIES

The 2024 **SPARK IT & Data Resilience Report**, **published in partnership with Veeam**, highlights the escalating costs and complexities of data breaches in Southeast Asia, with a 6% year-over-year increase, reaching an all-time high of $3.05 million. The report underscores that 82% of breaches involve cloud-stored data, emphasizing the need for robust cloud security measures. Organizations are increasingly adopting AI and automation, which have proven to reduce breach lifecycles by 99 days and save up to $1.25 million in breach costs. However, only 28% of organizations have extensively integrated these technologies.

Ransomware remains a significant threat, with 76% of organizations experiencing attacks in the past year. Despite increased investments in data protection, only a small percentage of organizations feel confident in their ability to recover quickly from such incidents. The report also reveals that nearly half of the surveyed organizations test their backup and recovery processes only once a year, which is insufficient for ensuring data resilience.

The findings call for a unified approach to data protection across heterogeneous IT environments, emphasizing the need for continuous improvement in backup strategies, AI integration, and compliance with evolving data protection regulations. The report concludes that building resilience in the cloud is an ongoing journey, requiring iterative enhancements and proactive measures to safeguard against cyber threats.

1 Source: The Next-Generation Cloud Strategy in Asia", NielsenIQ, 2023

2 Source: IBM, Cost of Data Breach Report, 2023

THE COST OF DATA BREACH IS GROWING

In Southeast Asia, the cost of data breach is growing at a rate of 6% YoY, with escalation and de-escalation costs increasing at a staggering 15% YoY in the same period.

82%[1] **of breaches involved data stored in the cloud — public, private or multiple environments**

1 in 3[1] **breaches are identified by an organisation's own security teams or tools**

58% **of organisations surveyed indicate a need to increase investments to strengthen IT, Data Resilience & BCP processes,**

Organisations have started modernising legacy applications to be compatible with the cloud and eventually, migrate all critical workloads completely to cloud infrastructure. While a big part of the cloud footprint will be managed as a private cloud, Nielsen predicts 27% of applications and data will be deployed into public cloud, while a good 24% of apps will be supported by a flavour of hybrid-cloud architecture. The complexities introduced by such heterogeneous environments, add operational and cyber-risks to the mission-critical business applications that run on today's modern IT infrastructure.

---

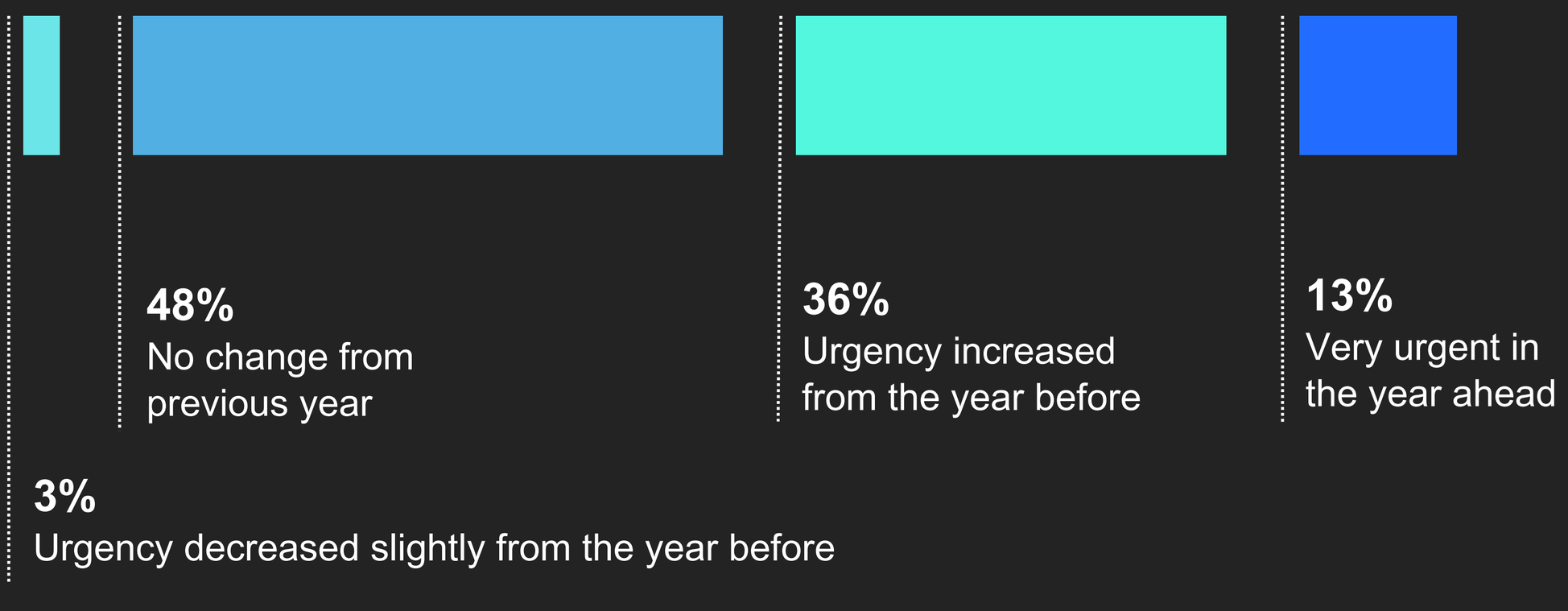
1 Source: IBM, Cost of Data Breeach Report, 2023

STATE OF ORGANISATIONAL READINESS IN S.E.A

1 in 2 CxOs

surveyed indicated an increase in urgency to address ransomware related data risk from 2023

Survey Question: On a scale of 1 to 5, rate how urgent it is in your organisation to address Ransomware-related data risks.



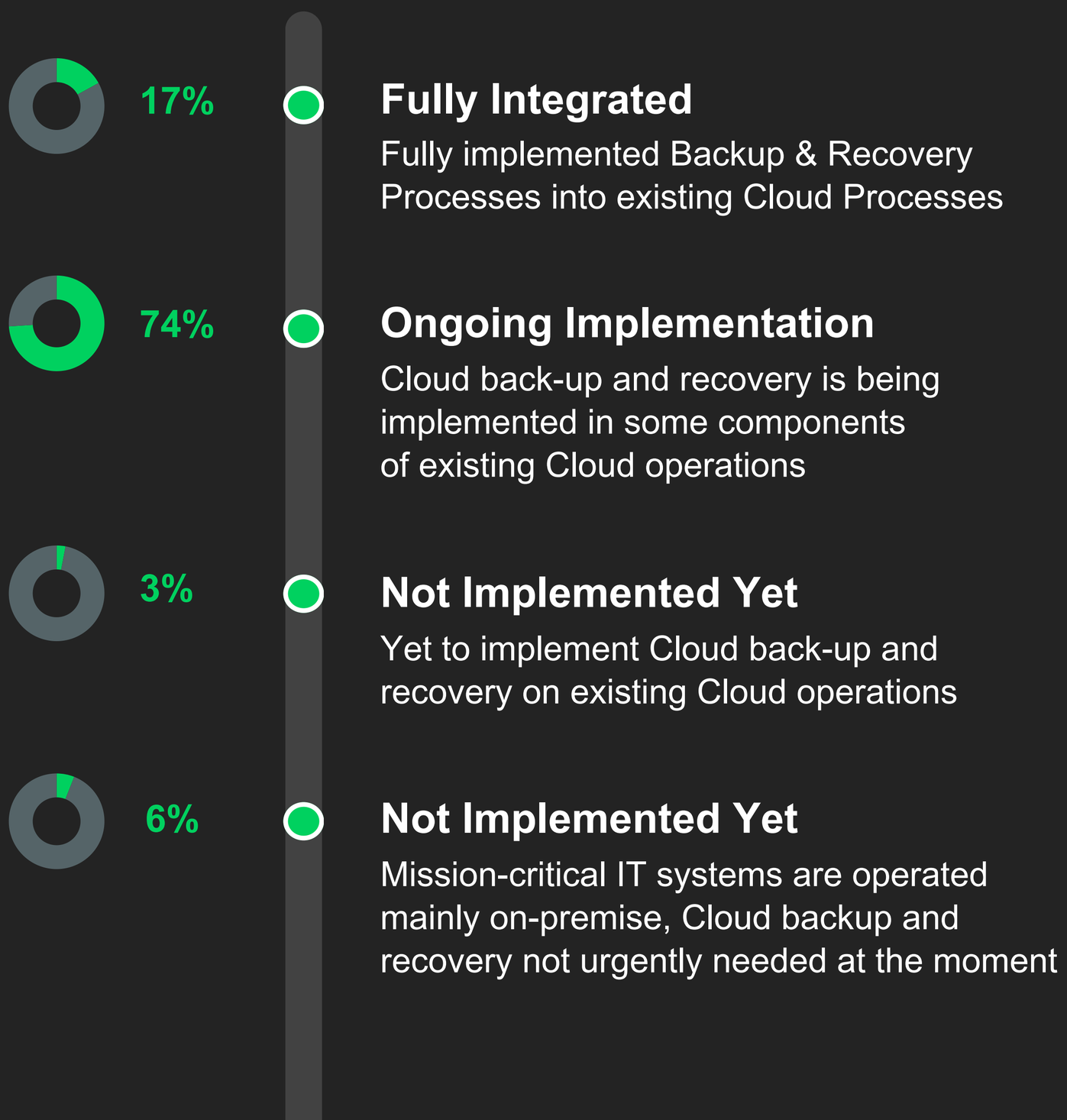
3%
Urgency decreased slightly from the year before

48%
No change from previous year

36%
Urgency increased from the year before

13%
Very urgent in the year ahead

Building resilience in the Cloud is an iterative journey, constantly evolving as Cloud estates continue to expand.



17%

Fully Integrated
Fully implemented Backup & Recovery Processes into existing Cloud Processes

74%

Ongoing Implementation
Cloud back-up and recovery is being implemented in some components of existing Cloud operations

3%

Not Implemented Yet
Yet to implement Cloud back-up and recovery on existing Cloud operations

6%

Not Implemented Yet
Mission-critical IT systems are operated mainly on-premise, Cloud backup and recovery not urgently needed at the moment

Survey Question: How would you rate the level of cloud-readiness of your organisation's IT Resilience & BCP Strategy?

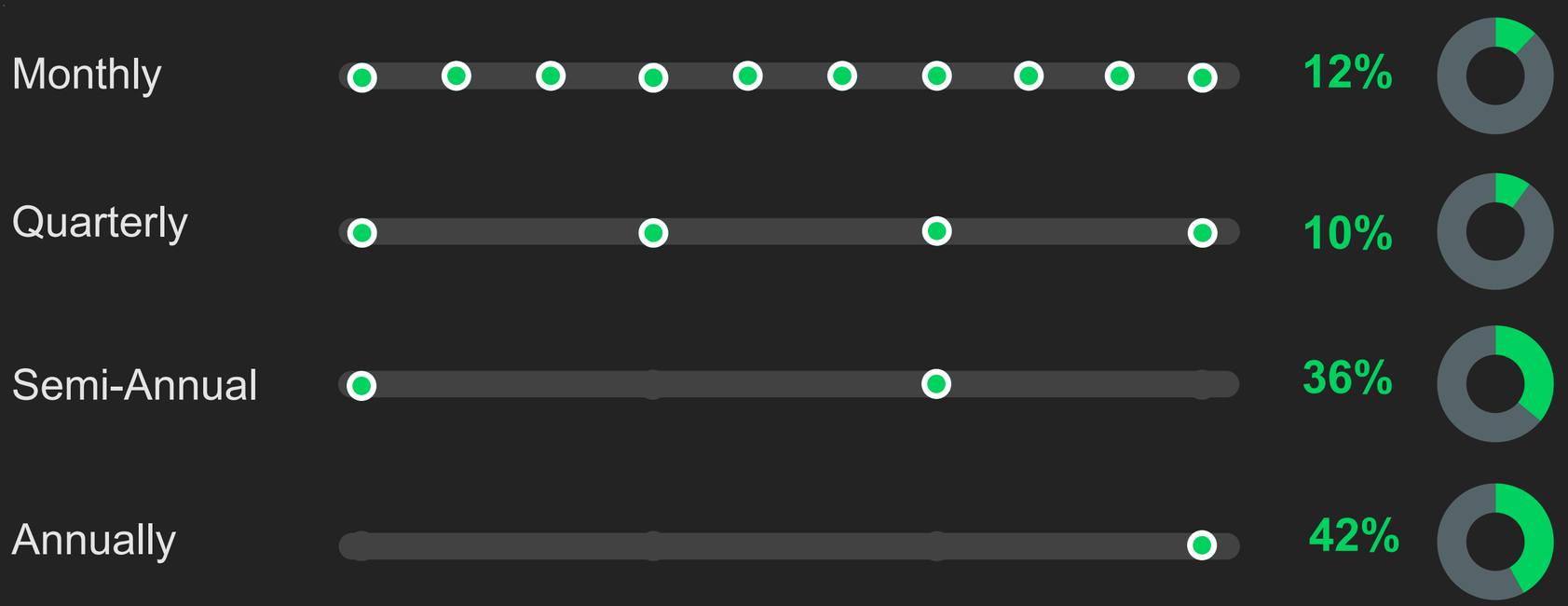
As organisations expand their cloud estates, tech leaders have to protect a larger and more fragmented footprint of data stores and critical applications across multi-cloud and legacy on-premise IT environments.

To ensure service availability and reliability of modern applications, the IT stack has to be replicable and recoverable, from code to cloud. This includes cloud VMs, micro services and CI/CD pipelines, both within proprietary platforms and open-source orchestrators.

STATE OF ORGANISATIONAL READINESS IN S.E.A

Almost half of organisations surveyed, test and validate existing back-up and recovery processes only once a year.

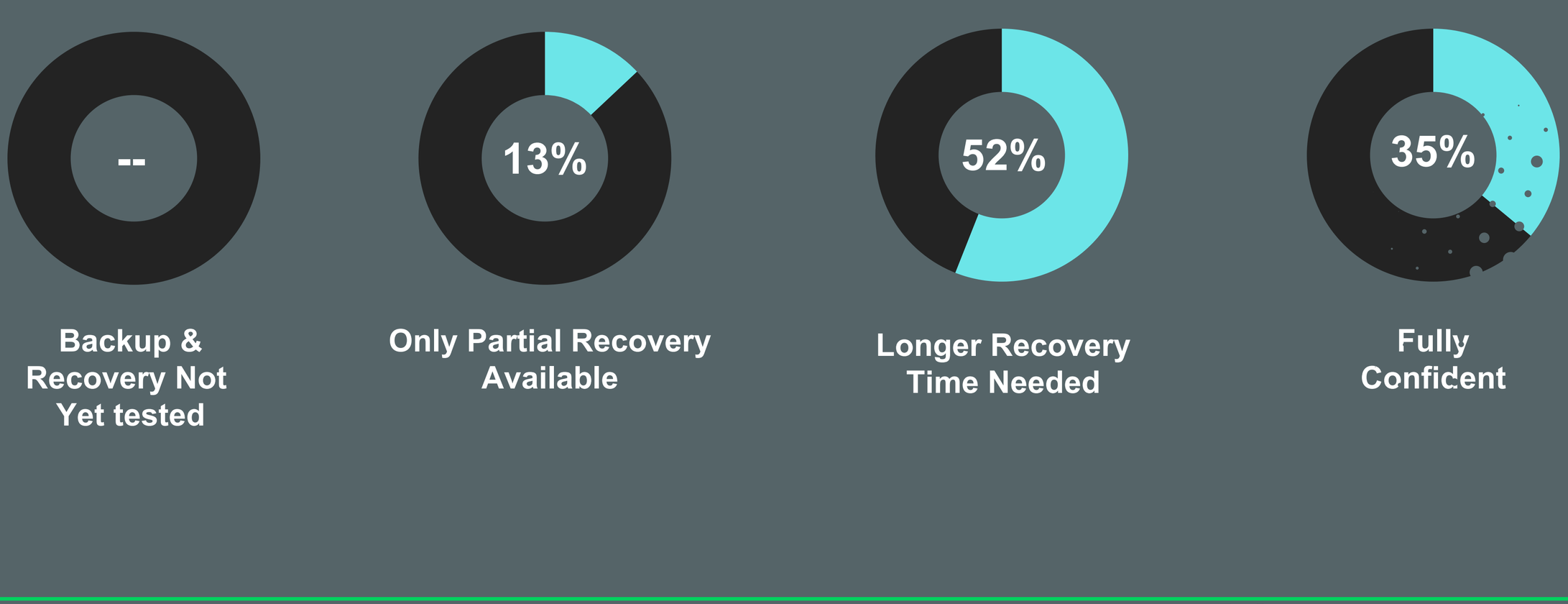
While organisations have implemented back-up and recovery protocols to some degree, documentation alone is inadequate if testing and validation drills are only conducted once a year. To simplify and automate back-up testing, Veeam's SureBackup platform provides automation validation tools that can support critical workloads, and automate verification of back-up files in an isolated environment.



Survey Question:
How often does your organization test and validate its backup and recovery processes?

More than half of CxOs surveyed indicated their organisations are only able to **recover only some critical data and workloads within 24 hours,** while 13% highlight backup & recovery does not cover all digital estates in their organisations.

Survey Question: Are you confident with your organisation's current IT backup strategy?



A.I. SHAPES DATA PROTECTION STRATEGIES TODAY

S.E.A: 99 Days shorter

Global: 108 Days shorter

Days shorter to detect & remediate a data breach

S.E.A: USD 1.25M Savings

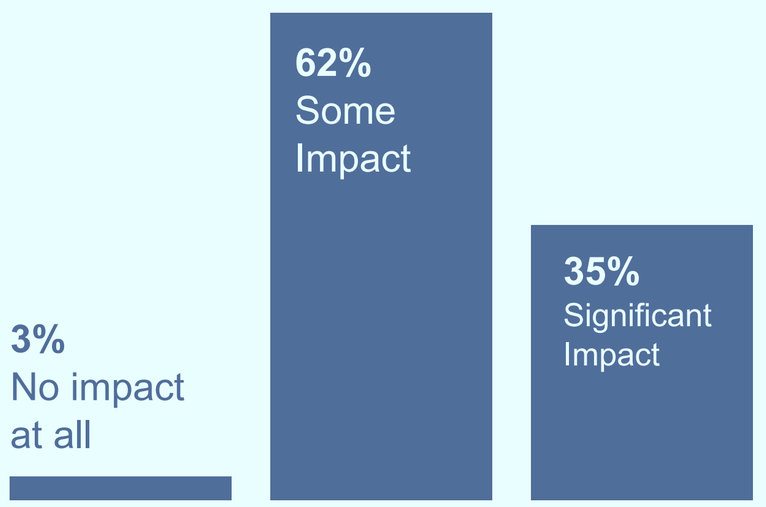
Global: USD 1.76M Savings

Savings in cost of data breach with the use of A.I. & automation in their data resilience processes

Organisations that adopt A.I. and automation extensively within their data protection stack, experience a data breach lifecycle that was 99 days shorter with nearly $1.25 million lower data breach costs compared to studied organizations that have not deployed these technologies.

Only **28%**[1] of organisations surveyed by IBM globally have integrated security AI and automation extensively in their I.T. operations.

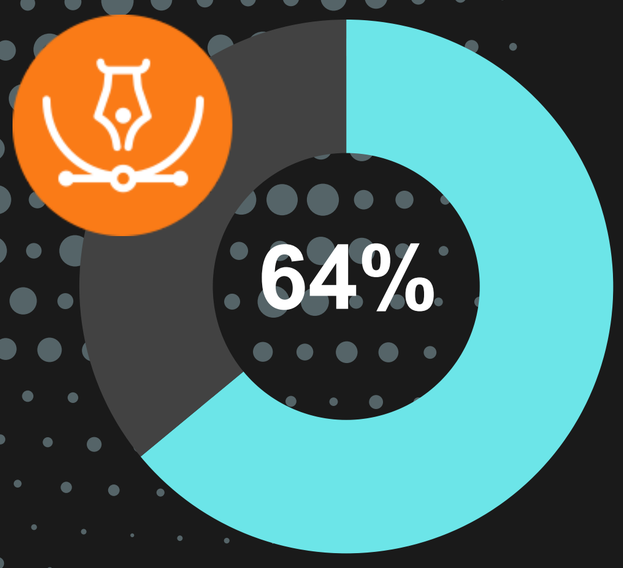
Survey Question:
Rate how significantly the rise of A.I. adoption in your organisation is impacting your enterprise data protection strategy?



Almost all organisations are pushed to reshape their enterprise data protection strategies both to deal with new A.I. vulnerabilities, as well as to use it's latest capabilities to improve observability, strengthen governance, as well as orchestrate & automate incident response.

1 Source: IBM, Cost of Data Breach Report, 2023

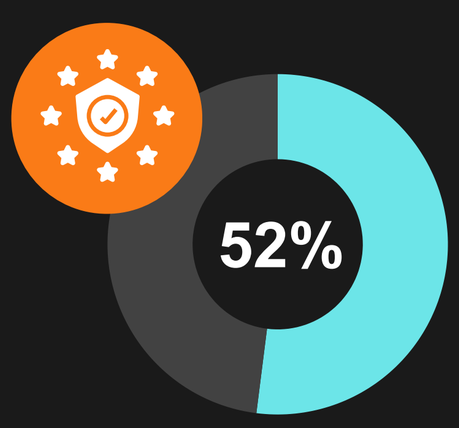
Top Challenge for Organisations



1. Unify data protection policies

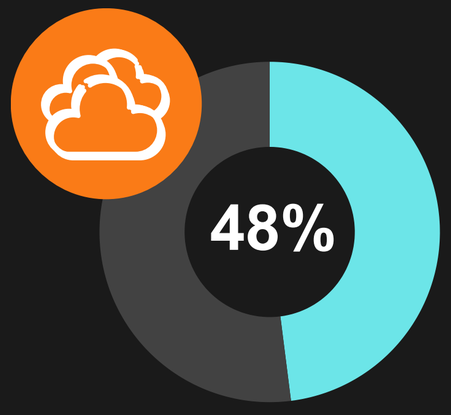
, processes, and tools across a heterogeneous IT environment spanning on-premises, cloud, and edge computing infrastructure,

Survey Question: What are your top challenges in improving your enterprise data protection toolkit?



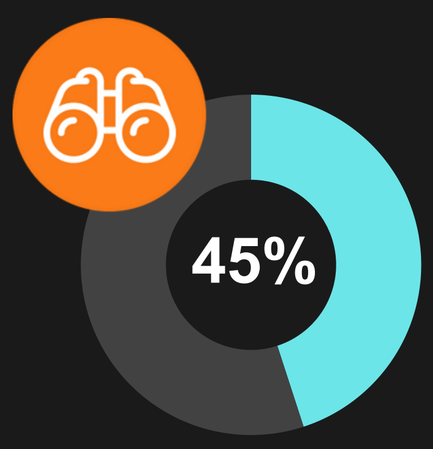
2. Ensuring Compliance

with evolving data privacy regulations (e.g. PDPA, GDPR, EU AI Act, etc.)



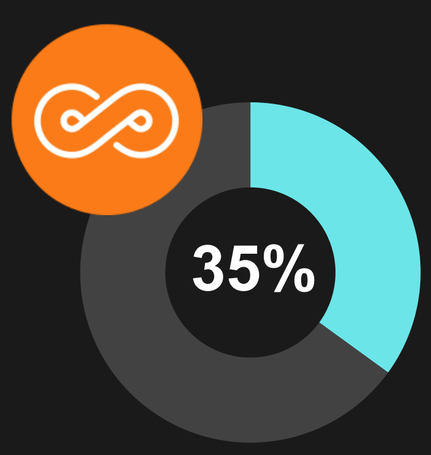
3. Extending Data & Cloud Back-up

and recovery into multi-cloud platforms, SaaS applications and CI/CD pipelines



4. Build Meaningful Analytics

to optimise backup and recovery performance, reduce costs, and demonstrate regulatory compliance

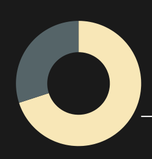


5. Develop/Re-skill In-house Talent

to design, deploy, and manage next-generation data protection solutions

MOST URGENT CAPABILITIES TO BUILD CLOUD-READINESS

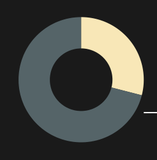
Perform recovery operations across on-prem and multi-cloud IT environments



Identify and recover critical data stores from both hot and cold storage tiers

Recover operations of Cloud workloads
e.g. containers, compute instances, kuberntes clusters etc.

Scan previous back-up versions for presence of advance persistent injections before recovery



CONCLUSION

Implementing unified data protection policies and toolkits, orchestrated over a single platform that span on-premises, cloud, and edge infrastructure is crucial for effective mitigation of operational and cyber risks.

By embedding artificial intelligence (AI) and automation into data resilience processes, organisations can significantly enhance threat detection, incident response, and overall efficiency, even realise massive dollar savings when remediating data breaches. Thus far, only a small percentage of companies have achieved this level of AI integration, highlighting a critical area for improvement.

Continuous testing and validation of backup and recovery processes are essential for maintaining data resilience. Regular drills and simulations can identify gaps and ensure organisations can recover critical data and workloads promptly in the event of an incident.

Additionally, organisations should prioritise up-skilling their workforce to design, deploy, and manage next-generation data protection solutions effectively.

By addressing these key recommendations, organizations can fortify their defences against evolving cyber threats, maintain compliance, and foster a culture of data resilience that underpins their digital transformation journey.

GET IN TOUCH

For General Enquiries
contactus@wahspark.com

Visit us at www.wahspark.com

Gladys Kan
Partnership Manager
SPARK
gladys@wahspark.com

GOH JING RUI
Research Specialist
SPARK
jingrui@wahspark.com

Sara Ramli
Community Manager
SPARK
sara@wahspark.com

www.wahspark.com