Current State Of Backup & Recovery in Manufacturing

2026
BENCHMARK
REPORT

Macrium Software | NewtonX®

Table of Contents

The **Macrium 2026 benchmark study**, conducted in partnership with **NewtonX**, examines how manufacturing organizations approach system protection, backup, & business continuity strategies.

The research surveyed 100 verified IT & OT decision-makers from mid-sized to enterprise manufacturing organizations with at least 2,500 employees across North America & the United Kingdom.

Research Context

The Critical Imperative of System Protection in Modern Manufacturing

In an era where manufacturing operations are increasingly digitized & interconnected, the ability to protect & rapidly recover critical information has evolved from a technical concern to a strategic business imperative.

Manufacturing organizations operate at the intersection of traditional processes & cutting-edge digital technologies, creating environments where a single point of failure can halt production lines, disrupt supply chains, & generate losses measured in hundreds of thousands of dollars per minute.

The Unique Complexity of Manufacturing System Protection

Unlike other sectors focused primarily on traditional IT infrastructure, manufacturing must safeguard diverse & interdependent systems spanning both IT & operational technology (OT). ERP systems, manufacturing execution systems, SCADA platforms, & programmable logic controllers all generate mission-critical data while simultaneously controlling physical production processes.

Many organizations operate with legacy systems - some decades old - alongside modern cloud infrastructure & emerging Industry 4.0 technologies.

These hybrid environments create unique challenges for implementing comprehensive backup & recovery strategies that accommodate proprietary protocols, real-time operational requirements, & distributed manufacturing sites.

The Rising Stakes

For manufacturing organizations, downtime represents a direct assault on operational efficiency & competitive positioning.

Unplanned downtime can cost mid-sized manufacturers tens of thousands to hundreds of thousands of dollars per hour, while eroding customer confidence, brand reputation, & supply chain commitments.

Despite these high stakes, many organizations struggle to achieve adequate backup & recovery capability. Target recovery objectives often exceed actual capabilities. Backup systems remain untested or tested too infrequently, & evolving cyber threats - particularly ransomware targeting manufacturing infrastructure - have introduced risks that traditional backup approaches were never designed to address.

The Path Forward

Addressing these challenges requires a fundamental shift in approach. Backup & recovery must be recognized as strategic capabilities that directly enable operational resilience, demanding investment in comprehensive testing programs & solutions purpose-built for manufacturing complexity.

This research illuminates the current state of system protection practices across manufacturing, identifies common challenges & emerging trends, & provides insights to guide organizations toward more robust capabilities.

The findings represent the collective experience of IT & operations leaders, offering a benchmark against which manufacturing organizations can evaluate their own capabilities & priorities.

Current State of Backup & Recovery

Key Insights

Tool Fragmentation Dominates the Landscape

Manufacturing backup environments are characterized by extensive platform diversity, with the vast majority deploying multiple solutions simultaneously. Organizations continue layering tools, treating different platforms as addressing distinct requirements.

This reflects manufacturing's inherent complexity where diverse system types resist unified approaches.

Hybrid Strategies Prevail, But Confidence Gaps Persist

Three-quarters employ hybrid backup approaches combining cloud & on-premise solutions, prioritizing protection for databases, ERP systems, & cloud workloads.

However, operational technology systems rank notably lower in protection priorities despite their criticality.

More concerning, a third of manufacturers lack confidence in meeting recovery targets & overall backup capabilities, revealing a disconnect between deployment & operational readiness.

Measurement Without Validation Creates Blind Spots

Manufacturers focus heavily on time-based metrics like RTO & RPO, but only a quarter track recovery test frequency.

This creates dangerous blind spots where organizations measure backup completion rates without validating actual recovery capability - a gap that may only become apparent during costly production outages.

Key Insights
Current Priorities

Consolidation opportunities exist for vendors who can address the full spectrum of manufacturing requirements

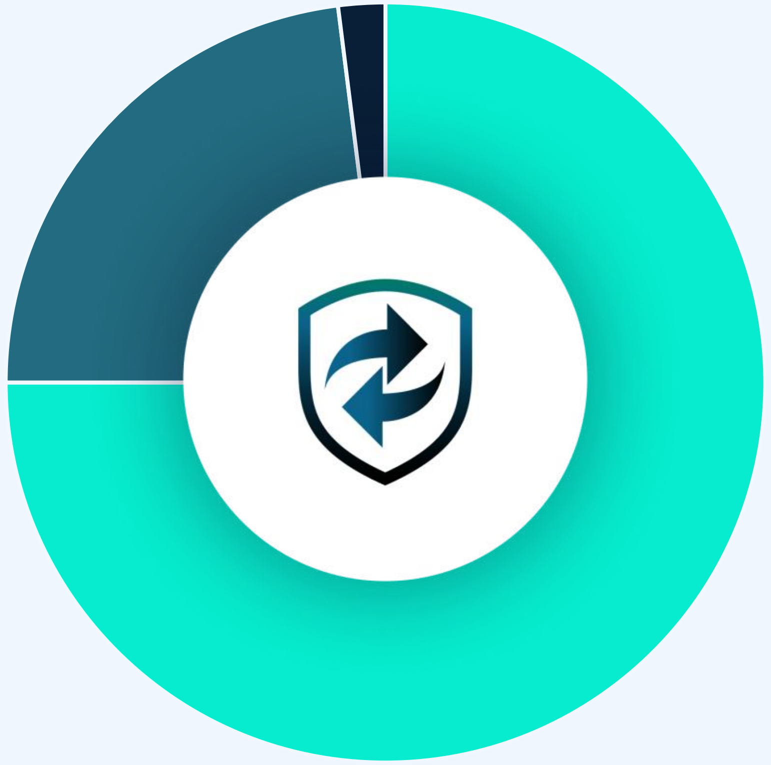
Testing & validation must move from periodic activities to regular operational practices

OT protection requires elevated priority given the criticality of manufacturing systems

Confidence-building through proven recovery capabilities, not just backup completion metrics

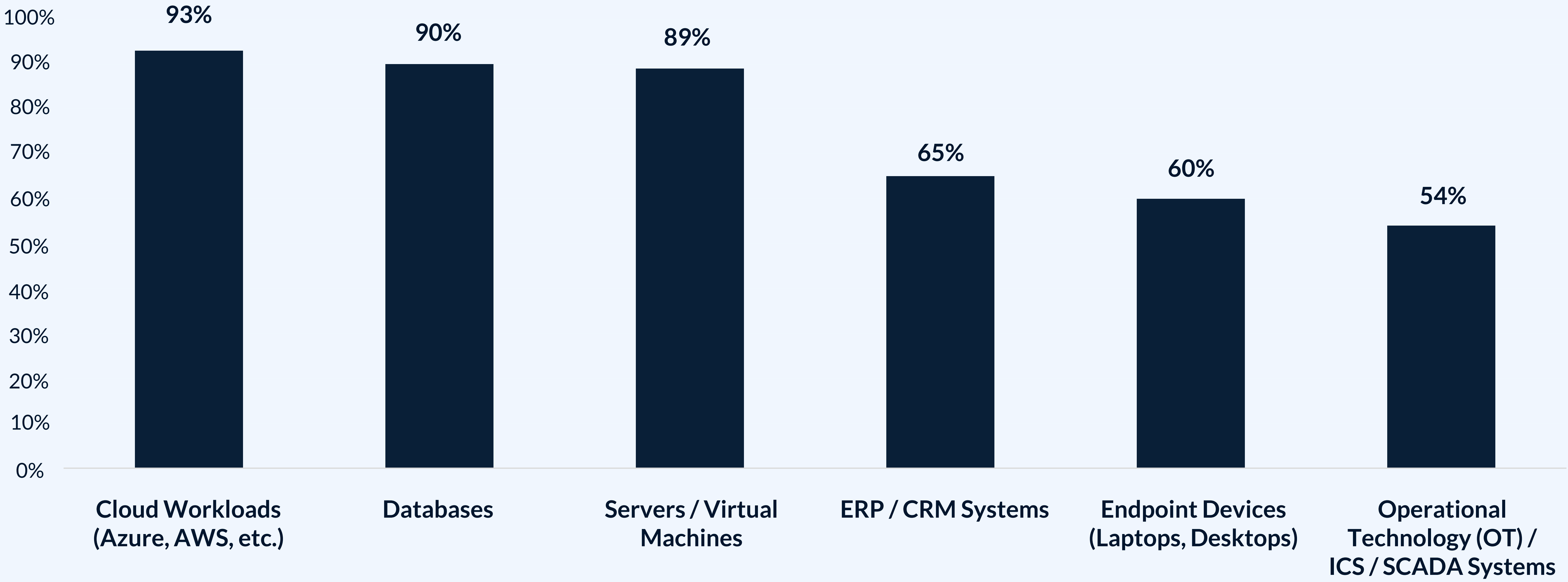
Three-quarters of manufacturers employ hybrid backup strategies, reflecting diverse system protection needs. Cloud workloads, databases, & servers lead protection priorities, while operational technology systems rank notably lower - suggesting gaps in OT protection despite their criticality to manufacturing operations.

Current Backup & Recovery Approach



- ● Hybrid Approach **(75%)**
- ● Cloud only **(23%)**
- ● On-Premise Solution **(2%)**

Systems & Data Types Managed for Backup

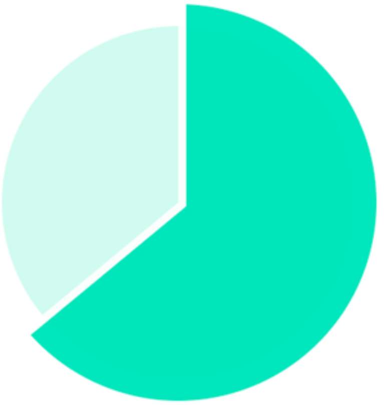


Macrium Software | NewtonX®

Base: All respondents n=100

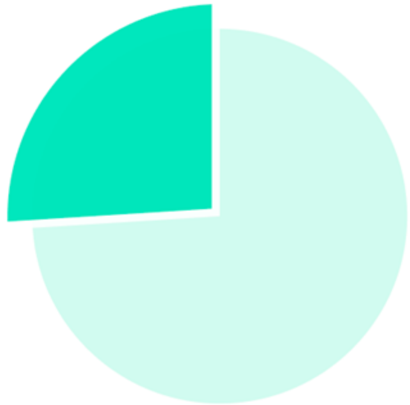
Backup & Recovery Solutions in Use

Manufacturing organizations operate highly fragmented backup environments, with nearly two-thirds (64%) using 2-3 different solutions & over a quarter (26%) deploying four or more tools to protect their IT & OT systems.



64%

2-3 different solutions



26%

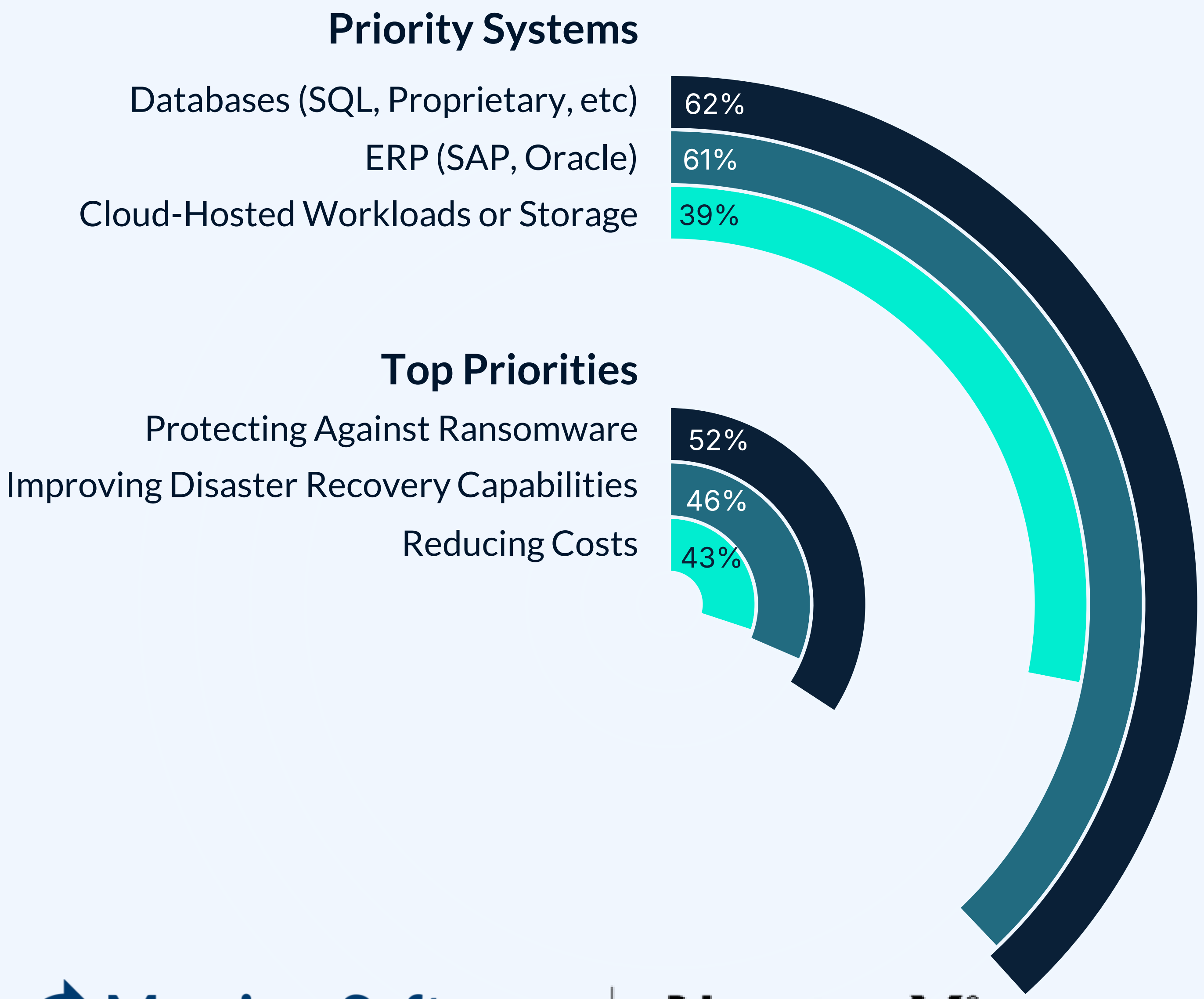
4 or more tools

Macrium Software | NewtonX®

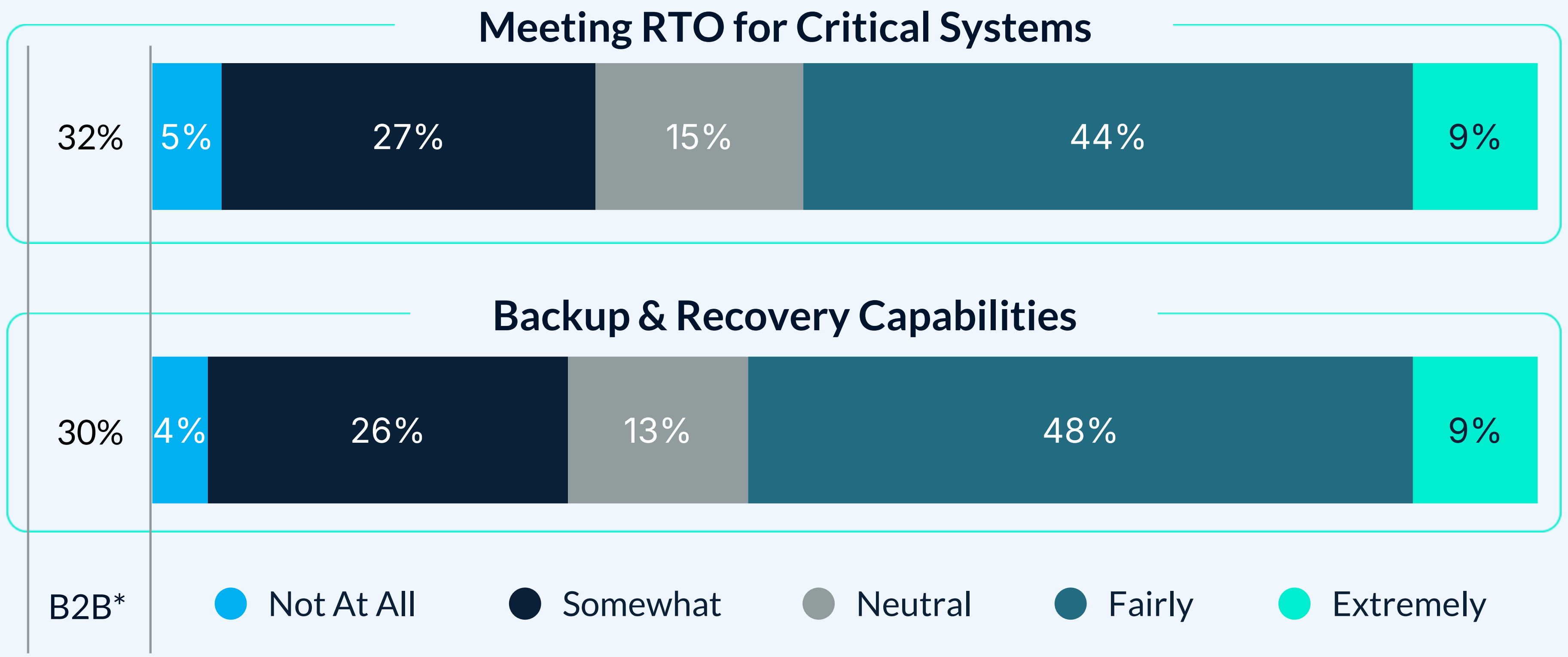
Base: All respondents n=100

Manufacturers focus backup on core business systems - databases, ERP, & cloud workloads—while prioritizing ransomware defense & disaster recovery. However, a third lack confidence in meeting RTOs for critical systems & in overall backup capabilities. This gap between investment & confidence suggests that deploying backup solutions does not guarantee operational readiness when recovery is needed.

Backup & Recovery Strategy



Confidence in...



UK is not as confident as North America in Backup & Recovery Capabilities (B2B* 46% vs. 27%)

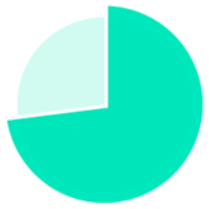
Base: All respondents n=100

* B2B = Bottom 2 box (Those selecting “Not at all confident” or “Somewhat confident”

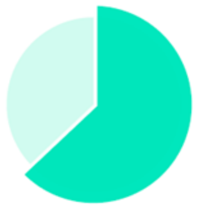
KPI Tracking For Backup & Recovery

Manufacturers prioritize time-based recovery metrics, with 73% tracking RTO & 63% monitoring RPO, reflecting the critical importance of minimizing downtime. However, a concerning gap emerges in validation practices: only 25% track recovery test frequency, & just 44% monitor the amount of data successfully recovered.

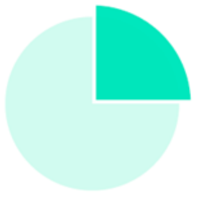
This reveals that organizations are measuring what's easy to track- backup completion rates & theoretical recovery times - rather than validating whether systems can actually be recovered when needed, creating dangerous blind spots that may only become apparent during actual production outages.



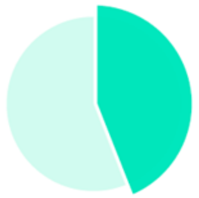
73%
track RTO



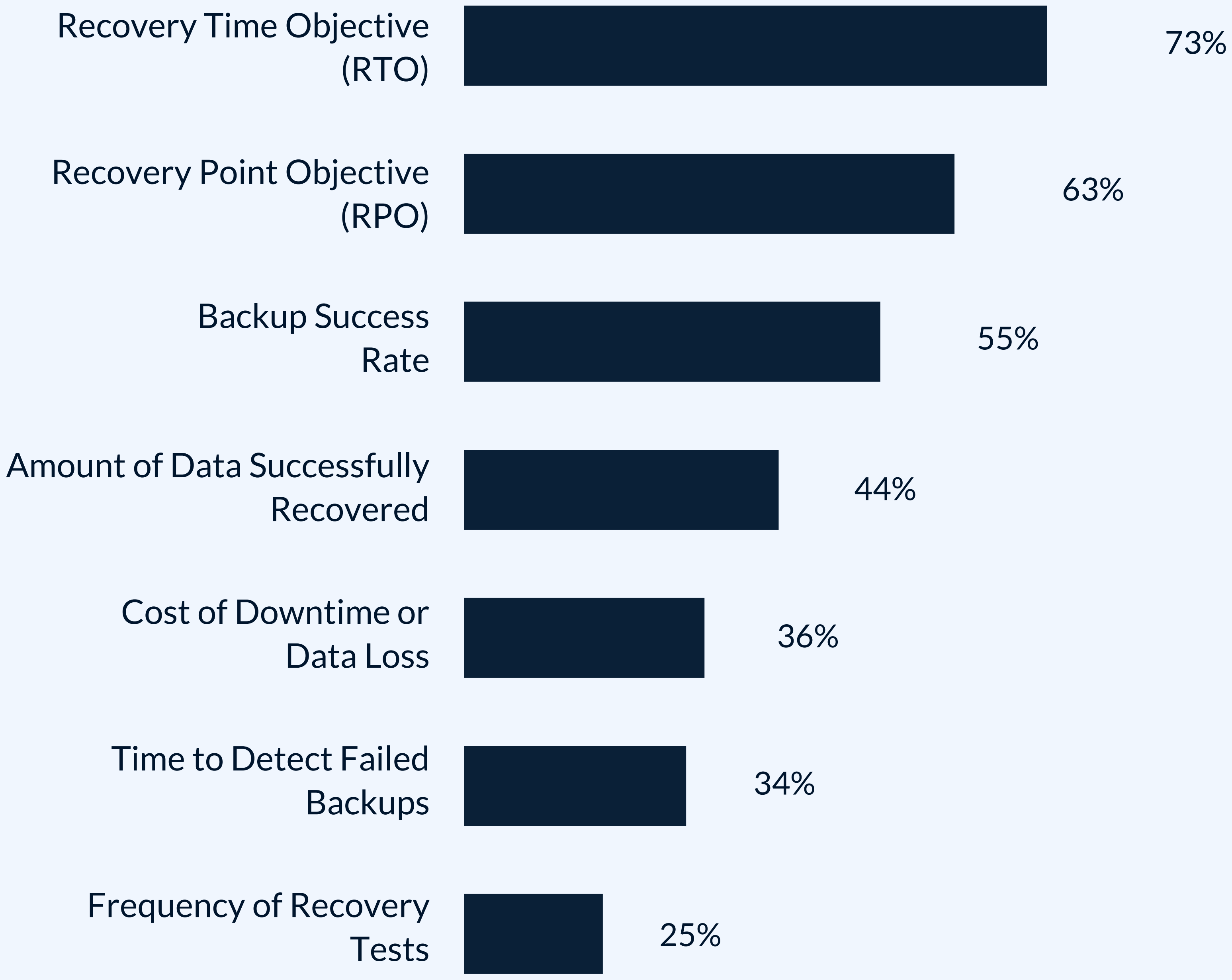
63%
monitor RPO



25%
track recovery test frequency



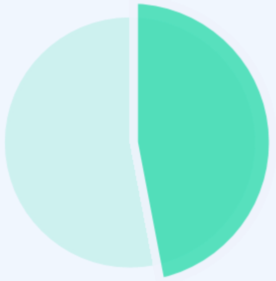
44%
monitor amount of data recovered



Base: All respondents n=100

Manufacturers operate predominantly hybrid environments, balancing modern and legacy systems. Cloud connectivity across production systems is rising, with many manufacturers now integrating cloud services into a substantial share of environments. However, recent high-profile vendor outages and supply-chain incidents are raising questions about how OT operations can stay resilient when disruption originates outside the plant.

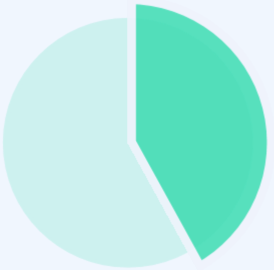
IT & OT Infrastructure



47%

Balanced Mix

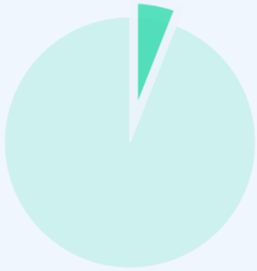
Approximately Equal Mix Of Modern & Legacy Systems



42%

Mostly Modern

Majority Current Systems With Some Legacy Still In Operation

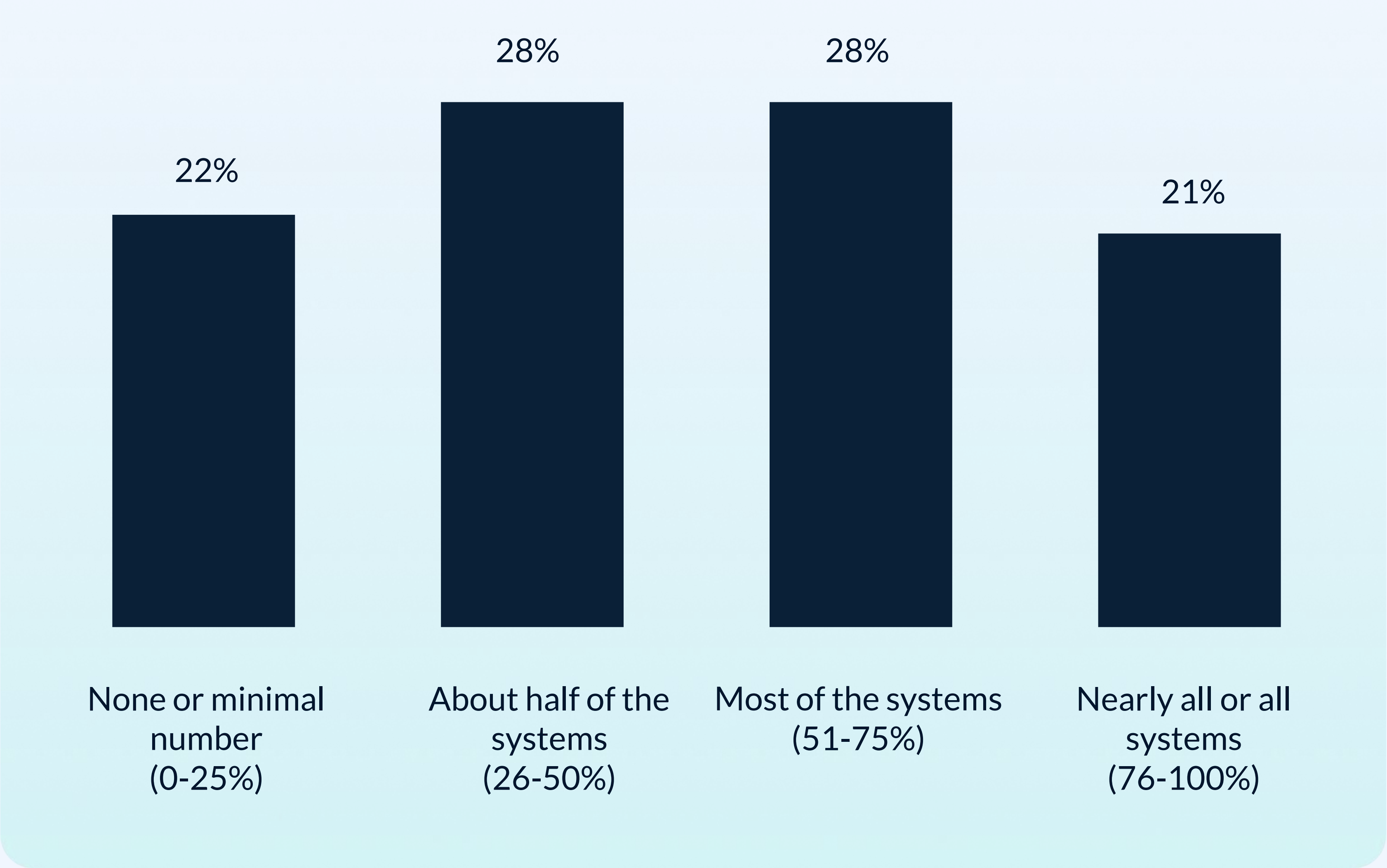


6%

Fully Modern

All Current-generation Systems & Cloud Infrastructure

Cloud-connected Manufacturing & Production Systems



Base: All respondents n=100

Risks, Resilience & Recovery Performance

Key Insights

Internal Operations Drive Downtime, With Severe Financial Consequences

Most manufacturers experience regular unplanned downtime, with operational missteps - not cyberattacks. Failed maintenance, configuration errors, & infrastructure failures dominate causes. Financial stakes are severe, with many facing six-figure hourly losses, yet recovery times consistently stretch beyond acceptable thresholds.

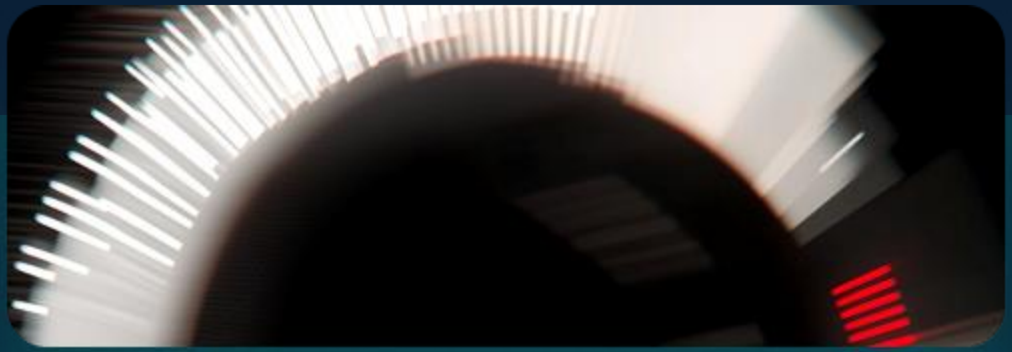
Testing Reveals Critical Gaps Between Plans & Performance

Only a small fraction meet stated recovery objectives during validation exercises, with many performing significantly slower & some never testing comprehensively. Organizations monitor operational metrics regularly but conduct full-scale exercises just once or twice annually. Backup completion is tracked continuously while recovery capability remains unproven until actual failures occur.

Dependencies, Compliance, & Vendor Proximity Shape Strategy

Manufacturers express widespread concern about third-party dependencies, with most considering vendor location strategically important. Compliance adds complexity through multiple frameworks with regional divergence. Recent disruptions have elevated backup priorities, though many still view system protection through a cybersecurity lens rather than broader operational resilience perspective.

Key Insights
Current Priorities



Shift focus from prevention to recovery speed given that internal operational issues drive most downtime

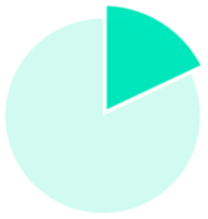
Regular, comprehensive testing must replace infrequent disaster recovery exercises to validate actual capabilities

Recovery time reduction should be prioritized given the substantial financial impact of extended outages

Recovery Process Lead for Downtime Events

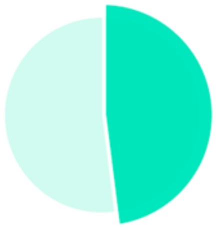
IT leadership drives recovery in nearly half of manufacturers, with joint IT/OT coordination teams handling two-fifths.

However, testing exposes a troubling disconnect: only 18% meet or exceed their recovery time targets, while 48% perform slightly slower & 26% fall significantly short of their RTOs. An additional 6% haven't conducted full recovery tests at all, meaning they operate without validated knowledge of their actual recovery capabilities.



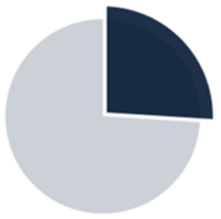
18%

meet or exceed recovery time targets



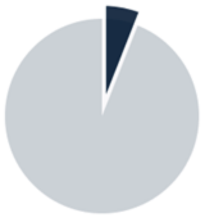
48%

perform slightly slower



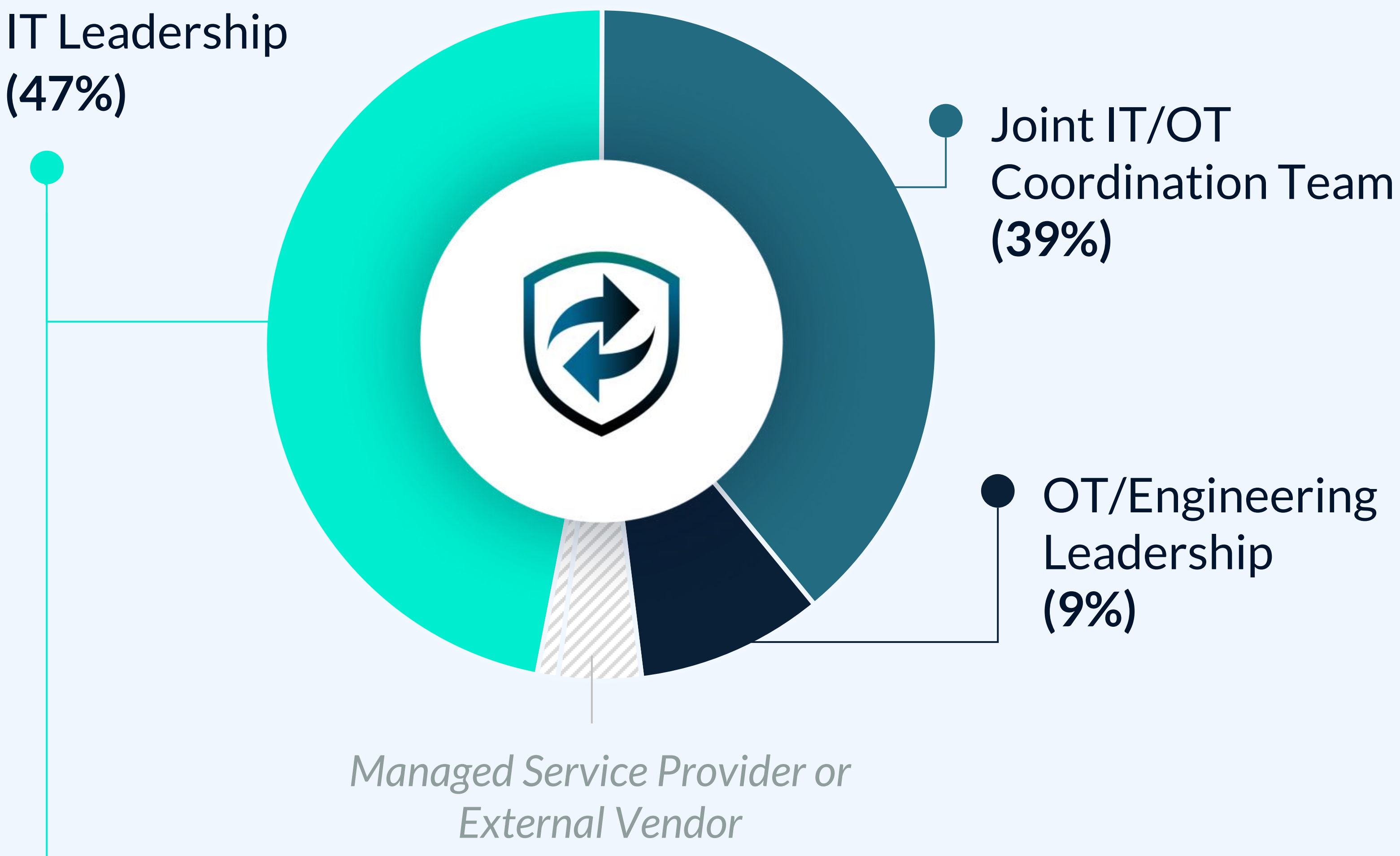
26%

fall short of RTOs



6%

haven’t conducted full recovery tests



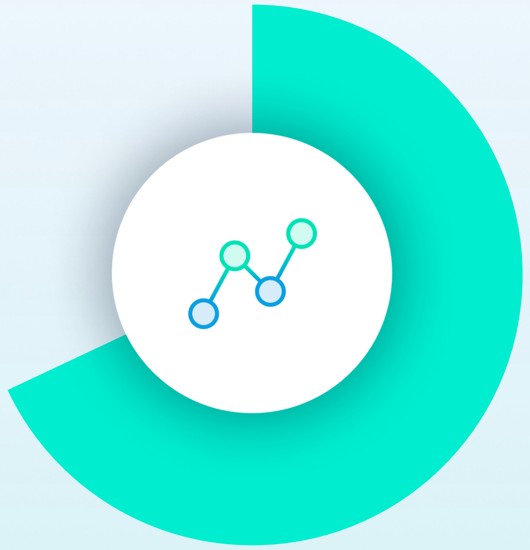
Higher for **North America** (54%) vs. UK (27%)

Base: All respondents n=100

While two-thirds of manufacturers review performance metrics monthly or quarterly, validation practices lag behind. Half test backups with similar frequency, but 60% conduct full disaster recovery exercises only twice yearly or annually. This gap between monitoring & validation means organizations track backup completion without regularly confirming actual recovery capability when systems fail.

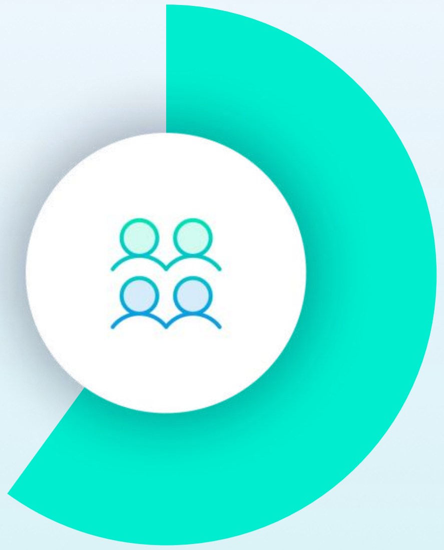
Frequency of...

Backup & Recovery Performance Metrics Review



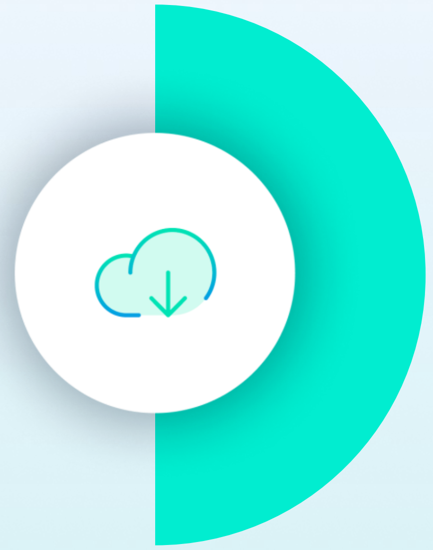
68%
Monthly or Quarterly

Organization-wide Backup Or Disaster Recovery Tabletop Exercises



60%
Twice Per Year or Annually

Backups Testing Or Validation To Ensure Systems Can Be Successfully Recovered

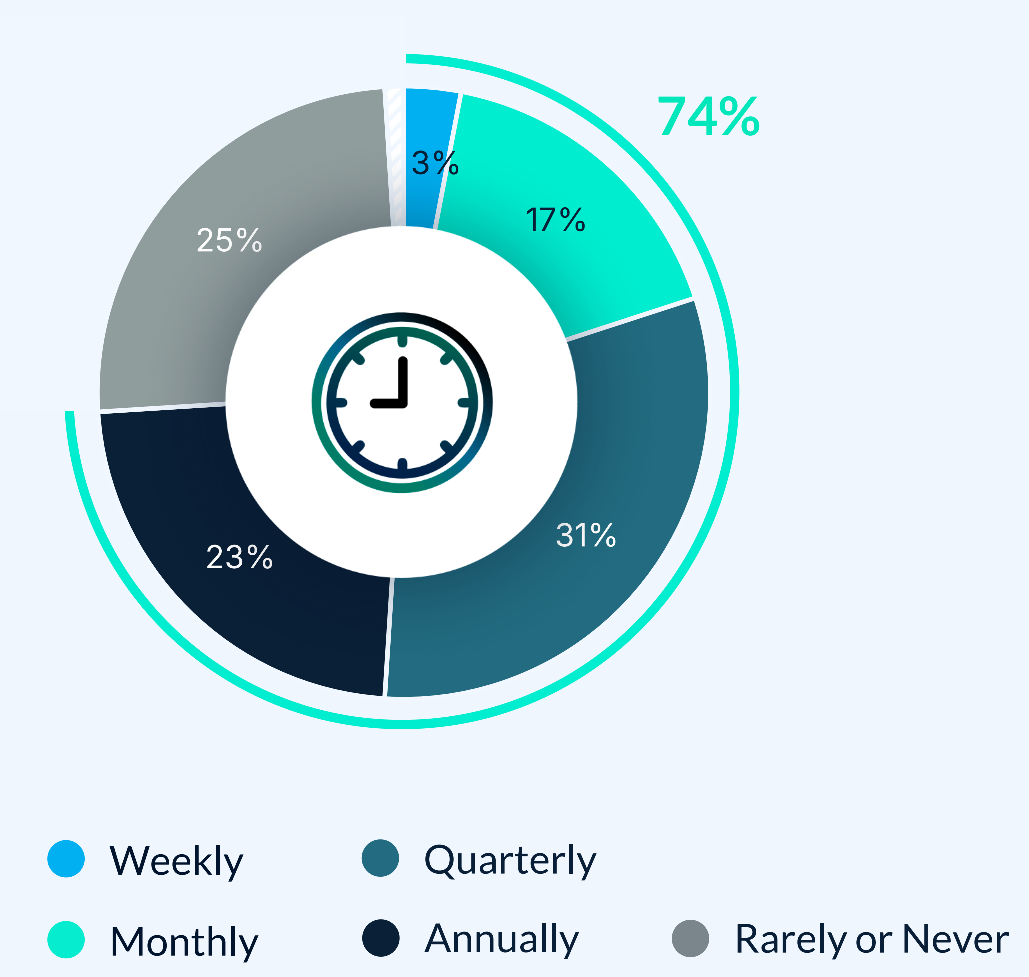


50%
Monthly or Quarterly

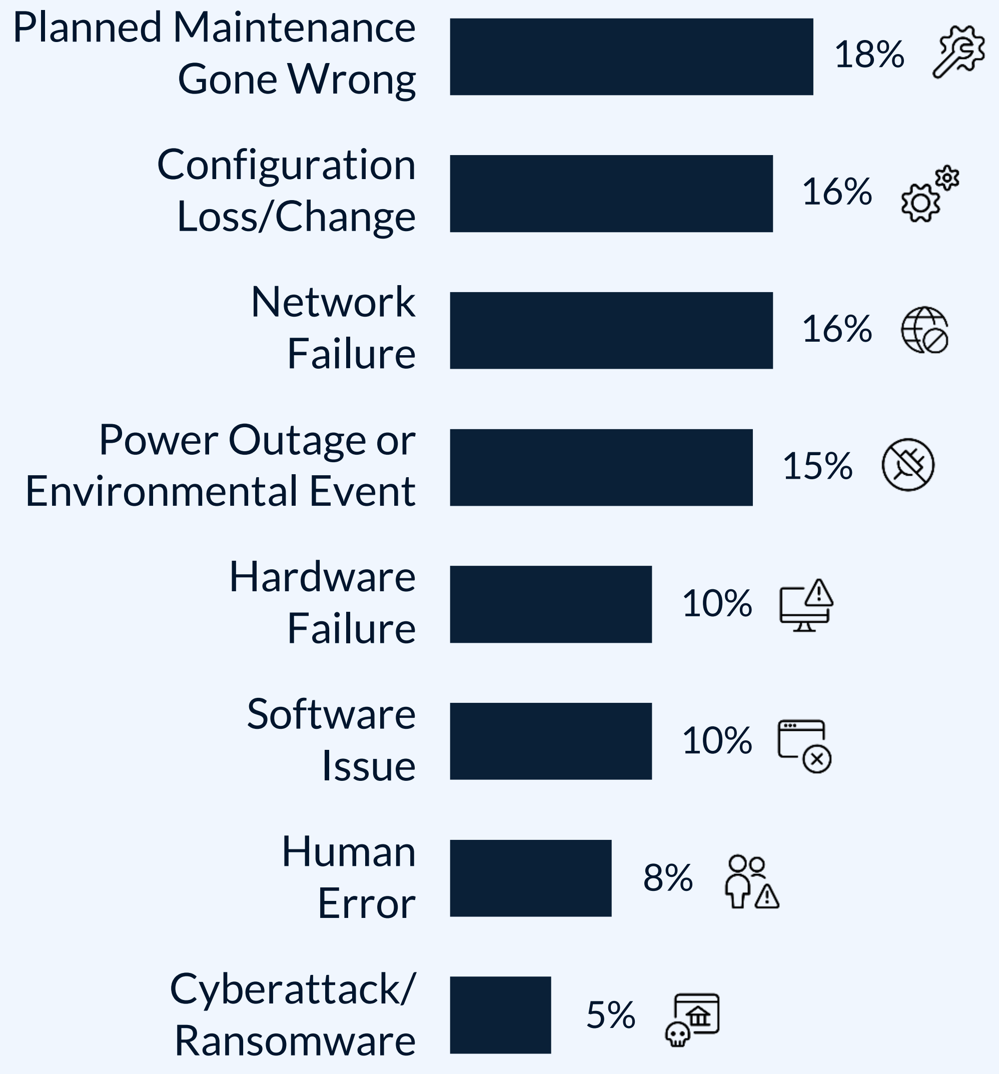
Base: All respondents n=100

Three-quarters of manufacturers experience downtime at least annually, with planned maintenance gone wrong as the leading cause, followed by configuration loss & network failures. This reveals most outages stem from internal operations rather than external attacks. Nearly half in North America & over a third in the UK estimate downtime costs exceeding $100K per hour.

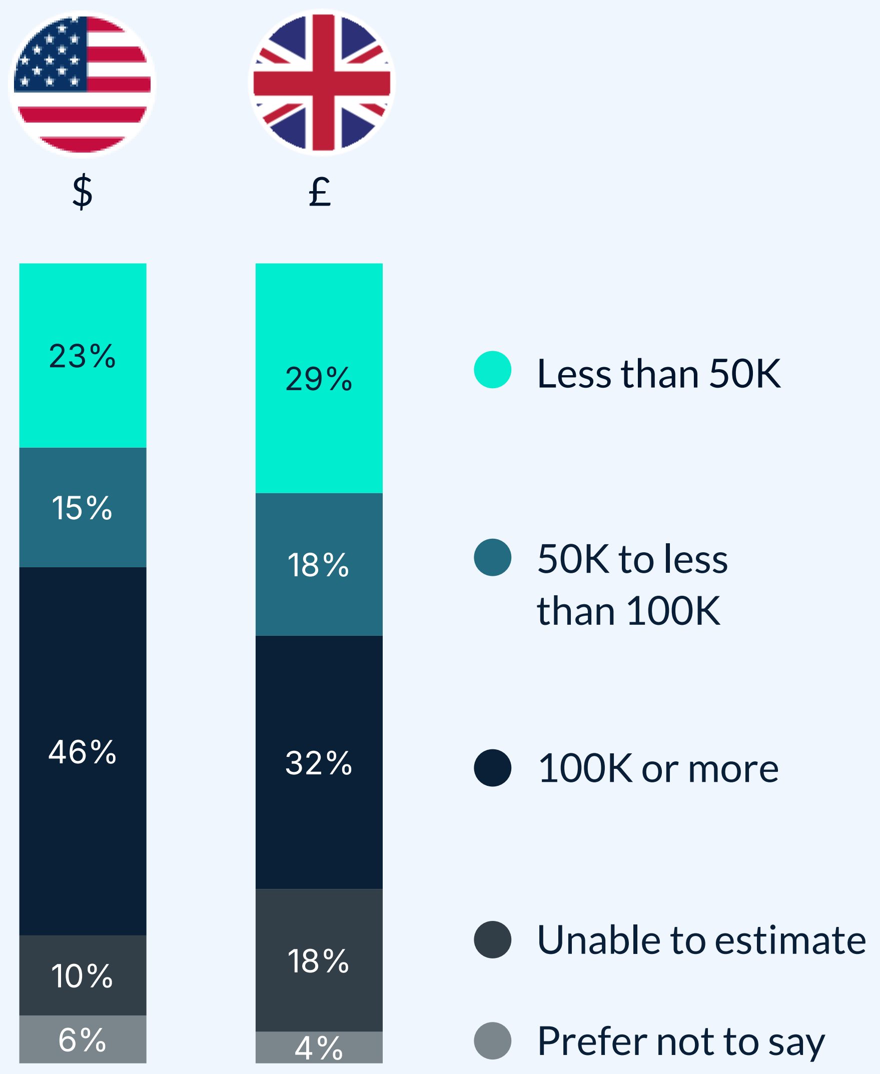
Downtime Frequency



Downtime Main Causes



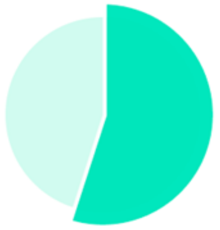
Downtime Cost Per Hour



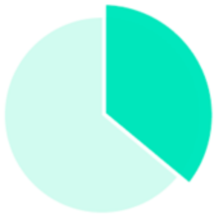
Base: All respondents n=100

Over half (55%) of manufacturing organizations experienced a ransomware incident in the past year, though most were successfully prevented or contained - 36% were blocked entirely & 11% were detected with minimal impact. However, 8% faced significant operational downtime, demonstrating that defenses remain imperfect.

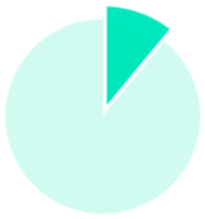
More concerning is the recovery time reality: three-quarters of organizations require over two hours to restore operations.



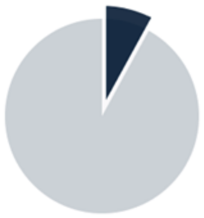
55%
experienced a ransomware incident in past year



36%
blocked entirely

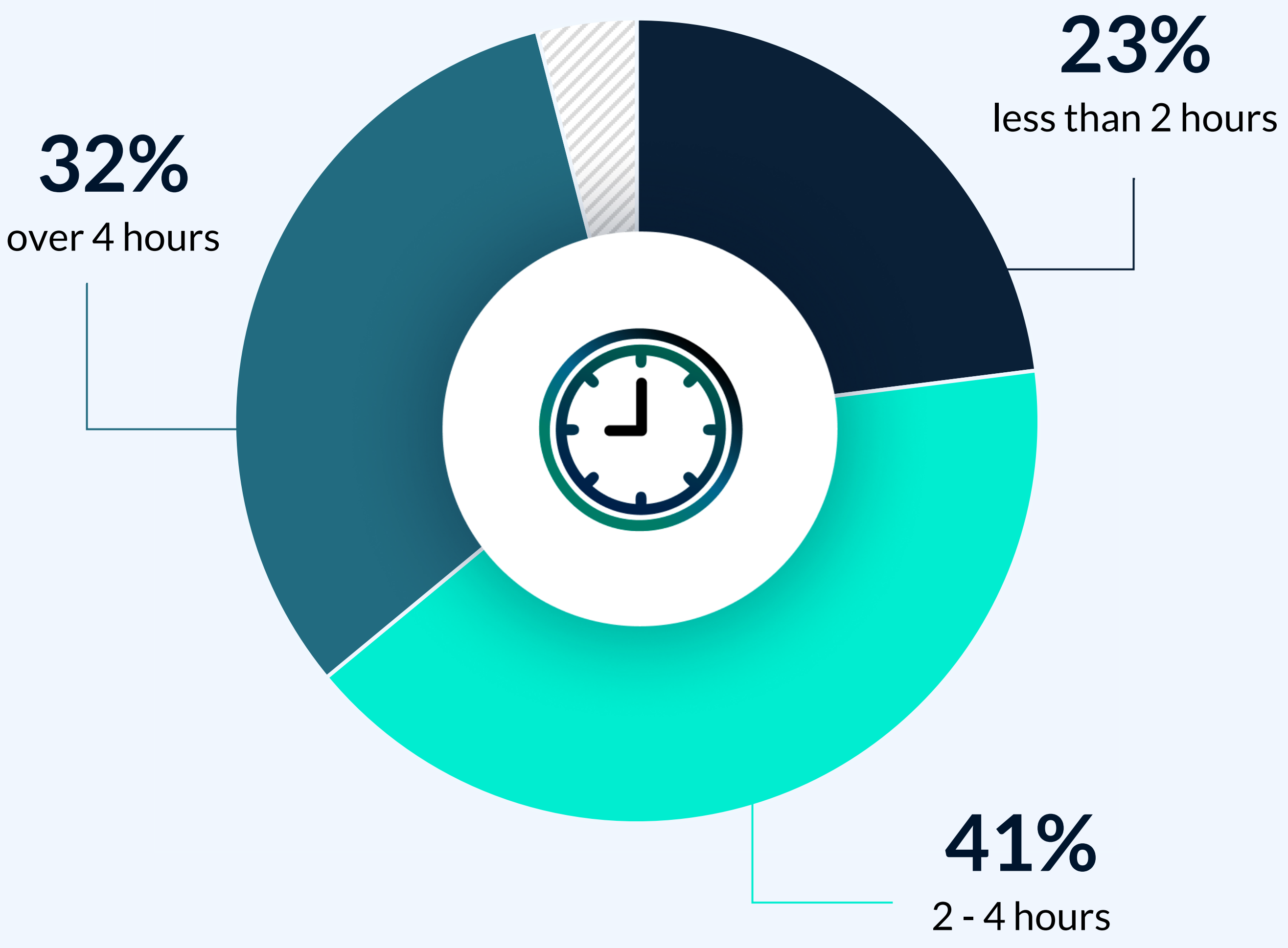


11%
detected with minimal impact



8%
significant operational downtime

Typical Recovery Time During Downtime

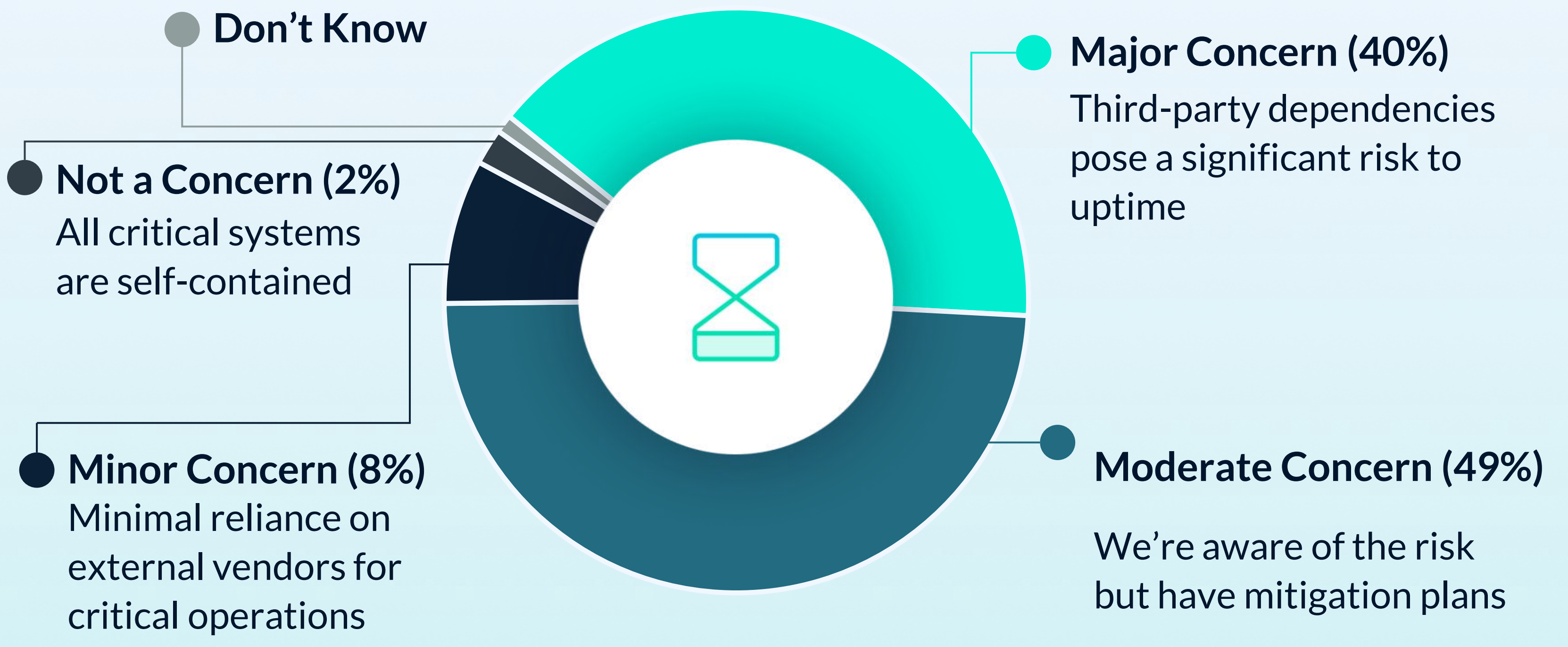


Recovery time is longer in **North America** vs. UK (over 4 hours 39% vs. 12%)

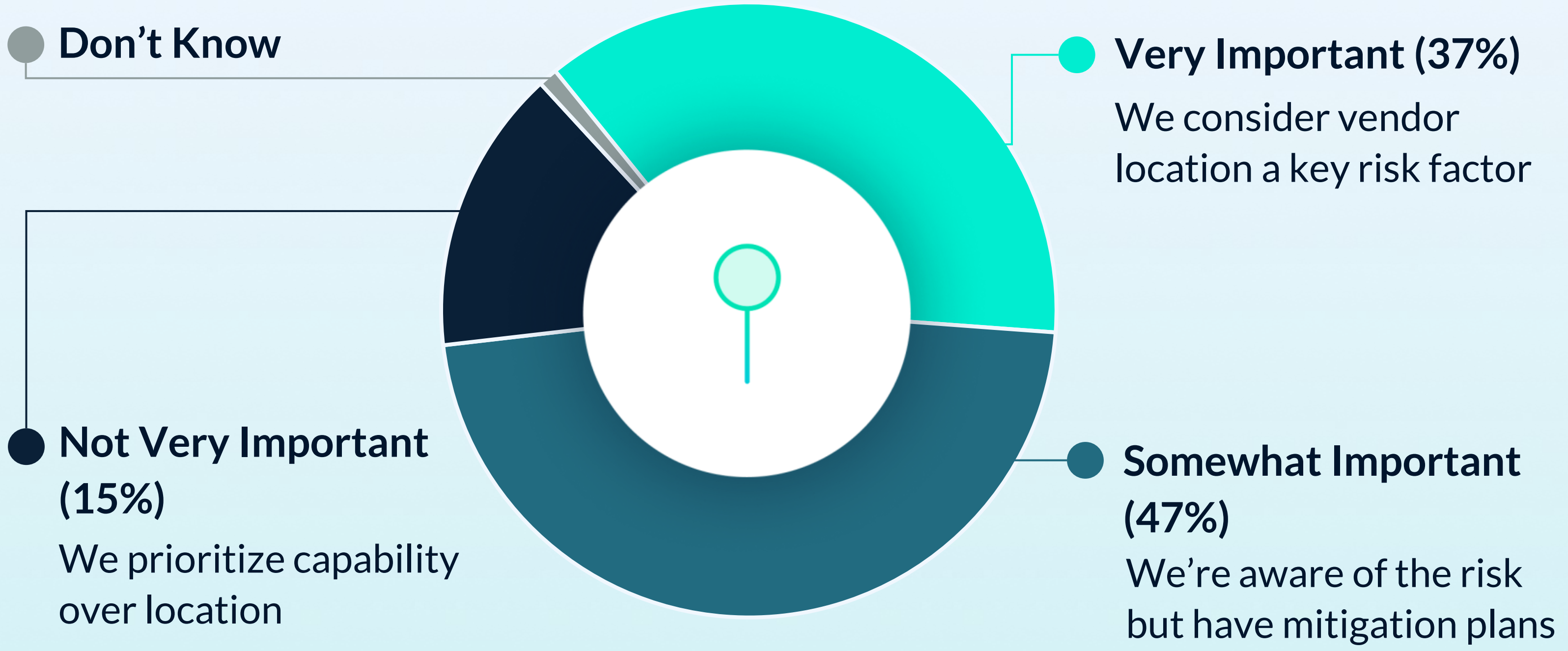
Base: All respondents n=100

Nearly nine in ten manufacturers express concern about third-party dependencies, reflecting heightened awareness of supply chain vulnerabilities. Over four in five also consider vendor regional location important to their resilience strategy, suggesting that backup effectiveness depends not only on solution capabilities, but also on vendor proximity, data sovereignty, & local support during critical recovery scenarios.

Concerns Over Third-Party & Supply Dependencies During Downtime



Importance Of Vendor Location For Resilience & Data Strategy

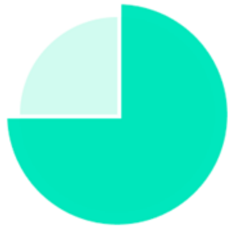


Third-Party & Supply Chain Dependencies are more of a **major concern** for **UK** vs. North America (62% vs. 32%)

Base: All respondents n=100

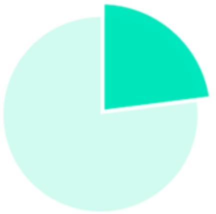
Recent operational disruptions have catalyzed significant shifts in backup & recovery priorities, with three-quarters of manufacturers reporting some level of impact. Among affected organizations, backup & recovery have become elevated priorities, with half reporting that resilience plans are now being reviewed in response to outages.

Only 23% indicate that recent incidents did not impact their backup priorities, with cybersecurity remaining their primary strategic focus.



75%

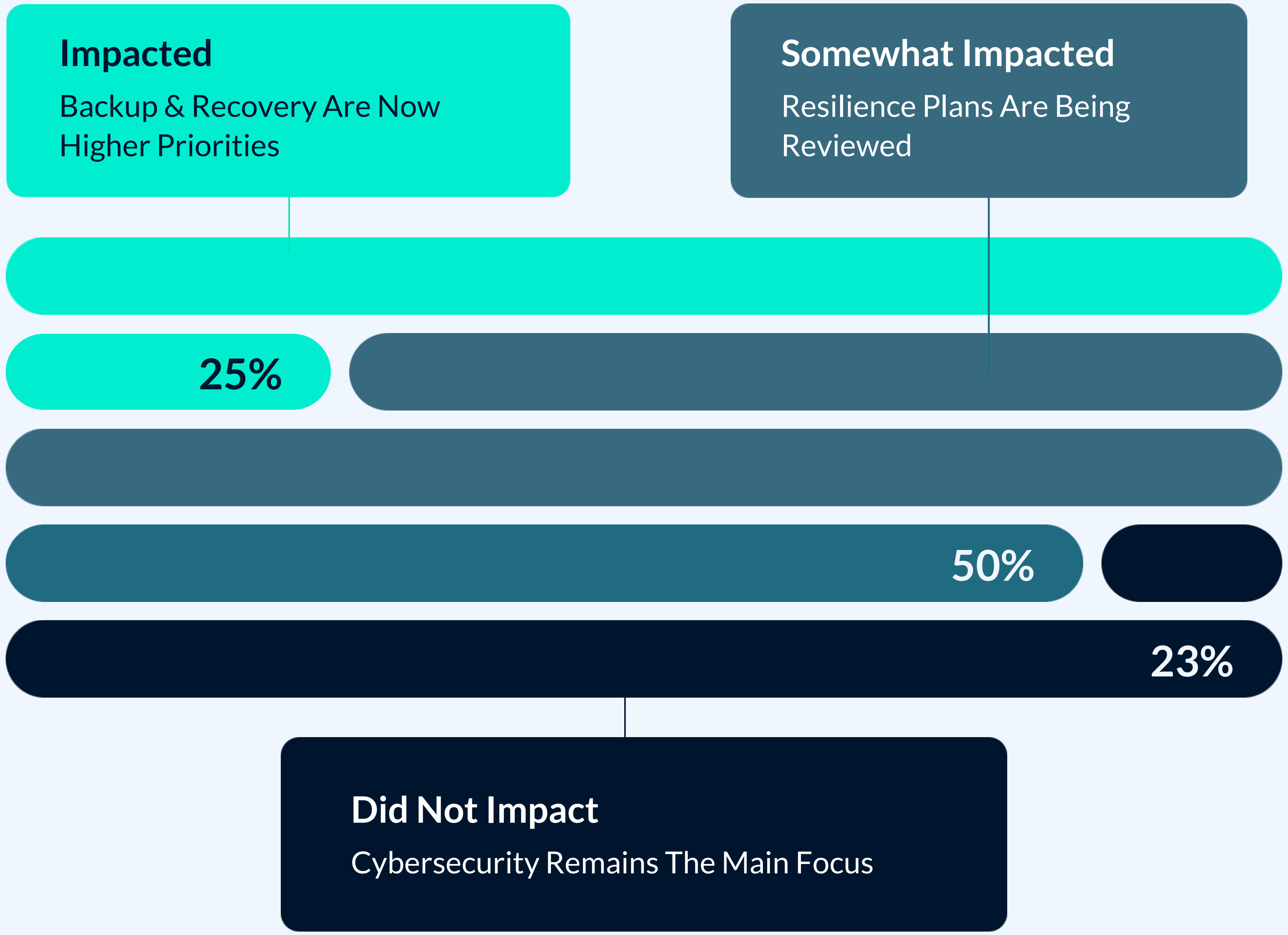
some level of impact



23%

cybersecurity as primary strategic focus

Impact Of Recent Outages On Backup & Recovery Priorities

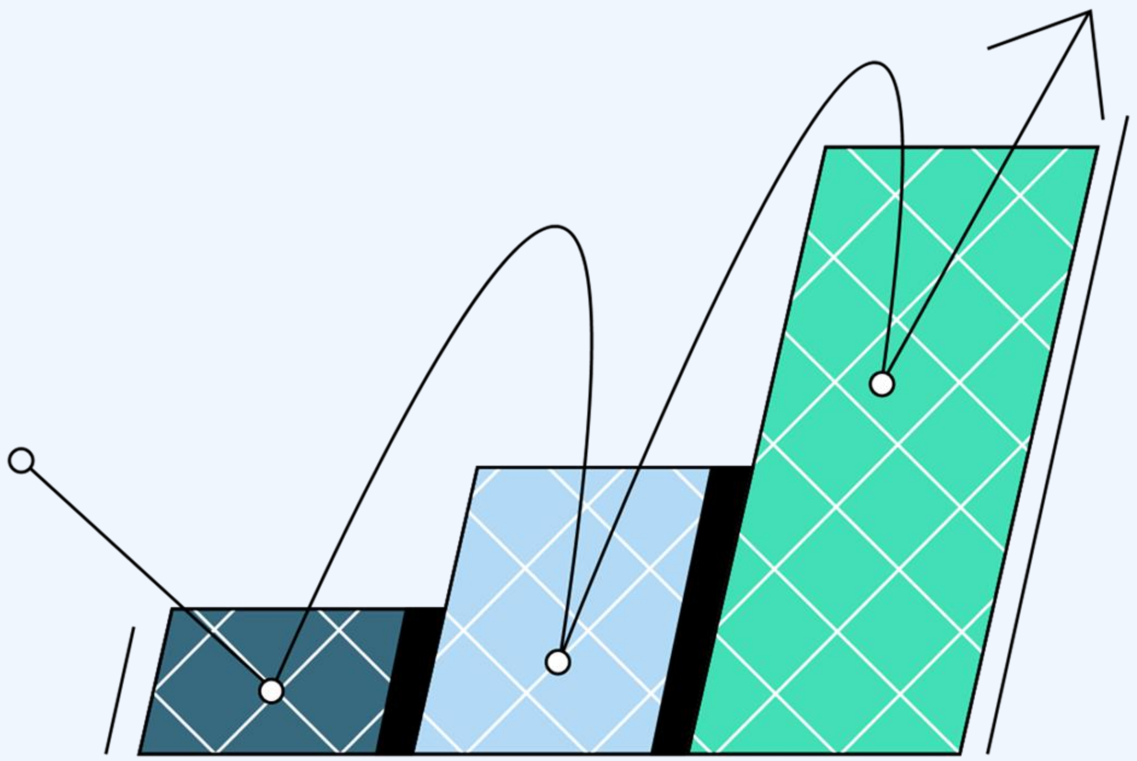


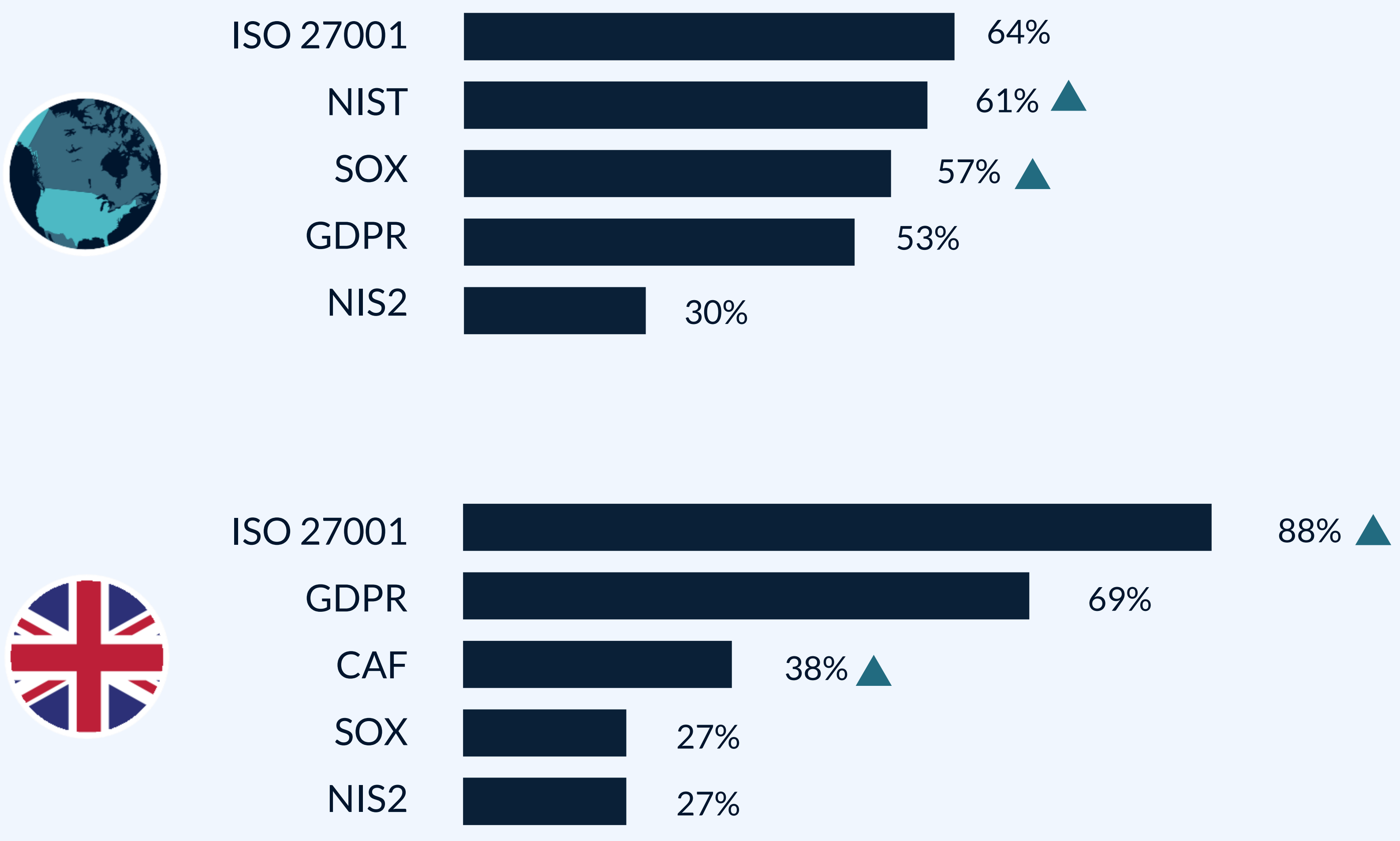
Base: All respondents n=100

Compliance Frameworks Relevant To Backup & Recovery Operations

ISO 27001 (Information Security Management) is the leading compliance standard in both North America & the UK. GDPR ranks high in both markets due to cross-border system protection requirements.

However, notable regional divergence appears in secondary frameworks, suggesting manufacturers must navigate a complex, multi-framework compliance landscape where universal standards like ISO 27001 provide baseline coverage, but regional operations demand additional, market-specific compliance measures that directly shape backup & recovery requirements.





▲ = Higher for specified market

Base: All respondents n=100 – North America = 74; UK = 26

Organizational Dynamics & Challenges

Key Insights

Internal Operations Drive Downtime, With Severe Financial Consequences

Most manufacturers experience regular unplanned downtime, with operational missteps - not cyberattacks. Failed maintenance, configuration errors, & infrastructure failures dominate causes. Financial stakes are severe, with many facing six-figure hourly losses, yet recovery times consistently stretch beyond acceptable thresholds.

Testing Reveals Critical Gaps Between Plans & Performance

Only a small fraction meet stated recovery objectives during validation exercises, with many performing significantly slower & some never testing comprehensively. Organizations monitor operational metrics regularly but conduct full-scale exercises just once or twice annually. Backup completion is tracked continuously while recovery capability remains unproven until actual failures occur.

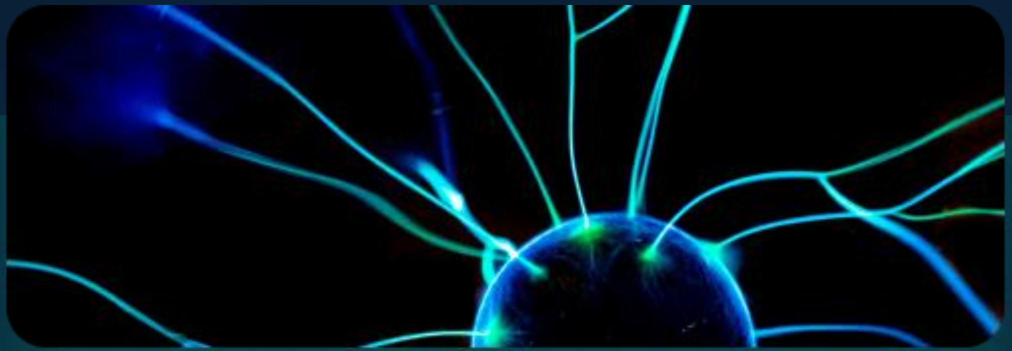
Dependencies, Compliance, & Vendor Proximity Shape Strategy

Manufacturers express widespread concern about third-party dependencies, with most considering vendor location strategically important. Compliance adds complexity through multiple frameworks with regional divergence. Recent disruptions have elevated backup priorities, though many still view system protection through a cybersecurity lens rather than broader operational resilience perspective.

Key Insights
Current Priorities

Address internal operational quality as the primary downtime driver

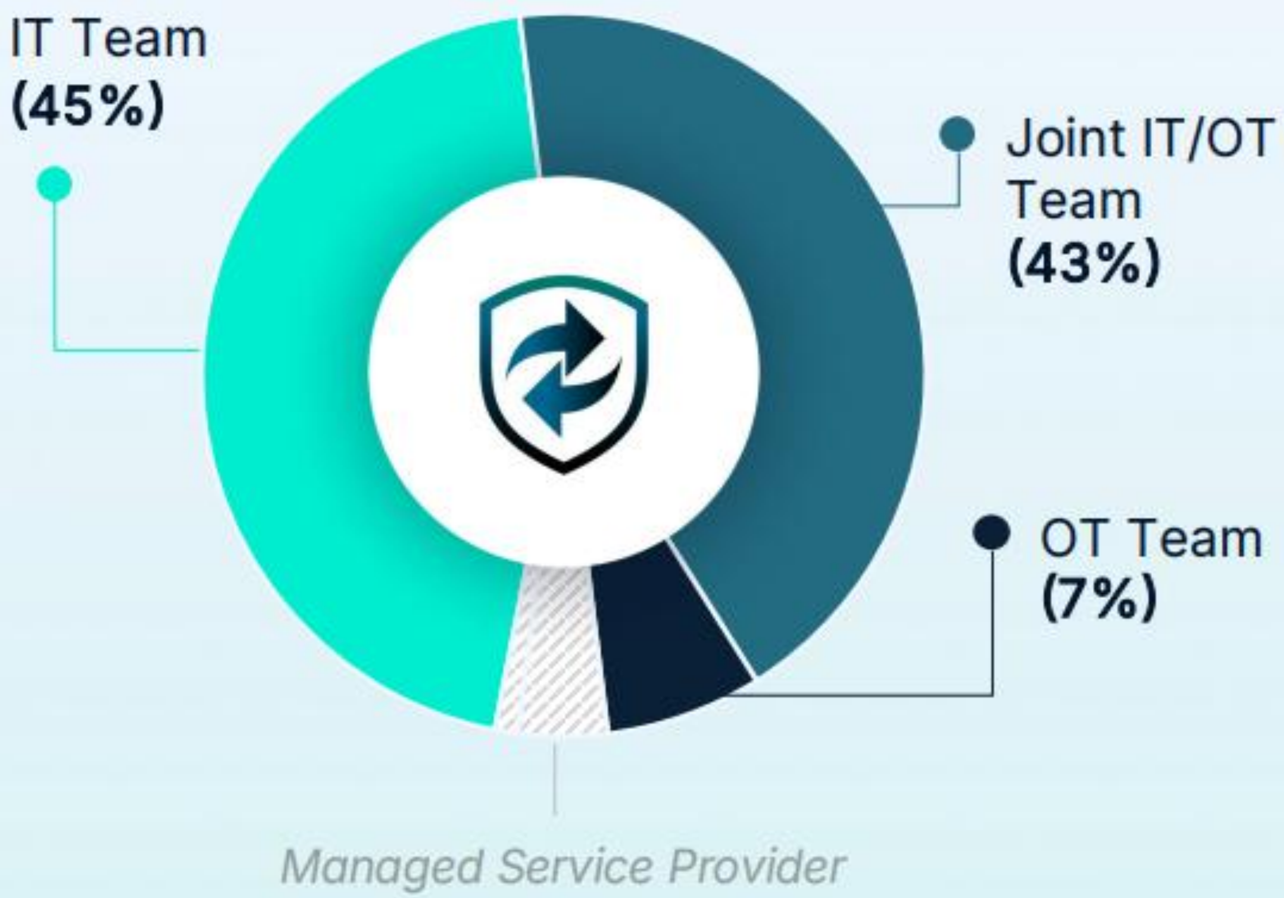
Increase testing frequency to validate theoretical capabilities



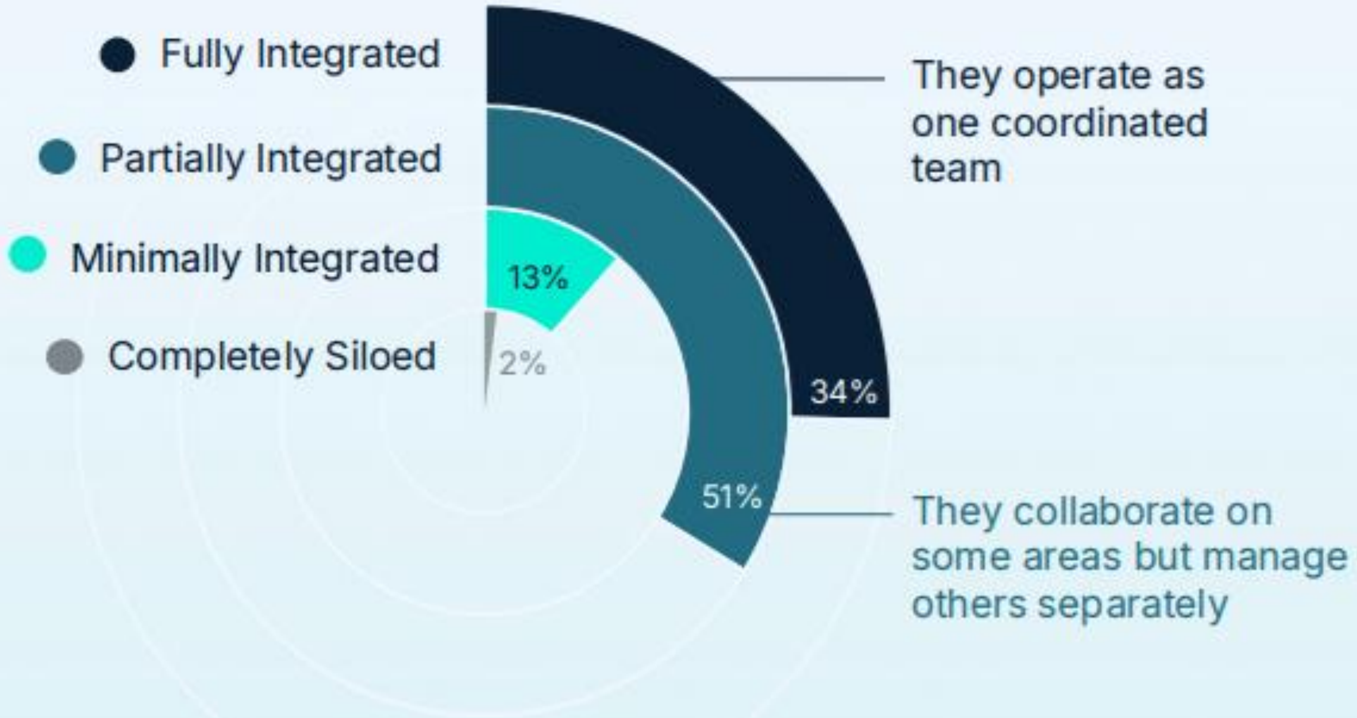
Adopt operational resilience mindset beyond cyber-focused approaches

OT backup ownership is nearly evenly split between IT teams & joint IT/OT teams, yet only a third achieve full integration. Most organizations operate in partial coordination, collaborating on some areas while managing others separately. This disconnect creates significant risk, as effective OT backup requires deep operational knowledge that siloed IT teams may lack.

Owners of OT Backup & Recovery Management



IT & OT Team Integration for Backup & Recovery



Partial / full integration is more prevalent in **North America** (91%) vs. UK (69%)

Base: All respondents n=100

Cultural Silos & Technical Complexity Dominate IT/OT Collaboration Challenges

45%
Cultural & Organizational Silos

Challenges Related To Team Dynamics, Trust, Priorities, Mindsets, & Departmental Separation Between IT & OT

20%
Technical Integration & Infrastructure

Issues With Legacy Systems, Incompatible Tools, Network Segmentation, & Technical Complexity Of Integrating IT & OT Environments

12%
Governance & Ownership Clarity

Lack Of Clear Roles, Responsibilities, Decision-Making Authority, & Accountability Between IT & OT Teams

8%
Resource & Budget Constraints

Financial Limitations, Competing Budget Priorities, & Insufficient Resources For Collaboration Initiatives

> “Working in silos, lack of understanding of integrations & dependencies on tightly coupled architecture.”

Department head or line of business head, Automotive, Transportation & Parts Manufacturing, UK

> “The biggest challenge is the clash of priorities & culture. For OT the primary priority is uptime & safety.”

Department head or line of business head, Healthcare & Medical Device Manufacturing, UK

> “OT sets the strategy but IT owns the infrastructure. So coordinating is challenging.”

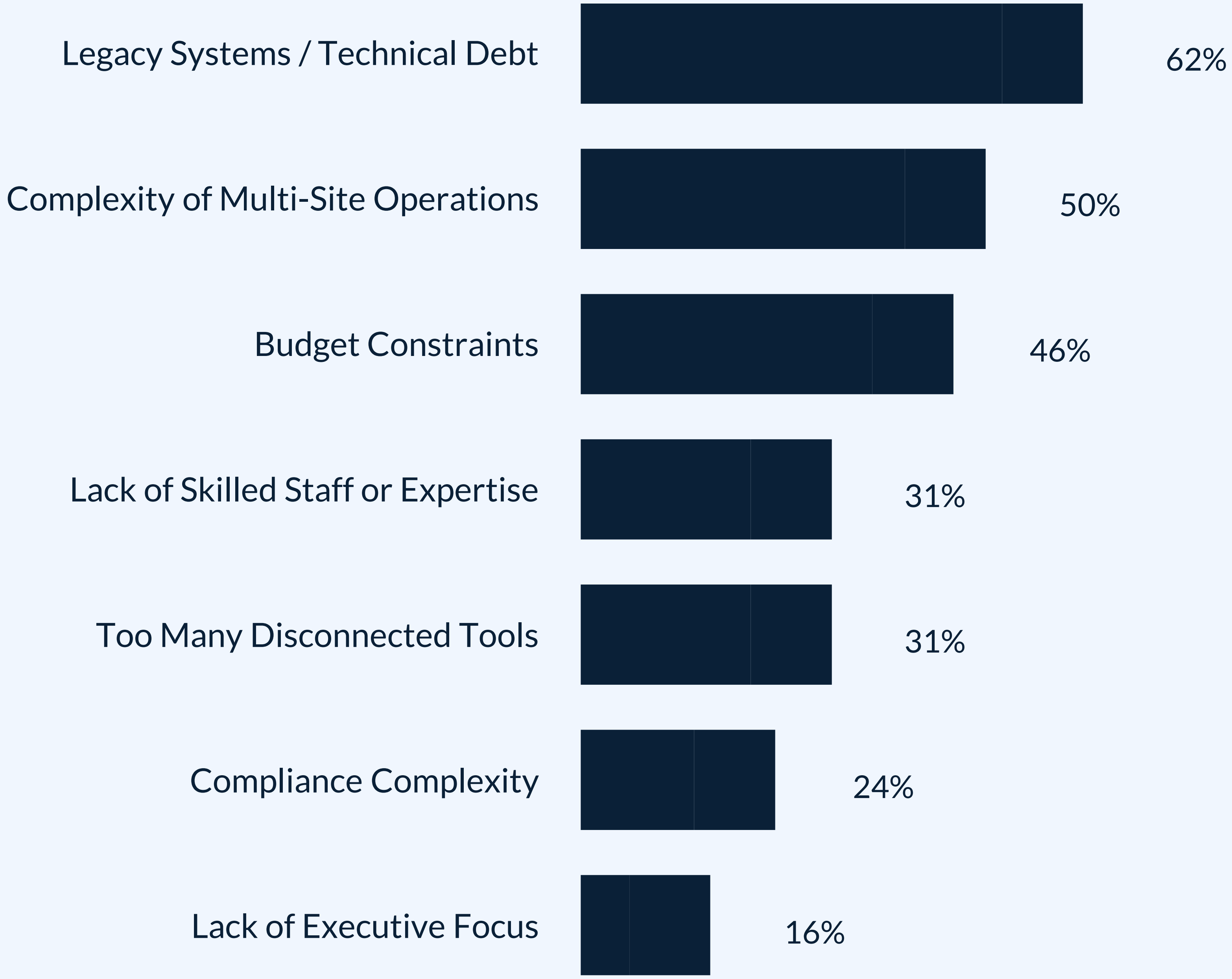
Senior director or Director Food, Beverage & Agricultural Product Manufacturing, US

Base: All respondents n=100

Key Challenges in Enhancing Backup & Recovery

Legacy systems & technical debt emerge as the dominant challenge. This is closely followed by multi-site operational complexity & budget constraints, forming a trio of structural challenges that fundamentally impede progress.

Notably, skilled staff shortages & tool fragmentation rank lower, suggesting the problem isn't primarily about resources or technology sprawl, but rather the foundational burden of outdated infrastructure that resists modernization



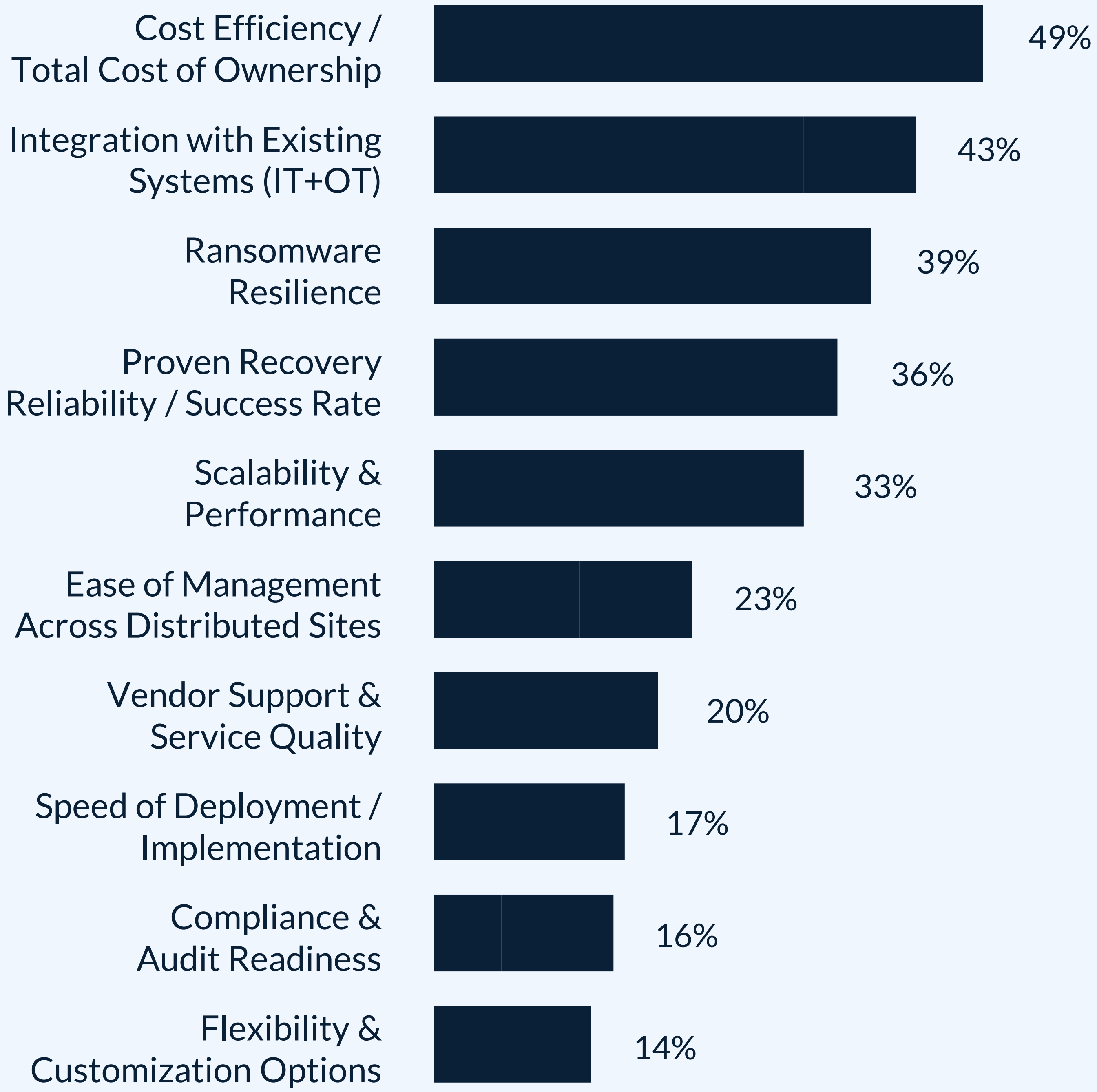
Legacy Systems / Technical Debt
62%
Complexity of Multi-Site Operations
50%
Budget Constraints
46%
Lack of Skilled Staff or Expertise
31%
Too Many Disconnected Tools
31%
Compliance Complexity
24%
Lack of Executive Focus
16%

Base: All respondents n=100

When evaluating backup & recovery solutions, manufacturers prioritize practical business outcomes over technical capabilities. Cost efficiency/total cost of ownership leads, followed closely by integration with existing IT & OT systems & ransomware - forming a clear top three that emphasizes value, compatibility, & threat protection.

The relatively lower rankings for ease of management, vendor support quality, & compliance readiness indicate these are viewed as table stakes rather than differentiators.

Key Factors In Evaluating Or Renewing Backup & Recovery Solutions



Base: All respondents n=100

Investment Priorities & Future Direction

Key Insights

Investment Growth Driven by Cyber Threats, Efficiency & Infrastructure Modernization

The overwhelming majority of manufacturers plan to increase backup spending, with cyber defense emerging as the clear top priority. Process automation & infrastructure upgrades follow closely, revealing three critical imperatives: protecting against evolving threats, improving operational efficiency, & addressing aging system vulnerabilities.

Digital Transformation Awareness Exceeds Execution

While most manufacturers recognize digital transformation's strategic importance, far fewer have committed meaningful resources to implementation. This execution gap reveals Industry 4.0 remains largely aspirational rather than operational.

Organizations appear constrained by the same barriers impeding backup modernization - legacy dependencies, financial limitations, & competing priorities. As environments grow more connected, this lag creates expanding protection requirements without corresponding capability investments.

Key Insights
Current Priorities

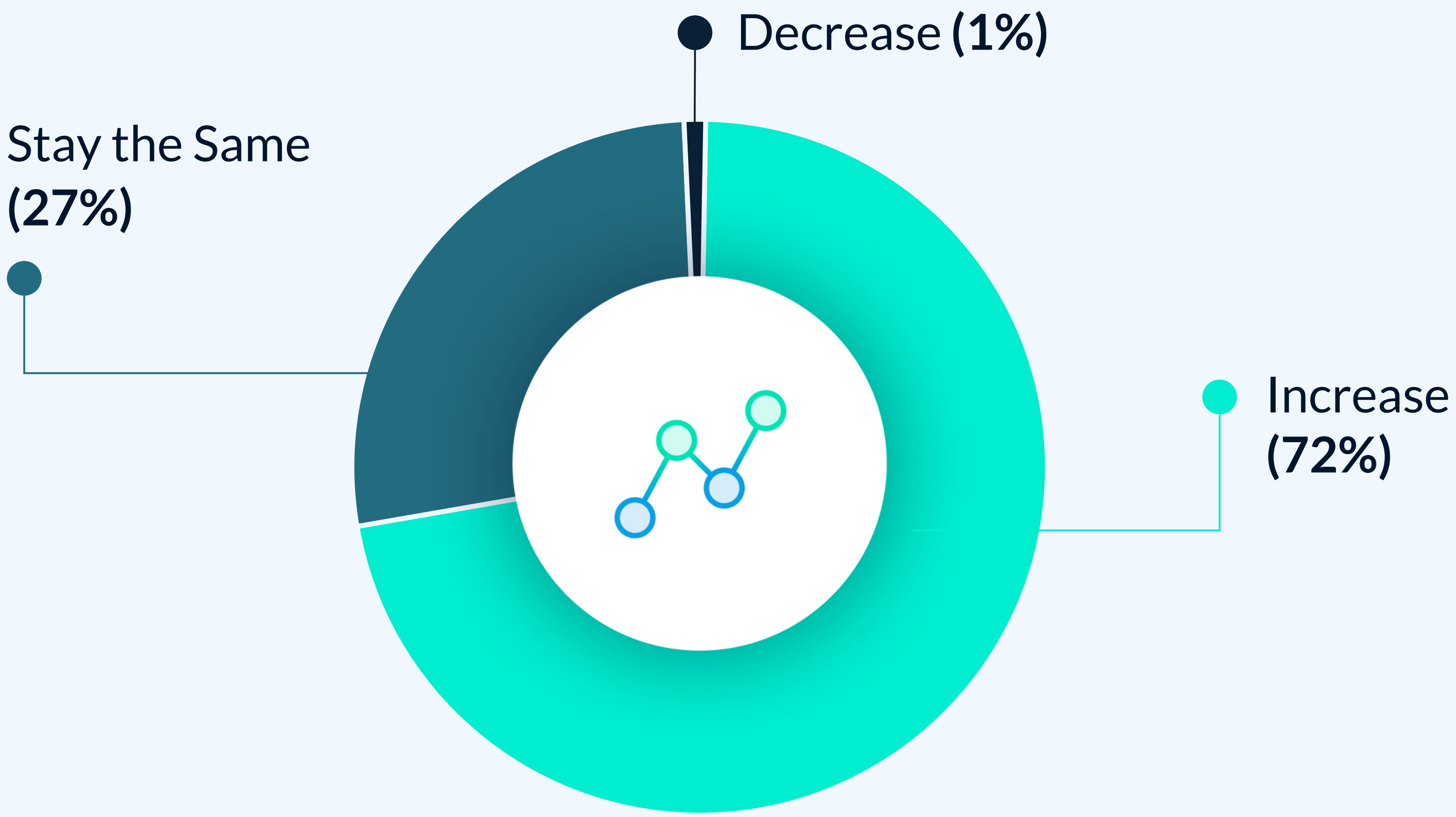
Cyber resilience dominates investment thinking, requiring solutions with proven threat defense

Legacy modernization creates opportunities for infrastructure refresh & protection upgrades

Digital transformation will eventually expand system protection requirements but investment timing remains uncertain

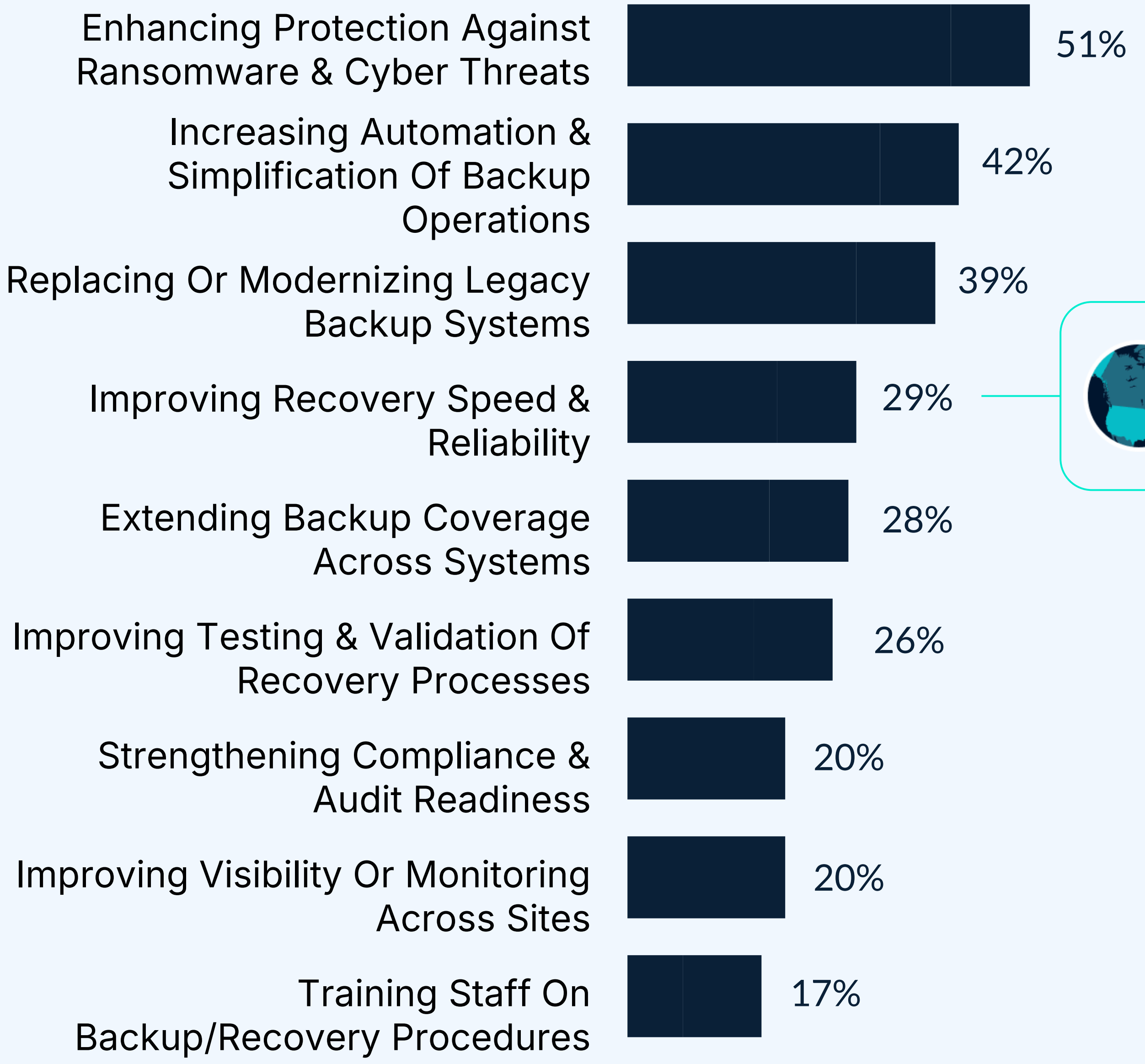
The vast majority of manufacturers are increasing backup investment, with nearly three-quarters planning budget growth. Ransomware protection dominates investment priorities, followed closely by automation & legacy system modernization- reflecting the triple challenge of escalating cyber threats, operational efficiency demands, & technical debt.

Projected Change in Backup & Recovery Spending



12% Spending Increase on Average

Investment Focus Areas



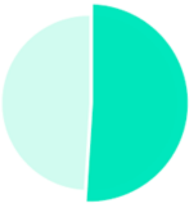
Higher for **North America** (35%) vs. UK (12%)

Base: All respondents n=100

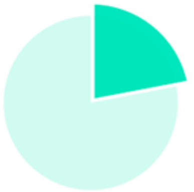
Current Industry 4.0 Focus Within Organizations

While 51% of manufacturing organizations acknowledge Industry 4.0 as an important focus, indicating widespread awareness of digital transformation imperatives, only 22% have elevated it to a top strategic priority with active investment. An additional 20% have it on the radar for future planning & 6% are discussing it without concrete plans, revealing that the vast majority recognize its importance but have yet to commit substantial resources.

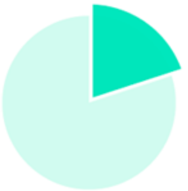
This significant execution gap suggests organizations face barriers in translating digital transformation vision into action, likely constrained by legacy system dependencies, budget limitations, & competing operational priorities.



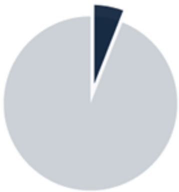
51%
acknowledge as important focus



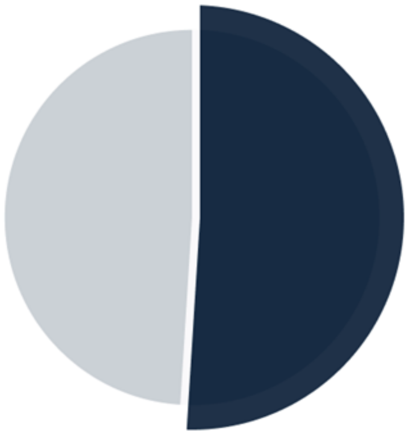
22%
elevated to top strategic priority



20%
in radar for future planning

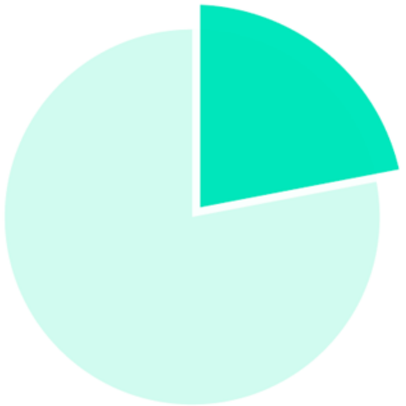


6%
without concrete plans



51%

Industry 4.0 Is An Important Focus But **Not Yet A Major Investment**



22%

It's A **Top Strategic Priority** & Active Area Of Investment

Base: All respondents n=100

Thank you

To speak with a manufacturing expert about your backup and recovery strategy, contact **sales@macrium.com**

Macrium Marketing Team
marketing@macrium.com

Macrium Software | NewtonX®