BE: READY RESILIENT

Global cyber resilience report

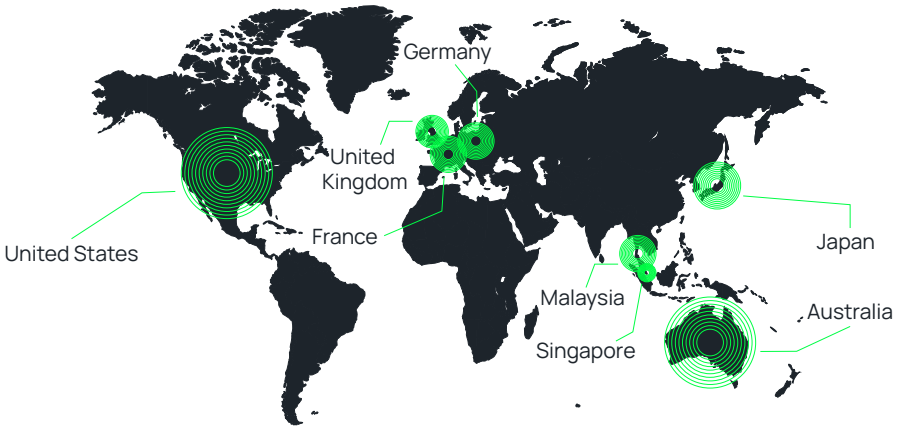
2024

COHESITY

Introduction

This third annual report is based on a 2024 survey of 3,139 IT and Security Operations (SecOps) decision-makers (split 50/50 between the two groups) commissioned by Cohesity and conducted by Censuswide. The survey polled public and private organizations in 8 countries: the United States (~500), the United Kingdom (~500), Australia (~500), France (~400), Germany (~400), Japan (~300), Singapore (~300), and Malaysia (~200) in June 2024.

Countries surveyed



Survey results show that organizations overestimate their cyber resilience capabilities and maturity—often overlooking **deficiencies in data recovery speed or capabilities.** In fact, only 2% of respondents indicated they could recover their data and restore business processes within 24 hours if a cyberattack occurred. The data also show that the majority of organizations are **willing to pay a ransom.** Three in 4 (75%) said their company would pay over $1 million to recover data and restore business processes and 22% of those said their company would pay over $3 million.

Additional survey highlights include these findings:

- **Close to 7 in 10 (69%) respondents said their organization had paid a ransom in the last year.** This was reported despite 77% also saying their company has a defined policy or protocol not to pay ransoms.
- **Only slightly more than 2 in 5 (42%) respondents said their organization could identify sensitive data and comply with applicable data privacy laws and regulations.** The rest said they lack the necessary IT and Security capabilities to do both.
- **A lack of data access control measures undermines Zero Trust Security efforts.** Alarmingly, almost half of respondents (48%) have not deployed multifactor authentication to strengthen their data access controls and align with Zero Trust Security principles. This leaves their mission critical data incredibly vulnerable not just to attacks from external threats but internal threats too.

The 2024 threat landscape

The 2024 threat landscape

Nearly all see rising cyber threats.

When we released our inaugural survey report in 2022, ransomware threats were already top of mind, with 74% of respondents saying they felt the threat of ransomware attacks in their industry had increased over the year. Just one year later, in 2023, that number jumped to 93%. Our 2024 respondents sounded the alarm even louder, with 96% of this year's respondents saying the threat of cyberattacks to their industry had or would increase this year.

And it's not just the threats causing concern. It's actual attacks. In 2022 and 2023, close to half of respondents said their organization had been the victim of a ransomware attack in the past six months. That figure is now far higher, at 2 in 3 (67%)[1].

Ransomware and other cyberattacks pose a real threat to businesses worldwide. And the threat landscape is worsening.

In 2024,

67%

said their organization had been the victim of a ransomware attack in 2024[1].

1: Respondent numbers and geography have slightly changed in 2024 compared to 2023. See methodology on **page 17** for more details.

7 industries hardest hit

We already know cyberattacks are a global menace, crossing borders to wreak havoc worldwide. But they also inflict damage across an array of industries. Survey respondents indicated these 7 sectors were the most impacted[2]:

- IT & Technology (40%)
- Banking & Wealth Management (27%)
- Financial Services (27%)
  (including insurance companies)
- Telecommunications & Media (24%)
  (including streaming services)
- Government & Public Services (23%)
- Utilities (21%)
  (including water, electricity, gas, and other energy services companies)
- Manufacturing (21%)

2: Respondents were asked to select their Top 7, so percentage figures total over 100% for this dataset.

3 areas of critical concern

1: A confidence-capability paradox

Data show a disconnect between strategic intent and actual capabilities.

Claims of confidence are generally a good sign, so long as this confidence is backed by concrete capabilities. But we're seeing a real disconnect between perception and reality when it comes to cyber resilience.

Respondents were asked if they feel their company has a cyber resilience strategy in place designed to address today's escalating cyber challenges and threats, based on a provided definition *[see right]*.

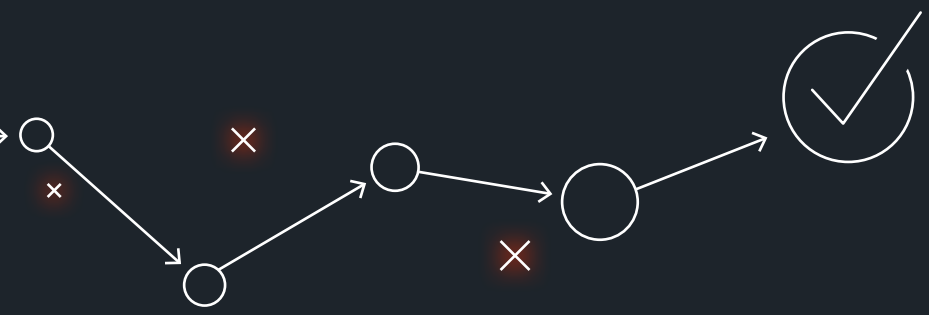
Even given our worsening cyber threat landscape, their responses skewed largely positive.

Respondents were provided with the NIST definition of cyber resiliency at the start of the survey:

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.

78%

said they have confidence in their company's cyber resilience strategy.



But feeling good about plans on paper is one thing. Building out and refining your capabilities to make sure you can execute your planned strategy is another.

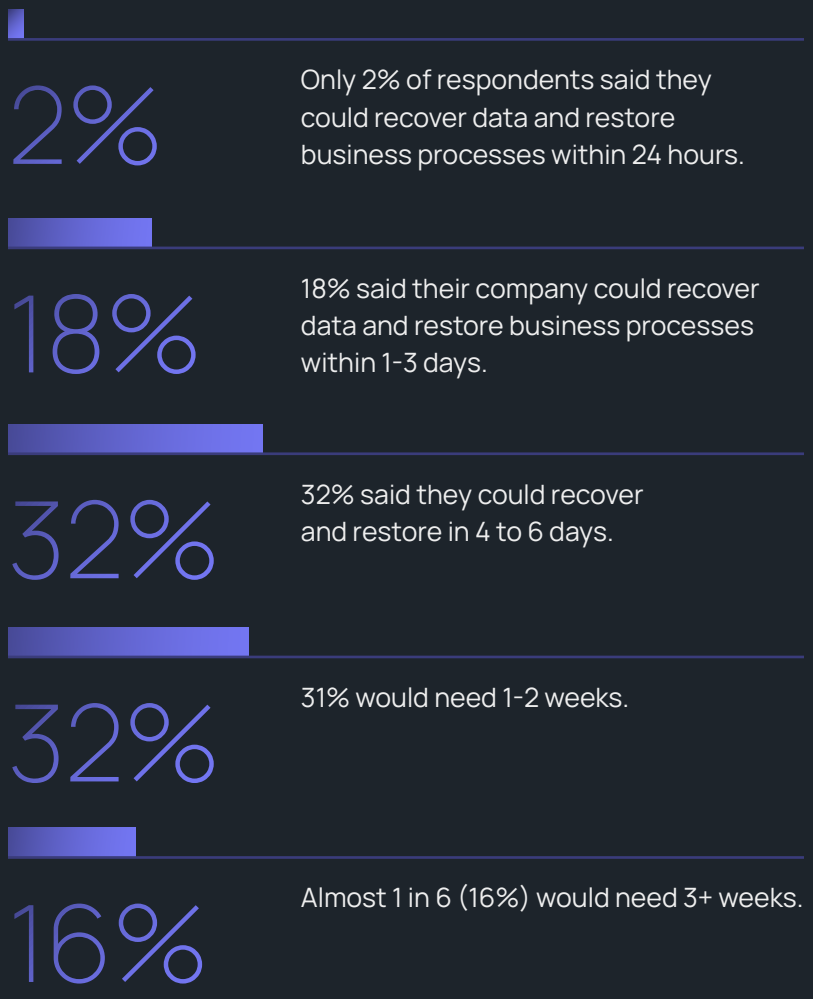
With over 2 in 3 (67%) revealing they had been the victim of a ransomware attack in 2024, and with recovery speeds quite slow, the gap between strategic intent and execution is notable.

If cyber resilience is measured by how quickly a company could recover data and restore business processes after an attack—without threatening business continuity—how fast is fast enough? That may be up to each individual company, but of greatest concern is that they're not meeting their own recovery targets.

When asked for their organization's "targeted optimum recovery time objectives (RTO) to minimize business impact in the event of a cyberattack or incident of compromise," 98% said their target was within one day. Almost half (45%) said their targeted optimum RTO was within two hours. Contrast this with the statistics above that only 2% could recover and restore within 24 hours.

This disconnect between RTO and reality is concerning and wide, and companies need to find a way to bridge this gap. Fortunately, a proven playbook with processes and tools can help improve real-world outcomes. **(See p. 17.)**

According to our survey data:

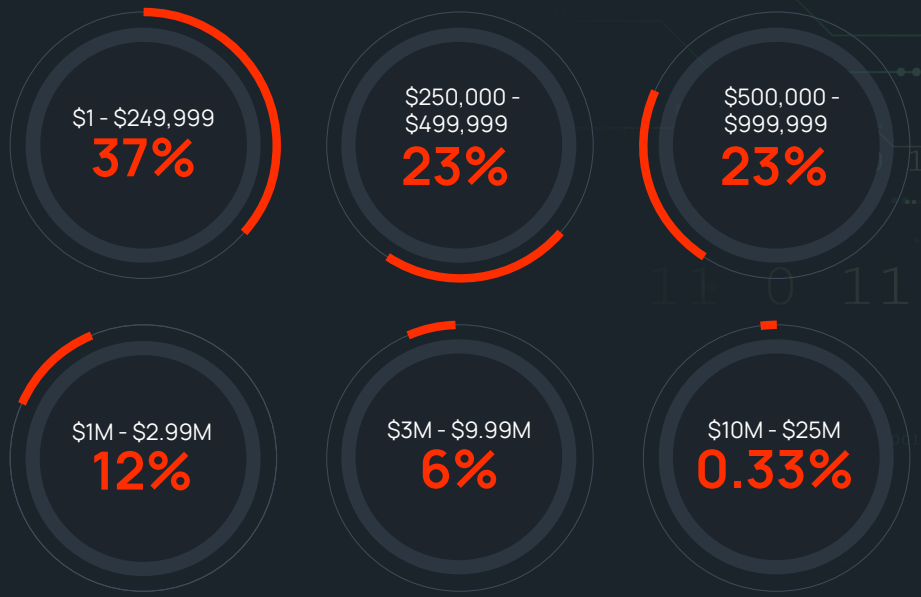


2: Rampant ransom payments

These payments often defy explicit 'do not pay' policies.

A further indicator that companies are less cyber resilient than they believe is the widespread (and growing) practice of paying ransoms.

In 2023, 90% of global survey respondents said their organization would—some unequivocally, some depending on the cost—consider paying a ransom if it meant they could recover data and business processes, or recover them faster. In 2024, close to 7 in 10 respondents (69%, or 2,100 total) reported actually paying ransoms. And the amounts were substantial[3]:



3: Respondents were given corresponding amounts in local currency values.

Paying ransoms has not only become routine, but it's often in direct opposition to those same organizations' 'do not pay' policies. Of those who paid the above amounts, 77% said their company had a 'do not pay' policy.

And don't forget: Ransom payments represent just a fraction of the total financial impact to an organization of suboptimal cyber resilience. The downtime, disruption, lost business opportunities, brand and reputational damage, increased cyber insurance and legal costs, and other fallout from successful cyberattacks exert a financial toll well beyond the dollar value of the ransom paid. And this financial toll doesn't vanish once ransom is paid.

Destructive cyberattacks, such as ransomware or wiper attacks, are not a matter of 'if' but 'when,' and they threaten business continuity. Organizations can tackle the impacts head-on by strengthening their cyber resilience—the ability to rapidly respond to and recover from cyberattacks or unplanned business disruption—by adopting modern data security, response, and recovery capabilities.

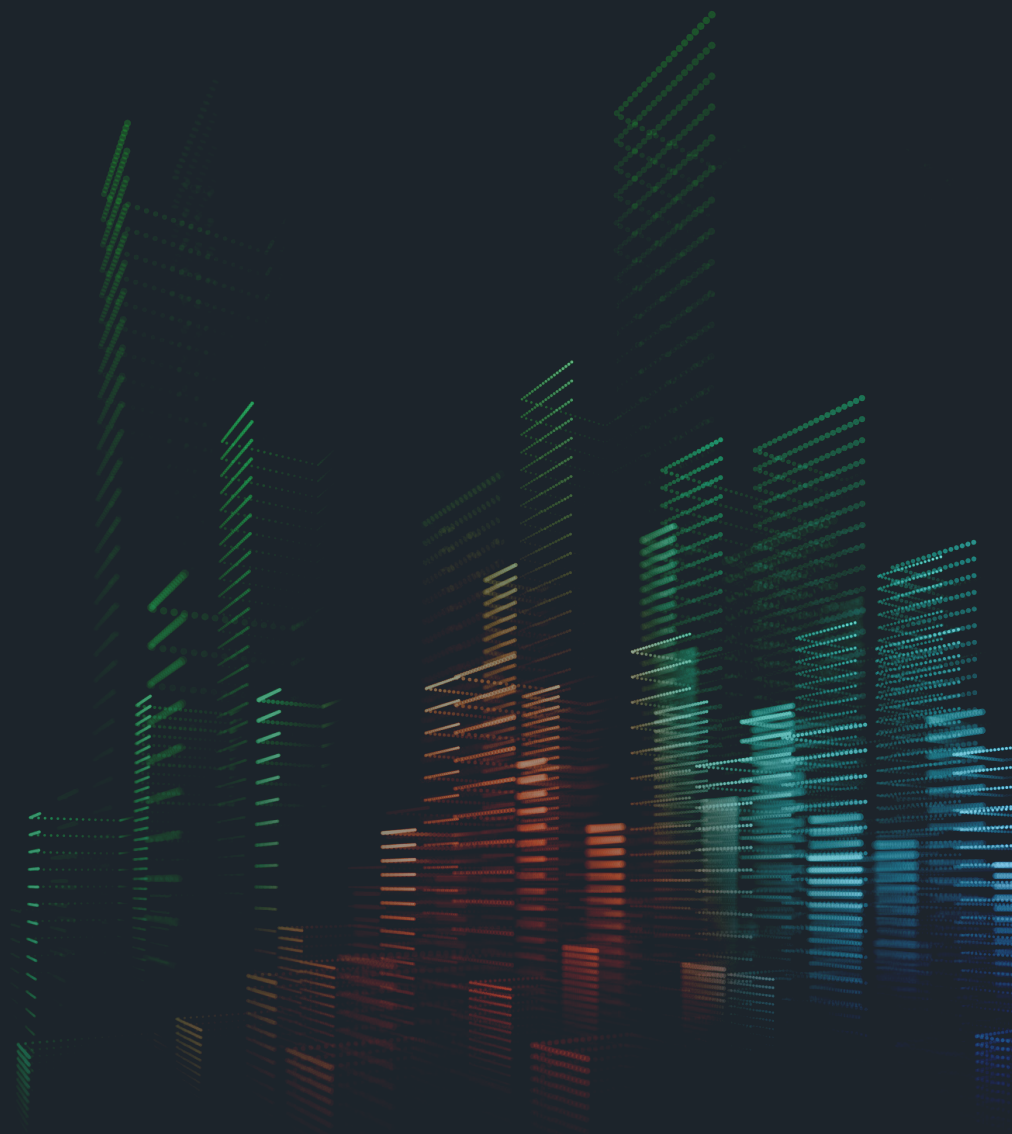
While organizations may have the greatest cyber resilience strategy, there's a gap when it comes to execution, as the majority are paying ransoms or would pay a ransom.

James Blake
Global Cyber Resilience Strategist, Cohesity

3: Alarming Zero Trust Security deficiencies

Gaps abound, though effective security capabilities are widely available.

When asked whether their data access control measures align with Zero Trust Security principles, just over half of companies had deployed multifactor authentication (MFA), and less than half had deployed features requiring multiple approvals before changes to data or role-based access controls (RBAC):



The most vital element of cyber resilience is the ability to recover business-critical data that restores key business processes. But you can't restore critical data, if you don't secure it from external or internal threats first. This starts with deploying effective data access controls like multifactor authentication (MFA) and role-based access controls (RBAC).

The fact that almost 1 in 2 organizations are not implementing these controls to protect sensitive data is alarming and demonstrates a significant risk to an organization's cyber resilience.

Especially given everyday consumers and end-users are often—and rightly—required to have MFA enabled to secure their account credentials, with MFA also an important defense measure against AI-based attack techniques.

Brian Spanswick
CISO and CIO, Cohesity

Cyber resilience requires constant vigilance

Cyber resilience requires constant vigilance

As the threat landscape continues to evolve, even governments and public institutions are going to great lengths to encourage more robust cybersecurity, data protection, and data privacy measures.

- **Only 42% of respondents** said they had all the IT and Security technology capabilities to identify sensitive data and comply with applicable data privacy laws and regulations.
- **79% of respondents** also said that advanced threat detection, data isolation, and data classification were vital to their organization's qualification for cyber insurance or to secure discounts on their cyber insurance policies.

But qualifying for cyber insurance, reducing premiums, or getting discounts should never be the end goal. These should be a benefit of having the necessary data protection and advanced data security capabilities in place to secure your organization's data and strengthen your cyber resilience.

A word on AI-based cyberattacks

According to respondents, organizations must now contend with AI-based cyberattacks or cyber threats. Four in five (80%) of those surveyed said they'd responded to what they believe to be AI-based attacks or threats within the last 12 months.

While it's difficult to determine with certainty if attacks are indeed AI-based, there's no question that the continuing and rapid evolution of the threat landscape will pose new threats. Having a modern, AI-powered data security platform in place, and working with a leader (or with an alliance of leading vendors), will help ensure your organization is best positioned for a cyber resilient future.

Conclusion and next steps

To recap, this 2024 global survey revealed three primary areas of concern

1 A confidence-capability paradox.

Execution of strategies designed to strengthen cyber resilience falls short, leading to successful attacks and slow recovery times.

2 Rampant ransom payments.

Payments surged, despite the existence of, and in direct contradiction to, widespread do not pay policies.

3 Alarming Zero Trust Security deficiencies.

Failure to implement effective data access controls like MFA and RBAC puts organizations and their data at unnecessary risk.

The good news? Identifying a problem is the first step towards fixing it.

These data points reveal areas of opportunity for improvement. And people, processes, and tools do exist to reverse these trends and close gaps to shore up cyber resilience.

Engage in more rigorous testing, drills, and simulations.

Regular testing and drills are essential to ensure that the backup and recovery process is effective and that all stakeholders are familiar with their roles during an incident. In addition to conducting regular disaster recovery drills to simulate real-world scenarios—helping the team practice and refine their response procedures—these drills help identify potential weaknesses and areas for improvement.

In addition, automated testing of backup data can verify the integrity and recoverability of backups without manual intervention. This automation helps ensure that backups are reliable and can be restored quickly when needed.

Finally, maintaining detailed documentation and recovery playbooks helps ensure that everyone knows their responsibilities and what steps to take during an incident. These playbooks should be regularly updated based on the results of testing and drills.

And this is just a start. To fully reduce operational risk, a transition to modern data security and management processes, tools, and practices is required. We've compiled our recommendations in **"An executive's guide to modern data security and management,"** a comprehensive white paper that describes how to make this modern model a reality.

Sign up for a Ransomware Resilience Workshop.

A cyber resilient posture requires organizations to focus on all elements of cyber incident response equally, being able to mitigate not just the likelihood of the attack but also the impact.

Sign up

The findings are based on a survey of 3,139 IT and Security decision-makers (split as close to 50:50 as possible) commissioned by Cohesity and conducted by Censuswide between 6/27/24 - 7/18/24. The top five industries that respondents selected as best representing their company's operations were IT & Telecommunications, Manufacturing, Financial Services (incl. Insurance), Banking & Wealth Management, and Hospitals & Healthcare. This year's survey polled 8 countries, with the addition of Singapore and Malaysia, as opposed to 6 countries in 2023, with a small reduction in overall respondents. This reduction is reflected in only 400 respondents being polled in Germany and France respectively, and 300 in Japan, compared to 500 respondents in each market in 2023. Censuswide abides by and employs the Market Research Society members, follows the MRS code of conduct and ESOMAR principles, and is a member of the British Polling Council.

COHESITY

Ready to strengthen your cyber resilience?

Get to know our AI-powered
data security at cohesity.com

9100082-001 EN 8-2024