COHESITY

The State of Data Security and Management Report 2023

July 2023

At a glance

The second annual State of Data Security and Management Report is based on a 2023 survey of over 3,400 IT and Security Operations (SecOps) decision-makers (split nearly 50/50 between the two groups) commissioned by Cohesity, Tenable, and BigID and conducted by Censuswide. The survey polled businesses and organizations in Australia, France, Germany, Japan, New Zealand, the United Kingdom, and the United States in April 2023.[1]

At a time when cyberattacks are getting worse and becoming more frequent, three notable findings stood out:

- **Most organizations don't have the necessary cyber resilience strategies or data security capabilities to address threats and maintain business continuity.**
- **Compared to 2022, fewer respondents are confident their organization can rapidly recover their data after an attack.**
- **Cyber insurance is getting harder to obtain.**

Increasing cyberattacks fuel continued ransomware concerns

When we released the inaugural State of Data Security and Management Report in 2022, ransomware threats were top of mind. In fact, 74% of last year's survey respondents said they felt the threat of ransomware attacks in their industry had increased that year.

We asked the same question for this year's survey, and the percentage rose significantly. A whopping 93% of respondents said the threat of ransomware attacks increased this year when compared with the same period last year.

And it's not just threats causing concern. It's actual attacks. For two years running, close to half of respondents said their organization had been the victim of a ransomware attack in the past six months.

1. Censuswide abides by and employs members of the Market Research Society, which is based on the ESOMAR principles.

If you're wondering whether ransomware and other cyberattacks still pose a real threat to your business, and to businesses worldwide, this global survey indicates the answer is yes.

93%

Said they felt the threat of ransomware attacks to their industry had increased in 2023.

Said their organization had been the victim of a ransomware attack in the prior six months.

45%

Problem 1

Most organizations lack strong cyber resilience strategies or data security capabilities to address threats and maintain business continuity.

Despite both the rise in threats and the high percentage of respondents whose organizations suffered recent attacks, there hasn't been a corresponding uptick in strategic measures to shore up cyber resilience. In fact, close to four in five survey respondents don't have complete confidence that their company has a cyber resilience strategy designed to address today's escalating cyber challenges and threats.

And it's not just about confidence. Organizations need cyber resilience and data security capabilities in place, too—to recover data and restore business operations, and to do so fast.

The NIST Cyber Security Framework is frequently cited by organizations as their reference framework for cybersecurity and cyber recovery. Through its identify, protect, detect, respond, and recover functions, the framework simplifies how to prioritize investments based on risks and operating priorities. And alignment to standards provides several benefits, as these frameworks guide the deployment of proper controls and processes, and create a common reference point for organizations to align security, IT, and business.

80% expressed concerns about their organization's cyber resilience strategy and whether it can address today's cyber challenges and threats.

(Respondents were provided with this NIST definition of cyber resilience at the start of the survey.)

“Cyber resiliency starts with getting the basics right, especially around your data. It’s essential to understand where your sensitive data lives, what it is, who has access to it, and the risks associated. As a Security community, we need to place data at the center of our security strategy.”

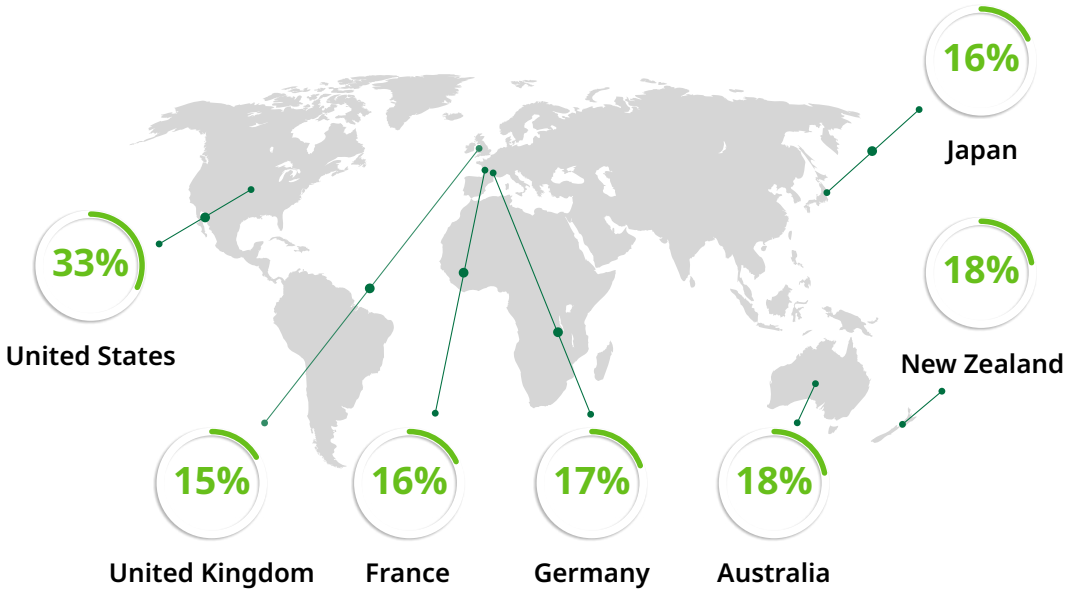
TYLER YOUNG, CHIEF INFORMATION SECURITY OFFICE, BIGID

Problem 2

Respondents worry that their organization could not recover after an attack.

When asked about the threat of ransomware, 40% of last year's respondents said "failure to recover data" worried them—even if their data was backed up. This year, 67% lack full confidence their company could recover data and critical business processes in the event of a system-wide cyberattack.

Of the small percentage globally (21%) who answered they were "absolutely confident" they could restore after a cyberattack without the risk of reinfection with malware, the United States was far more confident than its counterparts in other parts of the world:



What are the barriers that make getting back up and running so difficult? According to the survey, the top three challenges include:

34% Lack of integration between IT and security systems

Lack of coordination between IT and security professionals **33%**

32% Antiquated backup and recovery systems

...and when recovery is possible, it's not necessarily fast.

Slow recovery introduces unpredictability and harms the business. It also raises numerous questions.

When will your virtual machines, databases, and NAS data be back online and accessible? Will they be clean, or will recovering them reintroduce malware and reinfect your systems? Can you recover mission-critical data at scale to any point in time and location? If so, when? If not, what happens then?

When asked how long, on average, it would take their company to restore data and business processes if a cyberattack occurred:

Said it would take over 24 hours

Said it would take over 4 days

Said it would take over a week

And in a ransomware attack, every minute matters. The longer a business is down and its data is inaccessible, the greater the risk for serious, and often immediate, downstream impacts.

"Organizations cannot afford to be offline and unable to maintain operations, especially for more than a day. However, the stark reality is that many organizations are vulnerable to cybercriminals because they are incapable of rapidly recovering their data and business processes when necessary."

BRIAN SPANSWICK, CHIEF INFORMATION SECURITY OFFICER AND HEAD OF IT, COHESITY

When 95% can't recover data and business processes within 24 hours, not only are organizations vulnerable, but they're more willing to make choices that may incentivize future industry attacks. Choices that include paying a ransom.

Most would consider paying a ransom

Although paying a ransom is generally considered an action of last resort, 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. The countries most likely to go this route include:

- **Australia and New Zealand (95%)**
- **United States (94%)**
- **France (93%)**
- **United Kingdom (91%)**

Germany **(87%)** and Japan **(78%)** are still likely to consider paying, but less so overall.

Of course, when dealing with cybercriminals, you're not dealing with good faith actors. Always keep in mind there's no guarantee paying a ransom means your data will be recovered—or that if it is recovered, it'll be clean and free of malware.

Problem 3

Cyber insurance is getting harder to obtain.

With cybercrime predicted to cost the world $8 trillion annually ($10.5 trillion by 2025), more companies are trying to secure financial protection against losses from cyberattacks, data breaches, and other cyber-related incidents. They're turning to cyber insurance as one of their protection strategies.

This year, 74% of survey respondents said their company currently has cyber insurance. (In Japan, this number is only 61%.) But securing a policy isn't easy—and it's getting harder, according to almost half (46%) of survey respondents, who said it's more difficult to obtain cyber insurance today than it was three years ago.

The list of technologies and capabilities respondents deemed critical as companies try to secure cyber insurance is long. It includes:

- 40% Strong encryption
- 38% Ability to verify integrity of backup
- 37% Multifactor authentication (MFA)
- 34% Anomaly detection
- 33% Data isolation / air gapping
- 29% Immutability

Meeting critical capabilities may not only help secure hard to obtain cyber insurance policies, it may also help drive premiums down.

Cyber insurance is one more layer in a multilayered security approach to combating ransomware, and cyberattacks more broadly.

Problems abound. But so do solutions.

It *is* possible to strengthen cyber resilience.

Despite the severity of the problems covered in this report, there are ways organizations can strengthen cyber resilience in the face of escalating threats—whether from ransomware and other cyber incidents (as covered here), or from disasters like earthquakes, floods, system failures, or human errors.

Two concrete ways to drive cyber resilience include greater collaboration and deeper insights.

Greater collaboration

According to 87% of respondents, data and cybersecurity vendors must collaborate to provide complete and integrated anti-ransomware solutions.[2] When vendors work towards a common goal of defeating ransomware and creating integrated solutions that support clean recovery efforts, organizations reap the benefits. Greater cyber resilience is better for them, better for the customers they serve, and better for their industries. With nation-state actors committing more and more cybercrimes, thwarting these attacks and building resiliency against them is also better for the world.

Deeper insights

In addition to the benefits of collaboration among vendors, 90% of respondents feel their organization would benefit from a data security and management platform that provides insights on their overall security posture and cyber resilience. With these insights, organizations can lower the risk of operational disruptions and improve their ability to withstand cyberattacks. Plus, these insights can help speed and ease audits for compliance with industry and privacy regulations.

"Relying on traditional backup and recovery systems, which lack modern data security capabilities, in today's sophisticated cyber threat landscape, is a recipe for disaster. Instead, organizations should seek out data security and management platforms that integrate with their existing cybersecurity solutions and provide visibility into their security posture and improve cyber resilience."

BRIAN SPANSWICK, CHIEF INFORMATION SECURITY OFFICER AND HEAD OF IT, COHESITY

2. This statistic combines the results of respondents who selected either "Extremely Important" or "Somewhat Important."

“The only way to achieve cyber resilience is by prioritizing proactive security measures that will prevent cyberattacks in the first place. This approach should also extend to backup and recovery measures to ensure business continuity in the event of a cybersecurity incident. This requires organizations to not only manage their cyber risk, but better understand their exposure to risk by leveraging vulnerability and exposure data to make informed decisions on remediation efforts.”

RAY KOMAR, VICE PRESIDENT OF TECHNOLOGY AND CLOUD ALLIANCES, TENABLE

Conclusion

When an organization gets hit by ransomware, and data is stolen, wiped, infected, or otherwise compromised, that organization can't properly function until its data, processes, operations, and applications are restored. Making sure this recovery is clean, and happens fast, is critical to business resilience.

Given this reality, a comprehensive approach to data security and management is the best offense against continuing worldwide threats.

This year's global survey shows that:

1. **Most organizations still don't have the necessary cyber resilience strategies or data security capabilities in place to address these threats and maintain business continuity.**
2. **Fewer IT and SecOps professionals are confident their own organization can recover effectively—and rapidly—after a cyberattack.**
3. **Despite its proliferation, cyber insurance is harder to obtain and the list of technologies and critical capabilities needed to qualify is long.**

Ultimately, organizations that work with vendors who collaborate, partner, and integrate their solutions for cybersecurity and data security and management will be better positioned to withstand and recover from cyber incidents and lower their overall operating risks. Further, organizations with data security and management platforms that offer insights on their overall security posture will be better able to withstand threats and recover confidently.

Today's organizations can't afford to be unprepared.

6100022-001 EN 7-2023

COHESITY

COHESITY