Gartner
Peer Community™

Cyber Resilience: Evolving Backups and Incident Response

Effective backup and incident response capabilities are critical components of a cyber resilient enterprise. How are organizations currently upgrading their strategy?

- Almost all are working to improve processes or capabilities for backups
- Over one-third plan to improve backups using a cloud-based solution such as a backup-as-a-service provider
- Leaders plan to evolve incident response processes or capabilities, with many focused on improving post-incident reviews

Data collection: Feb 19 - May 31, 2024

Respondents: 129 information security and IT leaders with visibility into their organization's processes for data backups and incident response

About Gartner Peer Community One-Minute Insights:

Gartner Peer Community is for technology and business leaders to engage in discussions with peers and share knowledge in real time.

Surveys are designed by Gartner Peer Community editors and appear on the Gartner Peer Community platform. Once the respondent threshold is met, survey results are summarized in a One-Minute Insight.

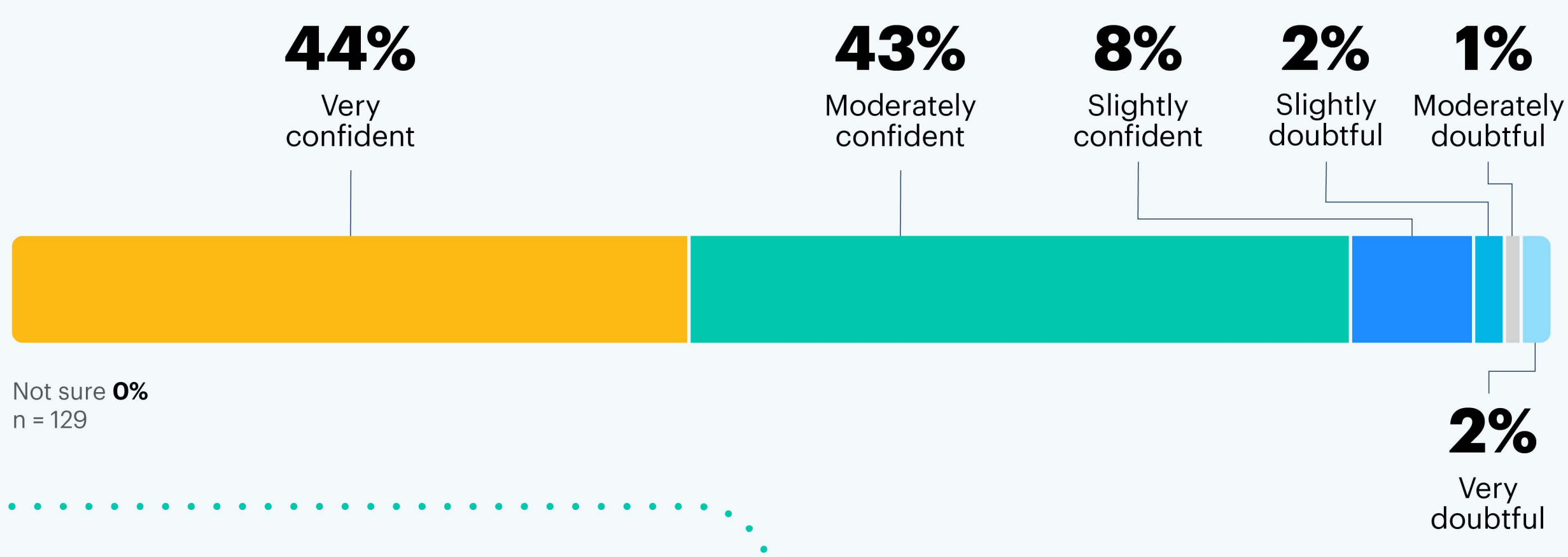
The results of this summary are representative of the respondents that participated in the survey. It is not market representative.

1 Minute Insights

Leaders are confident in current backups but intend to make improvements

95% of surveyed leaders are confident that their organization's **backups would adequately enable recovery of critical data** in the event of a cyber incident.

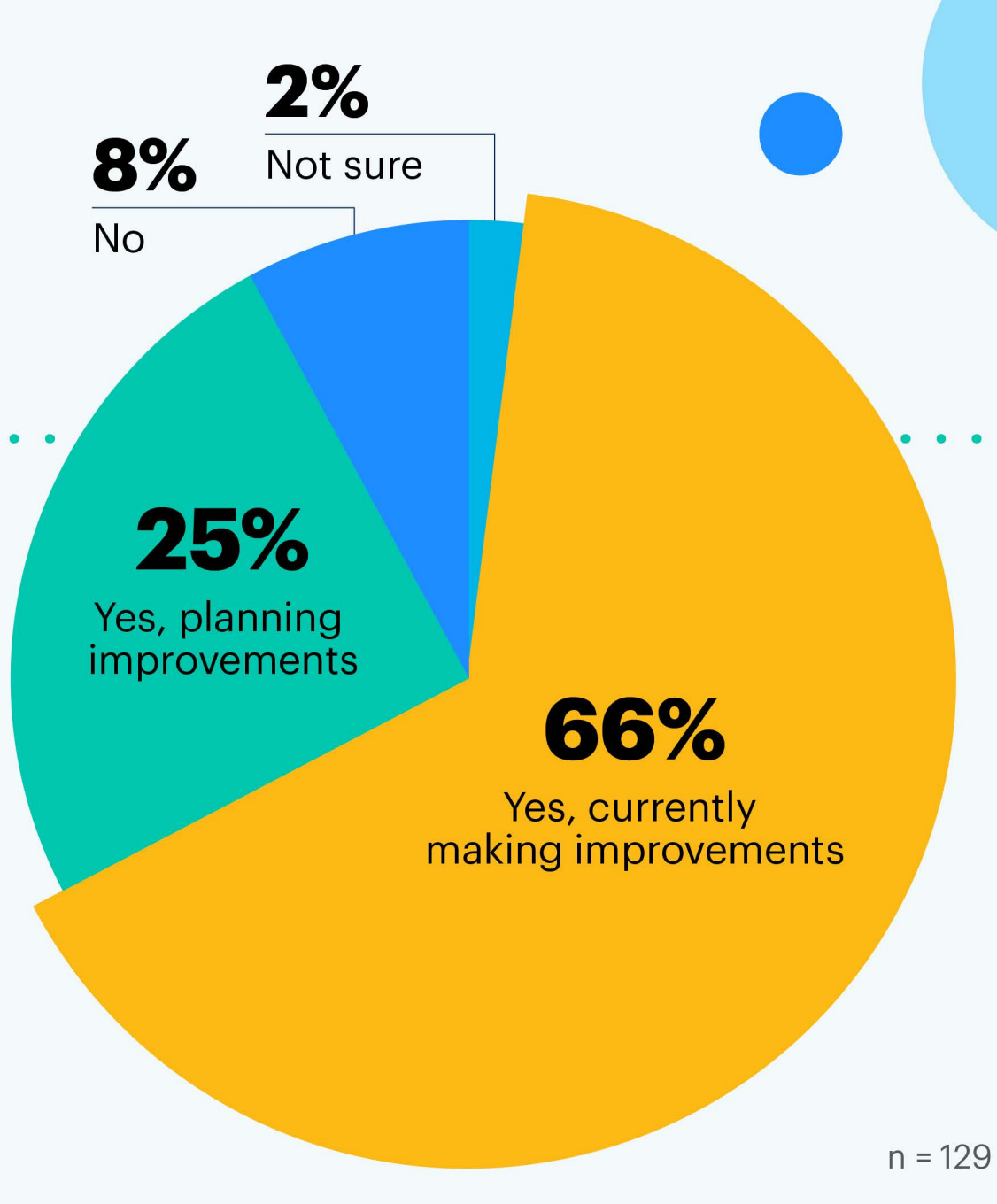
In the event of a cyber incident, how confident or doubtful are you that your organization's current backups are adequately maintained and protected (i.e., that they would enable recovery of critical data)?



Not sure **0%**
n = 129

Nevertheless, nearly all (**91%**) respondent organizations are working to **improve their backup processes or capabilities;** two-thirds (66%) have begun making improvements and 25% plan to.

Is your organization working to improve any backup processes or capabilities?



n = 129

Note: May not add up to 100% due to rounding

> "Cyber resilience is constant. You never stop reinventing and improving."
>
> Director, hospitality industry, 1,000 - 5,000 employees

Question: Please share any final thoughts on your organization's cyber resilience goals, strategies or challenges.

Organizations look to implement cloud-based solutions to improve backups

38% — **Implement cloud-based backup solution** (i.e., backup-as-a-service provider)

32% — **Improve data restoration testing**

30% — **Improve documentation**

Among those making or planning changes (n = 117), **38%** are improving backups by **implementing a cloud-based backup solution.** Nearly one-third are improving data restoration testing (32%) or documentation (30%).

How is your organization planning to improve backup processes or capabilities? Select all that apply.[1]

Modify recovery point objective (RPO) **28%** | Improve backup lifecycle management (e.g., retention policies) **28%** | Maintain offline backups **27%** | Implement backup versioning **26%** | Improve backup encryption **26%** | Implement or increase automation capabilities **24%** | Use storage snapshots **22%** | Use incremental or differential backups **22%** | Not permitted to disclose **22%** | Implement backup monitoring system(s) **21%** | Modify backup schedule **18%** | Not sure **1%** | Other* **1%**

n = 117
*Other includes: Network segmentation

> "Testing is so important. I wish testing tools/exercises were not so expensive."
>
> C-suite, healthcare industry, 1,000 - 5,000 employees

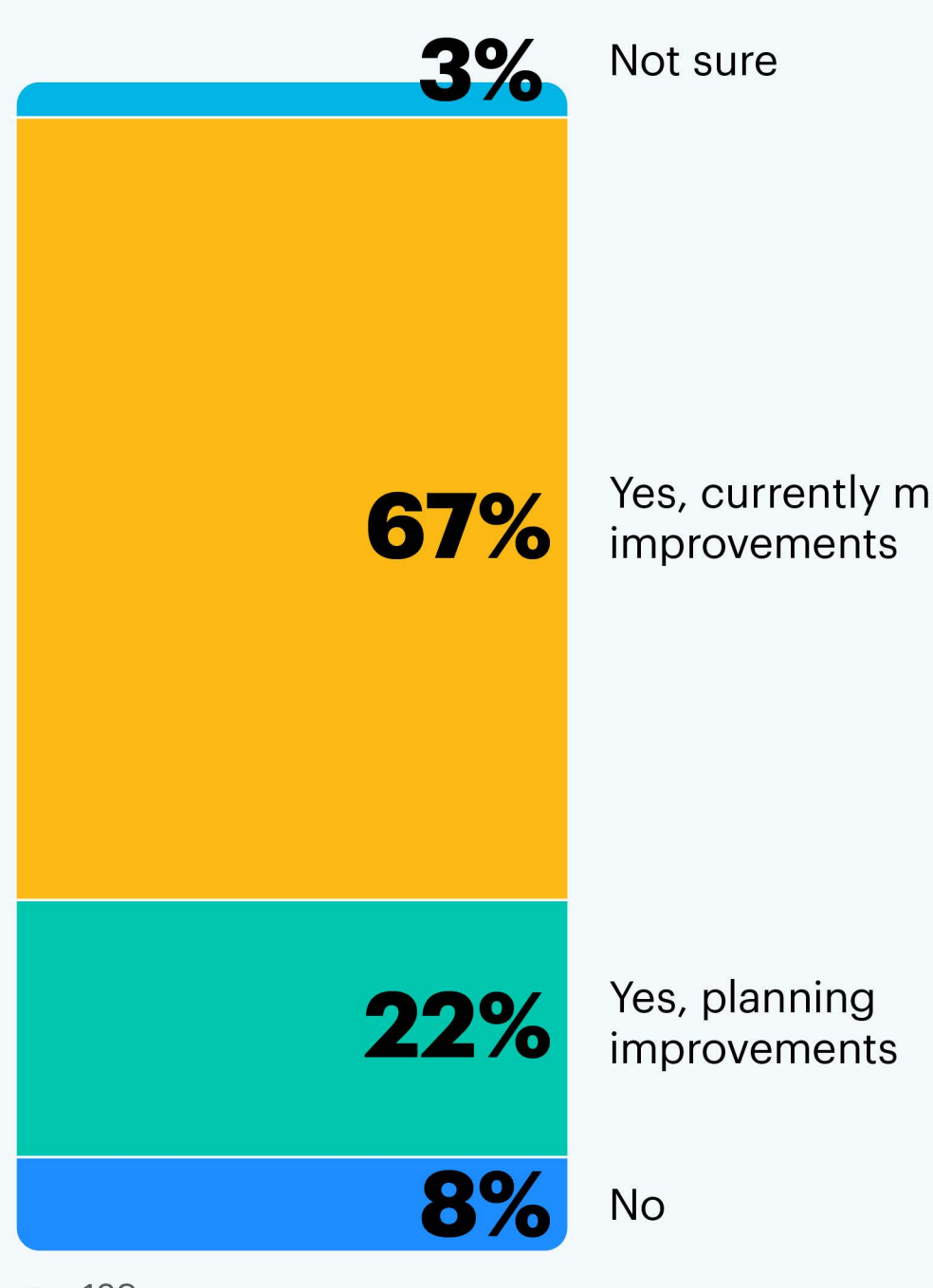
> "Air-gapping the data [and] ensuring anomaly detection is in place is the need of the hour. Encryption is another must and no longer optional."
>
> Director, software industry, 10,000+ employees

Question: Please share any final thoughts on your organization's cyber resilience goals, strategies or challenges.

Many are working to improve post-incident reviews, vulnerability assessments

89% of all respondent organizations (n = 129) are looking to **evolve incident response** (IR), with 67% currently making improvements to IR processes or capabilities.

Is your organization working to improve any incident response processes or capabilities?



n = 129

Many respondent organizations working on IR improvements (n = 115) are targeting **post-incident reviews (46%), vulnerability assessments (42%)** or **communication protocols (39%).**

How is your organization planning to improve incident response (IR) processes or capabilities? Select all that apply.[2]

Implement advanced threat detection tool(s) **27%** | Adding employees from non-IT/security functions to IR team **26%** | Establish continuous monitoring capabilities **25%** | Add threat intelligence sources or services **25%** | Implement security orchestration, automation and response (SOAR) tool **17%** | Hiring new IR team members **15%** | Not permitted to disclose **13%** | Implement digital forensics and incident response (DFIR) services **12%** | Not sure **1%** | Other **0%**

n = 115

> "The drills and simulation[s] are crucial to create awareness and muscle memory."
>
> VP, professional services industry, 10,000+ employees

> "Always improving in a manner that respects business velocity."
>
> Director, healthcare industry, 5,000 - 10,000 employees

Question: Please share any final thoughts on your organization's cyber resilience goals, strategies or challenges.

In their own words...

> "Currently [the] whole IT infra is moving or has moved to [a] connected environment, often resulting in backups or critical apps also dependent on online connectivity. Organizations should have some critical capabilities in offline mode as well. Also, hybrid cloud should be adopted instead of [a] complete public cloud environment."
>
> - C-suite, software industry, <1,000 employees

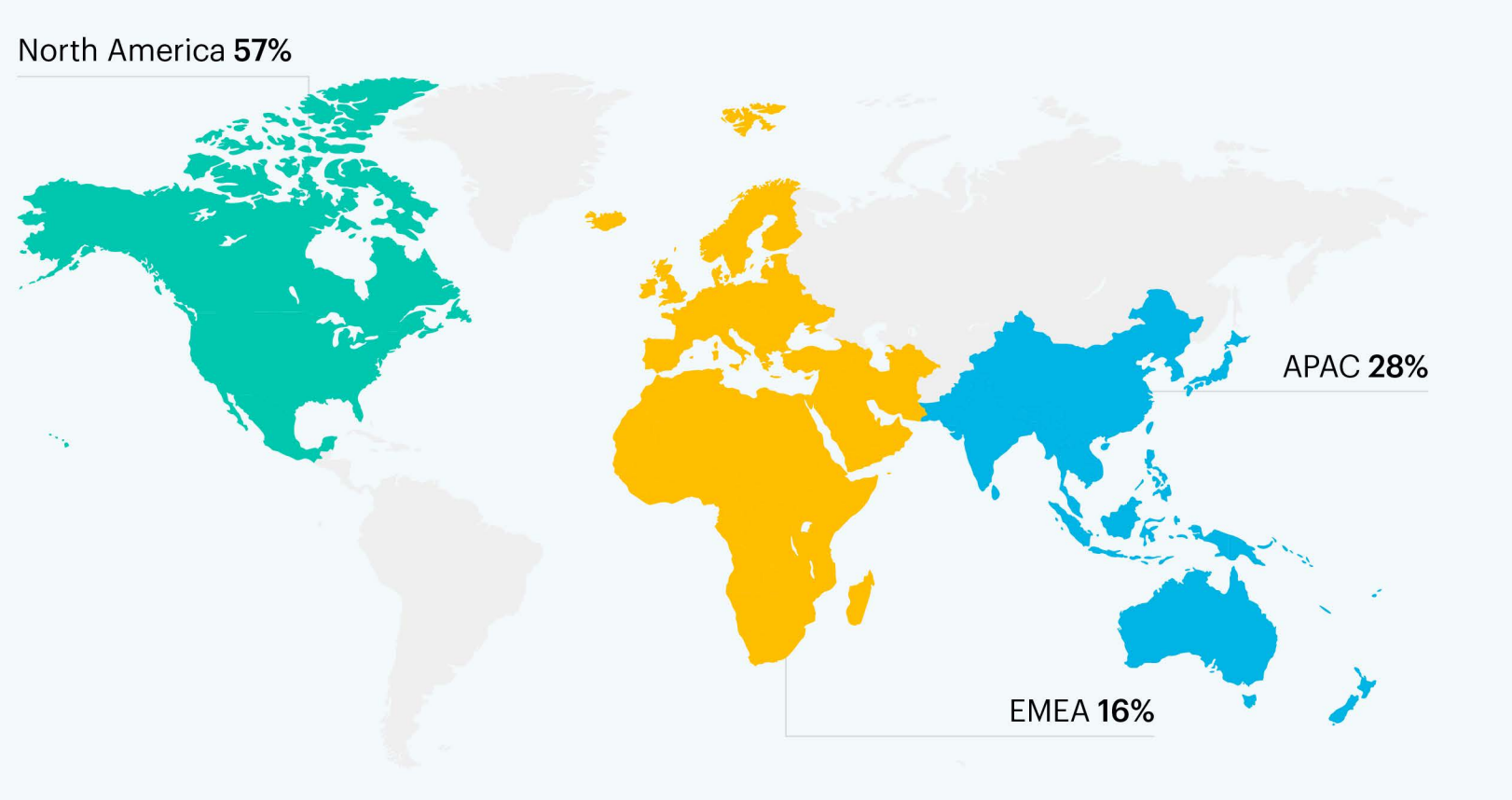
> "There is executive leadership support for purchasing/creating a fund for cryptocurrency in the event of ransomware situations — which is something that I would love to know more about [and] if this is something other experts suggest or not."
>
> - C-suite, professional services industry, 1,000 - 5,000 employees

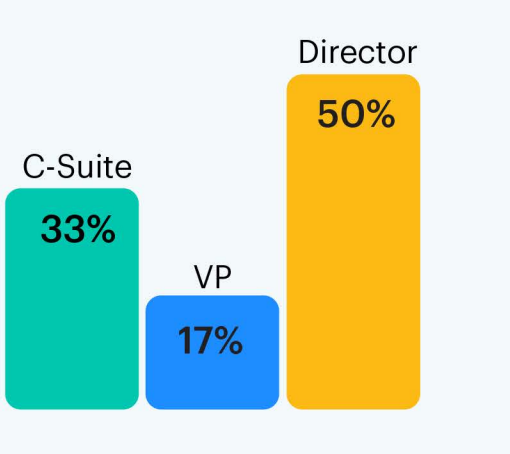
> "[Cyber resilience] is a strategy that must be constantly updated."
>
> - C-suite, software industry, 10,000+ employees

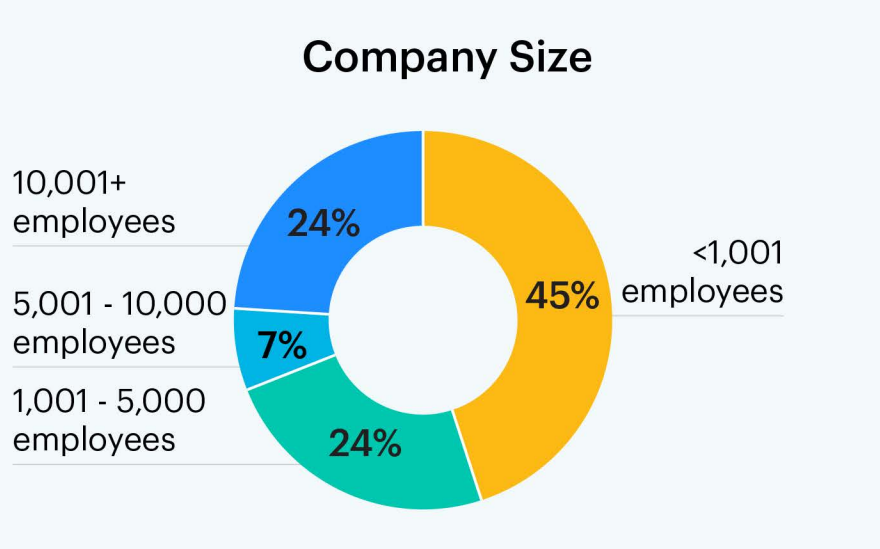
> "Management interest is driven by real life incidents."
>
> - VP, finance industry, <1,000 employees

Question: Please share any final thoughts on your organization's cyber resilience goals, strategies or challenges.

Respondent Breakdown





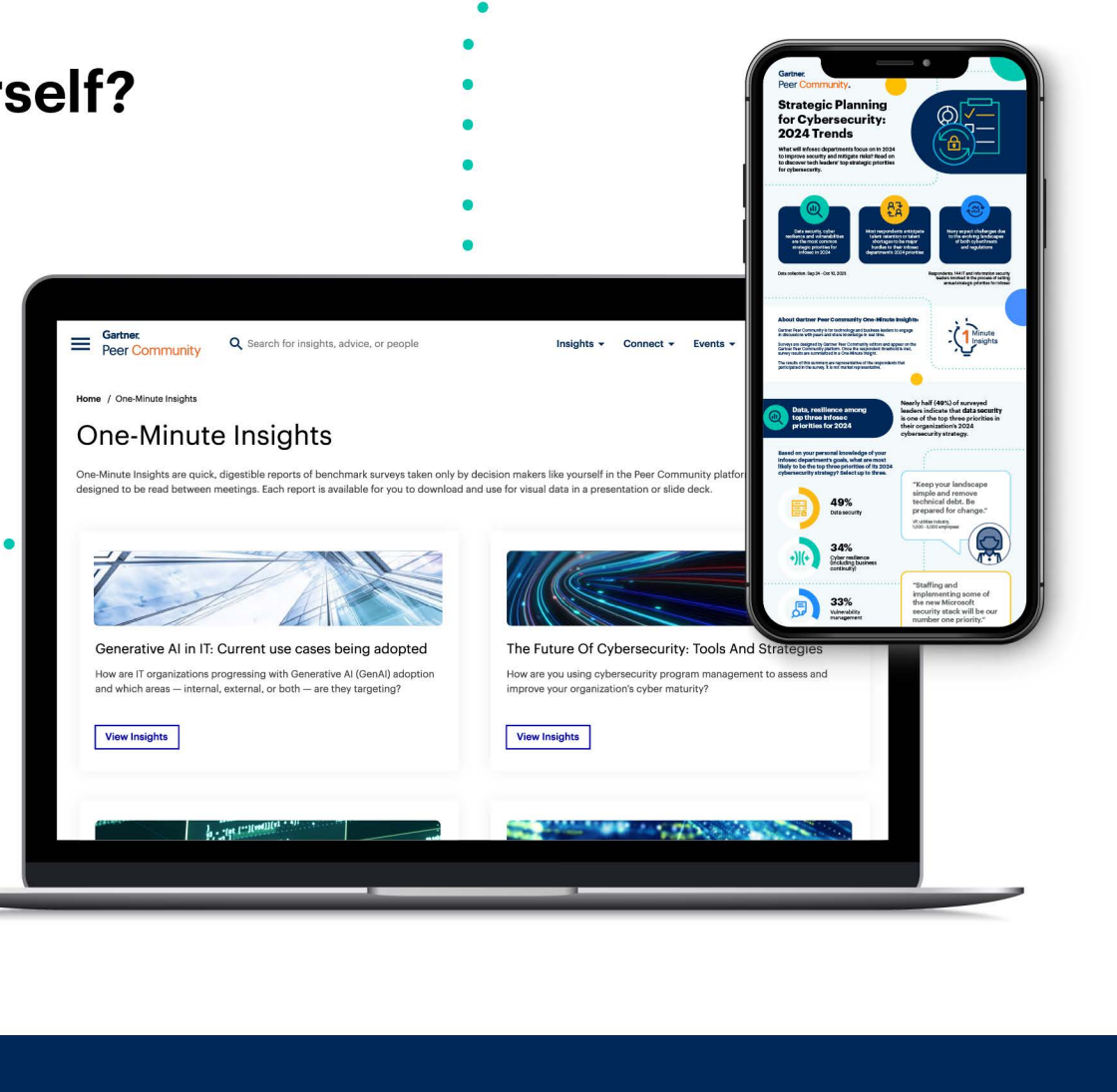


Note: May not add up to 100% due to rounding

Respondents: 129 information security and IT leaders with visibility into their organization's processes for data backups and incident response

Want more insights like this from leaders like yourself?

Click here to explore the revamped, retooled and reimagined Gartner Peer Community. You'll get access to synthesized insights and engaging discussions from a community of your peers.



Gartner

Source: Gartner Peer Community, Building Cyber Resilience: Incident Response and Backup Strategies survey

[1]Question shown only to respondents who answered "Yes, currently making improvements" or "Yes, planning improvements" to "Is your organization working to improve any backup processes or capabilities?"

[2]Question shown only to respondents who answered "Yes, currently making improvements" or "Yes, planning improvements" to "Is your organization working to improve any incident response processes or capabilities?"