Gartner
Peer Insights™

Cybersecurity Quarterly Benchmarks:
Q1, 2022

One-Minute Insights:

- Most are focussing on governance and compliance standards, new tool/initiative implementation, and tool/initiative evaluation this quarter
- While most consider their cybersecurity budget to be adequate, almost a quarter consider their budget to be stretched
- Cybersecurity breaches were common in Q1, with around a third reporting service disruption due to software supply chain attacks
- Over half report an increase in cybersecurity incidents in Q1 compared to the previous quarter
- Endpoint security is the most common focus for implementation/enhancement
- The most common challenge is integrating new tools with legacy technology

Most are satisfied with their current cybersecurity posture and feel confident about achieving their cybersecurity goals in Q1

Cybersecurity is ensuring business continuity by protecting their organization's digital assets, including sensitive data, from attack or employee negligence.

Amid rising global tensions at a time when nations are deploying IT armies and enacting cybersecurity mandates, what is the state of cybersecurity in Q1, 2022?

Use these insights to benchmark against your peers.

One-Minute Insights on timely topics are available to Gartner Peer Insights members. Sign up for access to over 100 more, and new insights each week.

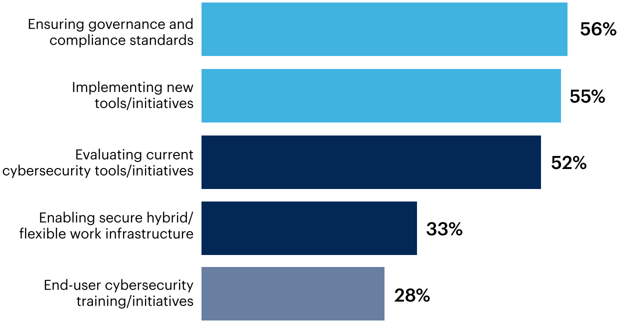
Data collection: Feb 14 - Mar 20, 2022

Respondents: 361 tech decision makers whose role relates to cybersecurity

Most cybersecurity projects are focussed on ensuring governance and compliance standards in Q1

The top cybersecurity projects decision makers are focussing on this quarter are related to **governance and compliance standards (56%), implementing new tools or initiatives (55%),** and **evaluating current cybersecurity tools or initiatives (52%).**

What cybersecurity projects are you focussing on this quarter?



Selling cybersecurity to the business (i.e., convincing business stakeholders and the board that cybersecurity is a business risk) **26%**, Auditing network/assets for known vulnerabilities **25%**, Hiring for cybersecurity roles **24%**, Talent management (e.g., upskilling or retaining current team) **24%**, Cultural overhaul (e.g., moving towards a DevSecOps culture) **22%**, Researching/exploring emerging cybersecurity technologies **16%**, Addressing ongoing disruption caused by a breach **11%**, Migrating cybersecurity to the cloud **10%**, Outsourcing cybersecurity **8%**, Bringing cybersecurity in-house **2%**, None of these **0%**, Other **0%**

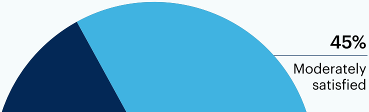
n=361

> **“Progress is made, but cybersecurity remains underprioritized as compared to business initiatives.”**
>
> - Director, finance industry, 10,000+ employees

> **“Everything in cyber security is challenging. So focus on talent instead of tools.”**
>
> - C-suite, finance industry, <1,000 employees

Though most are satisfied with the progress made on their cybersecurity goals in the last quarter, almost a quarter of decision makers consider their cybersecurity budget to be stretched

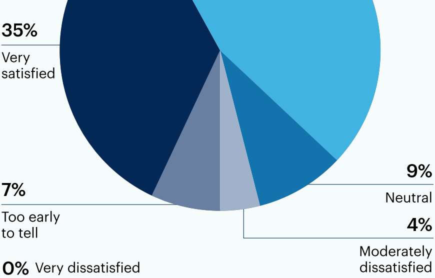
80%



feel **satisfied** with the progress made on their cybersecurity goals in the last quarter.

Were you satisfied with the progress made on your cybersecurity goals in the last quarter?

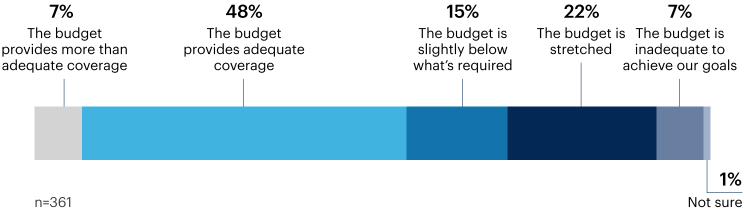
n=361



Regarding their cybersecurity for Q1, **55%** feel that their cybersecurity budget is adequate to achieve those goals.

That leaves **44%** feeling that their cybersecurity budget is not adequate. **22%** feel their cybersecurity budget is stretched in Q1.

Do you feel your cybersecurity budget is adequate to make progress on your cybersecurity projects this quarter?



n=361

"There is an increased impetus and board acceptance for investment and focus in [cybersecurity] and this is helping to drive implementation of advanced tools and processes and improving the overall security posture."

- C-suite, finance industry, 1,000 - 5000 employees

"Budget is a challenge in terms of tools and staff. End-user awareness continues to be a challenge."

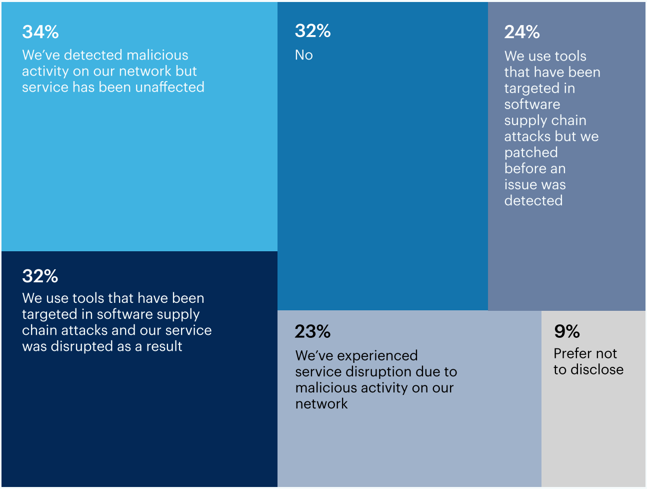
- Director, education sector, 5,000 - 10,000 employees

Only 32% report not experiencing a cybersecurity breach in Q1

The most commonly reported cybersecurity breach in Q1 was **malicious activity on the network that did not affect service (34%)**.

Almost a third (**32%**) report that **tools used by their organization had been victim to a software supply chain attack**, and they experienced service disruption as a result.

Has your organization been affected by a cybersecurity breach in any of the following ways this quarter?



We've experienced a ransomware attack **8%**, Not sure **2%**

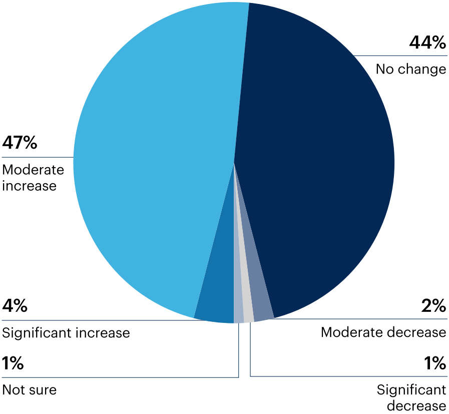
n=361

Over half (51%)

of respondents report that cybersecurity incidents **rose in Q1 compared to the last quarter.**

Has the frequency of cybersecurity incidents at your organization changed compared to the last quarter?

n=361

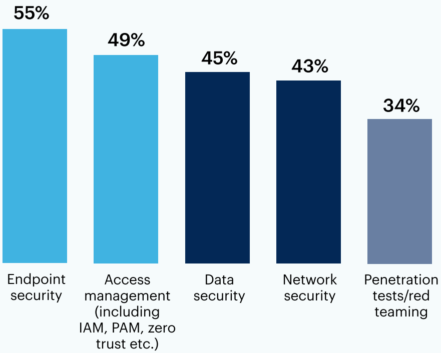


> "Leadership is never proactive and only pays attention after a successful breach."
>
> - Director, education sector,
> 1,000 - 5,000 employees

> "If you have to wait on human interaction to isolate and protect, it is already too late."
>
> - Director, software industry,
> 1,000 - 5,000 employees

Endpoint security is the most common area of focus, while integrating new tools into legacy systems is the most frequently cited challenge

The most commonly reported cybersecurity measures that decision makers are adding or enhancing in Q1 are **endpoint security (55%)**, **access management (49%)** and **data security (45%)**.



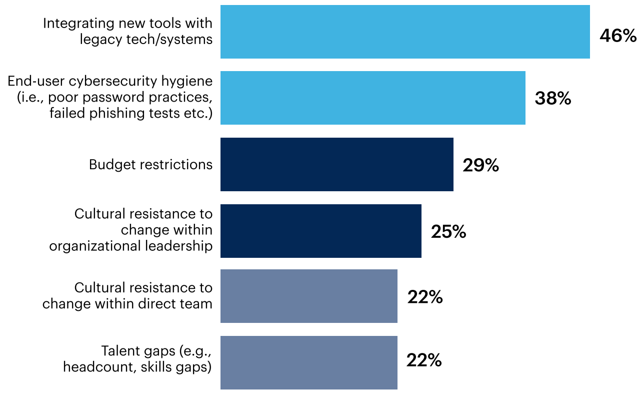
Are you focussing on adding or enhancing any of the following cybersecurity measures this quarter?

Disaster recovery **32%**, Firewalls (e.g., web application firewalls, network firewalls) **31%**, Hardware **13%**, Cybersecurity mesh strategy **11%**, Security event logging/insights (e.g., SIEM) **11%**, Deception technology **9%**, None of these **3%**, Other **1%**

n=361

The most commonly cited cybersecurity challenges in Q1 are **new tool integration (46%), end-user cybersecurity hygiene (38%),** and **budget restrictions (29%).**

What are your top cybersecurity challenges this quarter?



Increasing frequency of cybersecurity incidents **16%**, Bandwidth limitations (too much work for team to handle) **14%**, Government cybersecurity mandates **14%**, Lack of coherent cybersecurity strategy **8%**, Rising costs **8%**, Supply chain shortages (e.g., procuring hardware) **8%**, Lack of leadership **6%**, Attack disruption **4%**, None of these **0%**, Other **0%**

n=361

> "Client Identity and Access Management are huge areas that our teams will be focusing on as well as Identity Proofing."
>
> - VP, finance industry, 10,000+ employees

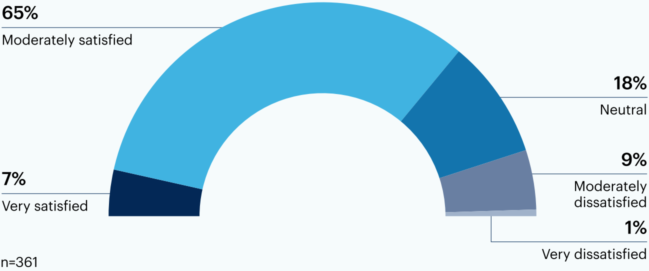
> "Enhancing the security culture and posture of our customers - which causes potential risk to our services."
>
> - C-suite, software industry, 1,000 - 5000 employees

> “We have signed up for a tool that provides AI based detection and blocking. It’s too early to tell, but its initial detections whilst in transparent mode are promising.”
>
> - C-suite, finance industry, 10,000+ employees

Most feel satisfied with their current cybersecurity posture, and confidence is high for achieving cybersecurity goals this quarter

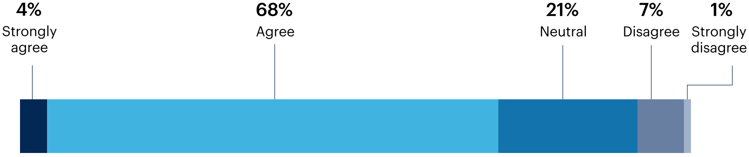
Most (72%) feel satisfied with their organization’s current cybersecurity posture.

Are you satisfied with your organization’s current cybersecurity posture?



72% feel **confident** they will achieve their cybersecurity goals in Q1.

To what extent do you agree with the following: “I am confident I will achieve my cybersecurity goals this quarter.”



n=361

> “When you wear many hats (cybersecurity being one of them), more visible projects tend to be pushed forward in priority and mindshare. It’s important to keep trudging forward with cybersecurity; if you take your foot off the gas pedal, you open yourself to attacks.”
>
> - Director, professional services industry, 1,000 - 5,000 employees

> “We feel confident about our goals this quarter.”
>
> - C-suite, finance industry,
> 1,000 - 5,000 employees

> “It will be a busy quarter.”
>
> - C-suite, healthcare industry,
> 1,000 - 5000 employees

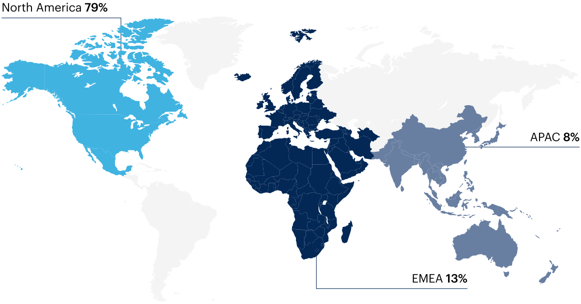
> “[It is] increasingly difficult to hire/retain [cybersecurity] talent.”
>
> - Director, software industry, 1,000 - 5,000 employees

Want more insights like this from IT leaders like you?

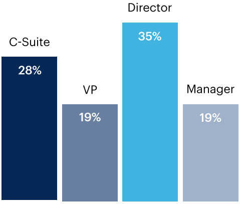
Click here to explore the revamped, retooled and reimagined Gartner Peer Insights. You'll get unprecedented access to verified reviews, synthesized insights and engaging discussions from a community of your peers.

Respondent Breakdown

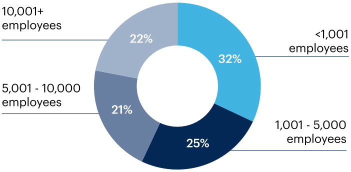
Region



Title



Company Size



Gartner

This content, which provides opinions and points of view expressed by users, does not represent the views of Gartner; Gartner neither endorses it nor makes any warranties about its accuracy or completeness.

Source: Gartner Peer Insights, Cybersecurity Quarterly Benchmarks: Q1, 2022 survey

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved.