Gartner
Peer Community™

Innovations in Security Awareness & Training

Security awareness and training programs aim to address the human element in cybersecurity, making them a must-have for any organization as the threat of social engineering attacks persists. How are leaders innovating to improve training so that more employees think and act securely?

One-Minute Insights:

- Just over one-quarter say their organization has a security awareness officer primarily responsible for the training program
- The majority of respondents say employees are required to complete security training on at least a quarterly basis, but ongoing training is relatively uncommon
- Most respondents deliver security awareness and training via a purchased solution
- About one-third say their security awareness and training content is lacking in regards to accessibility, relevance or technical complexity
- Over three-quarters of surveyed leaders expect to see their security awareness and training budget increase in the next year

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

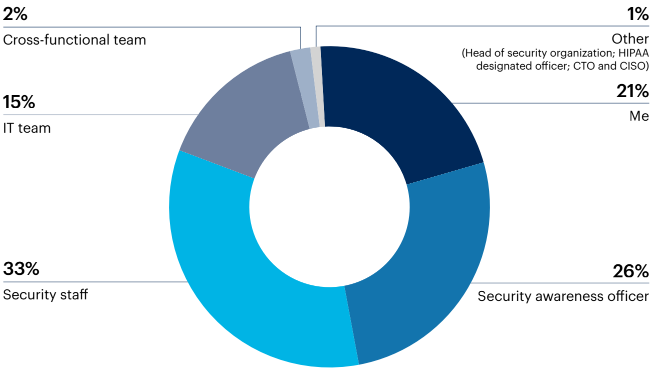
Data collection: Nov 15, 2022 - Feb 23, 2023

Respondents: 300 IT and information security leaders involved in the design and/or execution of their organization's security awareness and training program

Responsibility for awareness and training programs typically rests with security, but in some organizations it is owned by the security awareness officer

More than half **(59%)** of respondents say their organization's **security awareness and training** is owned by the **security function**, with **26%** indicating their organization has a **security awareness officer** for this purpose.

Who is primarily responsible for your organization's security awareness and training program?



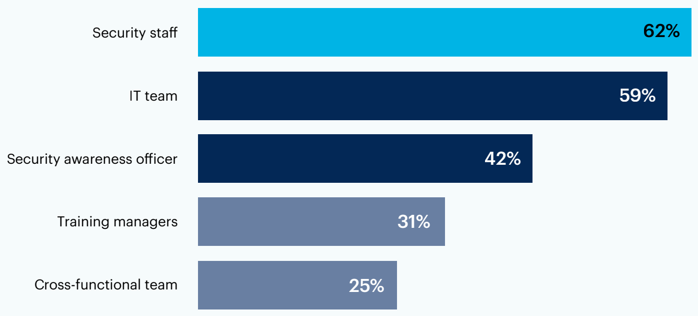
Training managers **<1%** | HR staff **<1%** | None of these **0%**

n = 300

Note: May not add to 100% due to rounding

While most leaders report that staff from security **(62%)** and IT **(59%)** teams are involved in **building and operating their security awareness and training program**, the inclusion of training managers **(31%)**, a cross-functional team **(25%)** or HR staff **(23%)** in these efforts is not uncommon.

Apart from yourself, who else is involved in the design and/or execution of the security awareness and training program? Select all that apply.



HR staff **23%** | None of these **2%** |
Other (Corporate communications team; Compliance team; Legal staff; CEO; CTO) **2%**

n = 300

> "There is a fine line to walk with security training metrics and individual integrity. We spent a lot of time discussing with HR and DPOs before settling on a model."
>
> - VP, manufacturing industry, 1,000 - 5,000 employees

> “My company has been working on getting more support from externals to increase security awareness.”
>
> - Director, telecommunications industry, 10,000+ employees

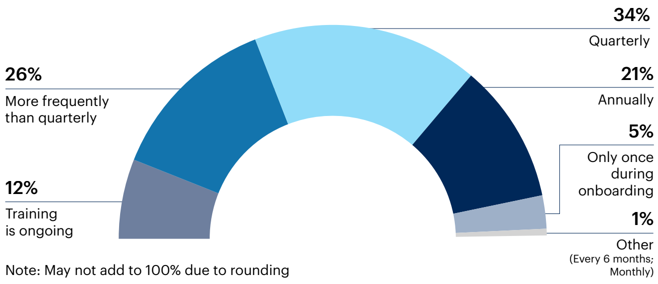
> “We are far from innovating in terms of security awareness and training.”
>
> - Director, natural resource extraction industry, 1,000 - 5,000 employees

Question: Do you have any final thoughts to share on security awareness and training?

Most leaders say employees must complete awareness and training modules at least quarterly, which are delivered via a purchased solution

72% of leaders say their employees are required to **complete security awareness and training modules** at least quarterly if not more often. Only **5%** of leaders say their employees receive this training just once during onboarding.

How often are most employees required to complete security awareness and training modules or activities?



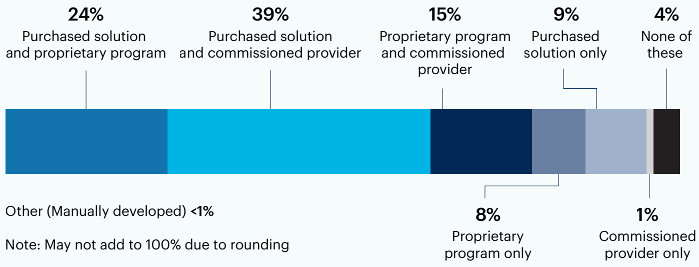
Note: May not add to 100% due to rounding

n = 300

Nearly three-quarters **(72%)** report using a **purchased solution** in some capacity to deliver **security awareness and training**; **39%** combine this solution with a **commissioned provider**.

47% say they use a **proprietary program** and just 8% rely on this exclusively to deliver training.

How do you deliver security awareness and training?



Other (Manually developed) **<1%**

Note: May not add to 100% due to rounding

n = 300

> “We looked at a very capable security awareness and phishing testing platform last year, but getting the capex approved is difficult as our industry is under financial pressure.”
>
> - C-suite, finance industry, <1,000 employees

> “Ongoing training is critical, but getting employee participation is a challenge.”
>
> - Director, educational services industry, 1,000 - 5,000 employees

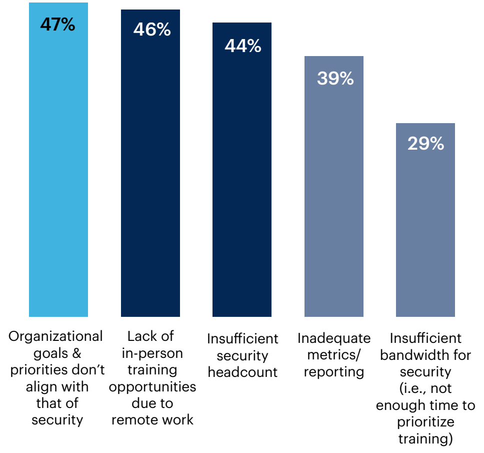
Question: Do you have any final thoughts to share on security awareness and training?

Strategic misalignment and content-related challenges are common, and many say engagement levels show room for improvement

Many **(47%)** cite **strategic misalignment between security and the business** as one of the **biggest operational challenges** facing their **security awareness and training program**.

Respondents also listed insufficient opportunities for in-person training **(46%)**, as well as gaps in security headcount **(44%)** and metrics or reporting **(39%)** as major hurdles.

What are the biggest operational challenges for your security awareness and training program? Select up to 3.

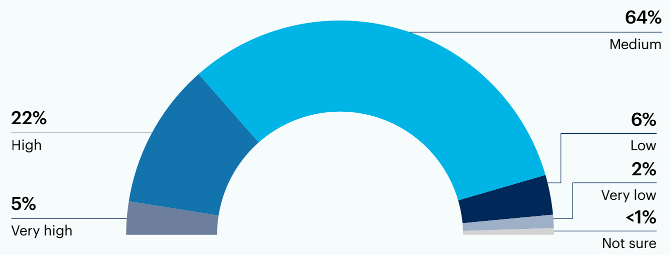


Insufficient budget **17%** |
Lack of executive support **11%** |
Lack of effective tools **9%** |
Lack of board support **5%** |
None of these **4%** |
Other (Time; Staff think it's a waste of time) **1%**

n = 300

Almost two-thirds **(64%)** indicate **moderate engagement** levels with their **security awareness and training**, while **27%** say employee **engagement is high**.

What is the level of employee engagement with your security awareness and training?



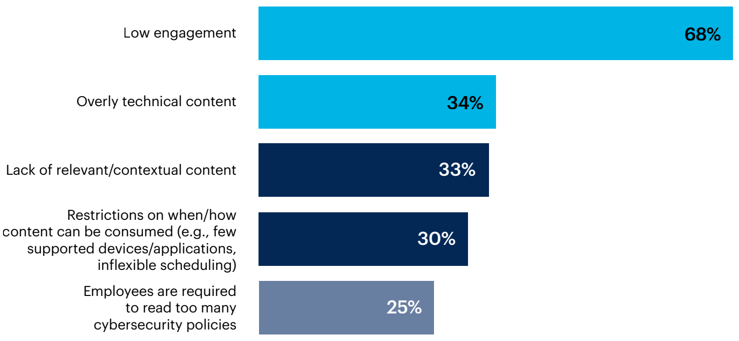
Note: May not add to 100% due to rounding

n = 300

But in terms of their **security awareness and training program's design**, more than two-thirds **(68%)** of leaders say **low engagement** is one of the **biggest challenges**.

About **one-third** pointed to **content-related issues**, including the use of material that is overly technical **(34%)** or lacks relevance **(33%)**, as well as restrictions on when or how employees access content **(30%).**

What are the biggest challenges you've had with the design of your security awareness and training program? Select up to 3.



Mistargeted campaigns **23%** | Ineffective messaging **22%** | None of these **5%** |
Other (Language barriers; Resource availability; Time to implement) **1%**

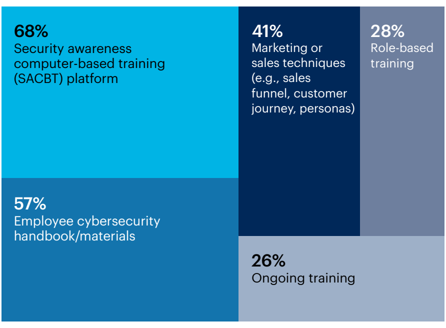
n = 300

> **"Without real executive buy in and not just lip service, security will never be a high enough priority for most employees."**
>
> - Director, software industry, 1,000 - 5,000 employees

> **"It is an ongoing challenge as risks continue to develop. The more inundated with info the staff become, the more blind they become and the more fatigued they are. The balance is tough."**
>
> - C-suite, healthcare industry, <1,000 employees

Question: Do you have any final thoughts to share on security awareness and training?

Less than half say their security awareness and training program uses marketing or sales techniques, but most expect funding increases

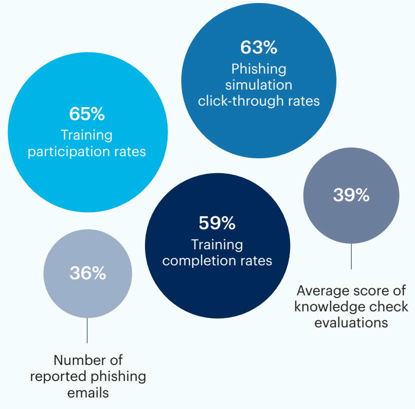


The majority of respondents have programs that incorporate a **security awareness computer-based training (SACBT) platform (68%)** or an employee cybersecurity handbook **(57%)**, and many say their program design employs marketing/sales techniques **(41%)**.

Does your program design incorporate any of the following? Select all that apply.

Expert instructor-led courses **23%** | Nudge techniques **13%** | Remedial training **11%** |
Showcase phishing campaign results **11%** | Consequences for clicking phishing links **10%** |
Training modules featuring real examples of breaches that occurred at your organization **9%** |
Policy requiring employees to pass training to gain certain access rights **8%** |
Showcase training/knowledge check results to create competition **6%** | None of these **1%** | Other **0%**

n = 300



The **most common program metrics** used by respondents are training participation rates **(65%)**, click-through rates for phishing simulations **(63%)** and training completion rates **(59%)**.

Few **(8%)** say they use the **number of required password** changes as a **performance metric** for their **security awareness and training program**.

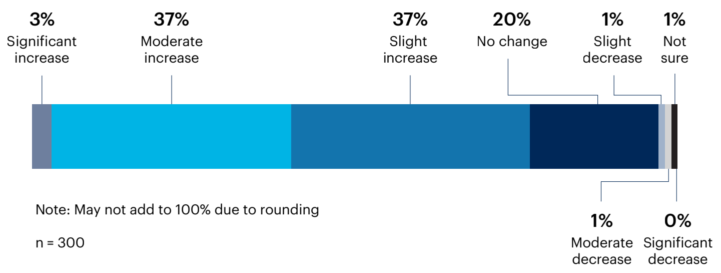
What metrics are you using to track the effectiveness of your security awareness and training program? Select all that apply.

Number of cybersecurity incidents due to data misuse/policy violations **21%** | Completion rates for non-mandatory training **17%** | Number of cybersecurity incidents due to human error **17%** | Number of required password changes **8%** | None of these **2%** | Other **0%**

n = 300

77% anticipate their **security awareness and training budget** will **increase** by some degree in the next year; only **2%** expect to see any **decrease** in funding.

Do you expect your budget for security awareness and training to change in the next year?



Note: May not add to 100% due to rounding

n = 300

> “It’s difficult to make it fun and interesting, but it is crucial.”
>
> - Director, real estate industry, <1,000 employees

> “We have had separate versions of security training for technical and non-technical people that’s applied based on their role.”
>
> - VP, software industry, <1,000 employees

> “It should be a continuous and relational program. Individual and independent activities do not last.”
>
> - VP, transportation industry, 10,000+ employees

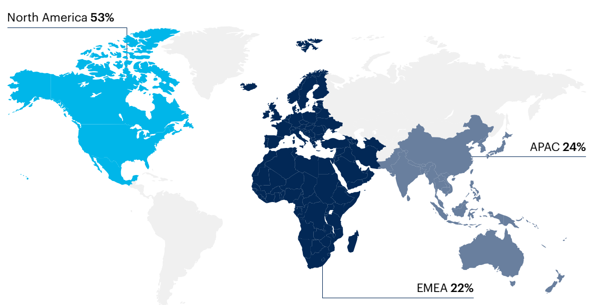
Question: Do you have any final thoughts to share on security awareness and training?

Want more insights like this from IT leaders like you?

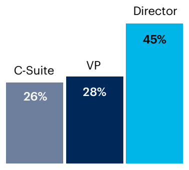
Click here to explore the revamped, retooled and reimagined Gartner Peer Community. You’ll get access to synthesized insights and engaging discussions from a community of your peers.

Respondent Breakdown

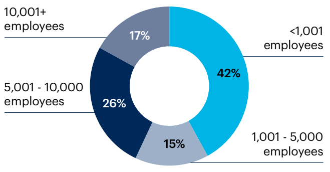
Region



Job Level



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 Community, Innovations in Security Awareness & Training survey

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved.