2023 SECURITY AWARENESS STUDY

How Effective Are Your Awareness Programs — and Do Your Employees Agree?

INSIDE:

Executive Summary
Complete Survey Results
Expert Analysis

Study Sponsored by Proofpoint

proofpoint®

iSMG
INFORMATION SECURITY
MEDIA GROUP

INTRODUCTION

TOM FIELD
SVP, Editorial
Information Security Media Group

Welcome to the report summarizing the **2023 Security Awareness Study**.

The reason for this survey

How often do you hear one of these phrases?

- Our employees are our strongest line of defense.
- Our employees are our single biggest vulnerability.

The first statement is true; the second one need not be. The key: effective security awareness programs.

But who decides whether an awareness program is effective—or what even makes it effective? Is it the cybersecurity executive or business leader who designs and administers the program? Or is it the employee who completes the training?

This research project seeks to assess the efficacy of cybersecurity awareness programs from both perspectives—the security professional and the non-security employee. The goals of this survey are to determine:

- The frequency, content and efficacy of current cybersecurity awareness programs
- How employees rate the success of awareness efforts
- Awareness program gaps and how they can be filled in 2023

The responses from cybersecurity professionals are compared to those of non-security professionals to assess not just the biggest awareness gaps but the shared understanding of those gaps—and, of course, how they can be filled in the year ahead.

Best,

Tom Field
SVP, Editorial
Information Security Media Group
tfield@ismg.io

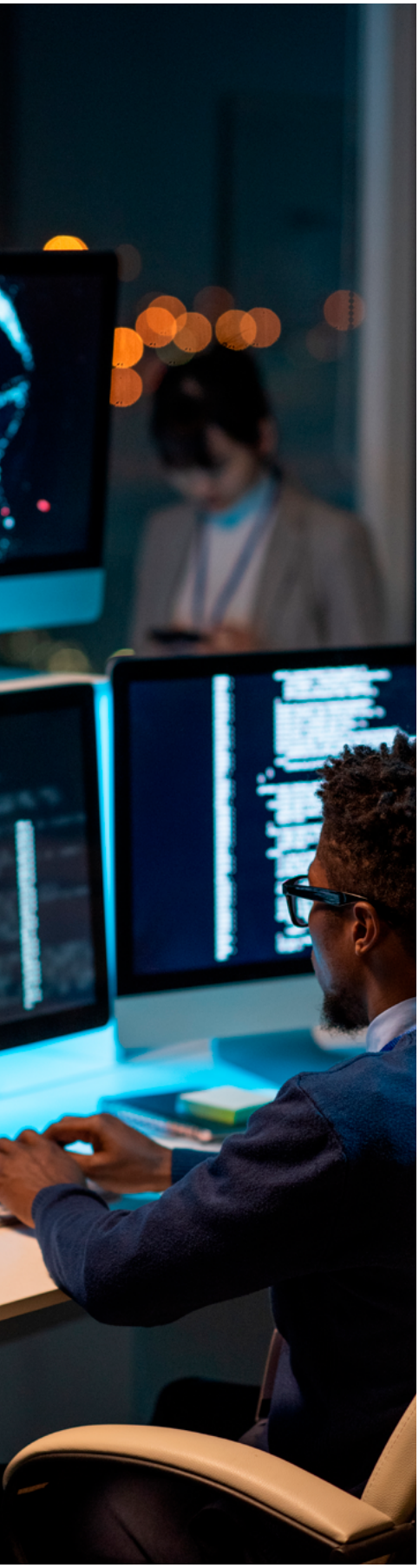


TABLE OF CONTENTS

ABOUT THIS SURVEY:

This survey was conducted in spring and summer of 2022. Focused on financial services across regions, the study attracted more than 330 responses from across sectors and regions. Of the respondents, nearly 200 were cybersecurity professionals. More than 130 were non-security pros.

Introduction **2**

By the Numbers **4**

Executive Summary **5**

Survey Results **8**

Conclusions **27**

Expert Analysis: Sara Pan, Team Manager, Product Marketing, Proofpoint **29**

ABOUT PROOFPOINT INC.:

Proofpoint Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyberattacks. Leading organizations of all sizes, including 75% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web.

More information is available at www.proofpoint.com.

proofpoint.

BY THE NUMBERS
STATISTICS THAT JUMP OUT FROM THIS STUDY

SECURITY PROS SAY:

56%

Our organization's cybersecurity awareness efforts are above average or superior

64%

There are no incentives for "good" cybersecurity behavior

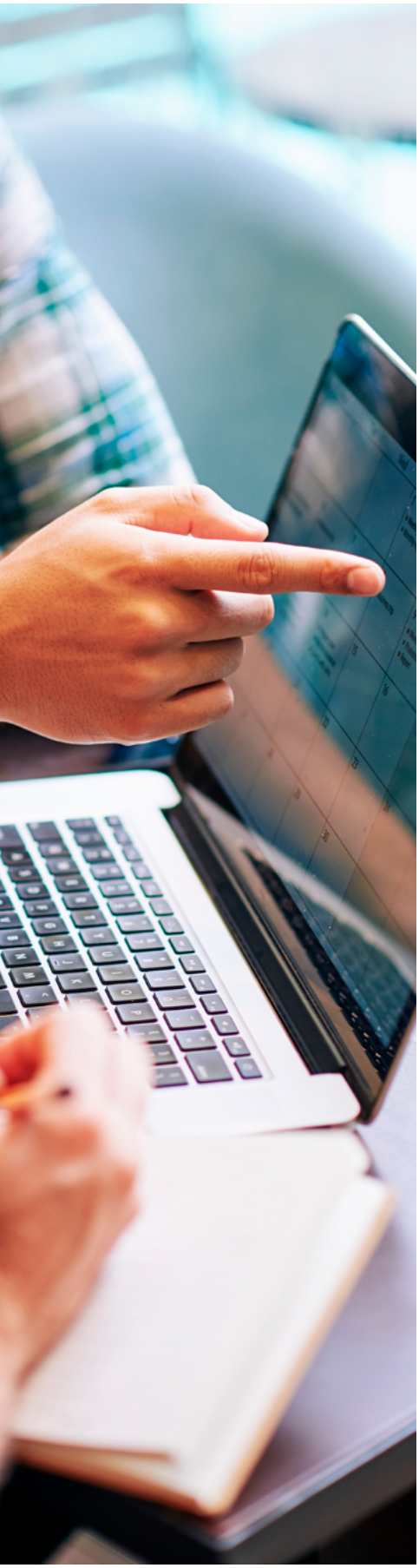
NON-SECURITY PROS SAY:

67%

Our organization's cybersecurity awareness is above average or superior.

38%

Our employees are "just going through the motions" when it comes to training



EXECUTIVE SUMMARY

This truly is a tale of two surveys, as researchers strive to identify the gaps between what cybersecurity professionals say is being offered for standard awareness training and what non-security pros in the field say is the reality of the training they receive. Together, these two groups offer insight into the most important training topics, the best methods and frequency of training, and gaps to fill in 2023.

Mainly, the respondent groups are in agreement on topics such as:

Enterprise Security Posture

- **Security Pros:** Enterprise security posture is above average or superior — 52%
- **Non-Security Pros:** Enterprise security posture is above average or superior — 55%

Quality of Awareness Efforts

- **Security Pros:** Quality of current awareness efforts is above average or superior — 56%
- **Non-Security Pros:** Quality of current awareness efforts is above average or superior — 69%

Most Effective Forms of Awareness

- **Security Pros:** Phishing simulation exercises — 31%
- **Non-Security Pros:** Phishing simulation exercises — 36%

Goals for these two surveys were similar, but also unique where necessary.

For Security Pros: Survey goals were to determine:

The frequency, content and efficacy of current cybersecurity awareness programs:

- 57% say training is done annually.
- The top three training topics are:
  - Phishing/BEC — 94%
  - Passwords/authentication — 86%
  - Ransomware — 77%

SOME INTERESTING DATA POINTS

SECURITY PROS:

- **Most Effective Types of Training:**
  - Phishing simulation exercises — 31%
  - Virtual self-paced computer-based training — 17%
  - In-person classroom training — 14%

- **How Programs Are Evaluated:**
  - Click rate on simulated phishing tests — 73%
  - Completion rates on educational materials — 64%
  - Reporting rate on simulated phishing test — 58%

NON-SECURITY PROS:

- **What Employees Say They Have Gained From Training:**
  - I can identify suspicious attachments that might lead to phishing scams — 86%
  - I feel comfortable asking for help if I am unsure what to do — 86%
  - I know how to report a phishing attempt — 84%

- **Topics That Need More Attention:**
  - Phishing/BEC — 54%
  - Social engineering — 45%
  - Home/remote networking standards — 44%
  - Ransomware — 40%

Awareness program gaps and how they are being filled:

- The top three gaps are:
  - There are no incentives for good behavior — 46%
  - Employees are just going through the motions — 43%
  - There are no consequences for repeat offenders — 31%

- Planned future investments:
  - Phishing simulation exercises — 49%
  - Virtual self-paced training — 40%
  - Third-party programs — 31%

Survey Goals for Non-Security Pros:

The frequency, content and efficacy of current cybersecurity awareness programs:

- Programs are offered annually — 40%

Most effective types of training:

- Phishing simulation exercises — 36%
- In-person classroom training — 16%
- Virtual self-paced computer-based training — 16%

Awareness program gaps and how they should be filled in 2022:

- Employees are just going through the motions — 38%
- There are no incentives for good behavior — 38%

In the report that follows this summary, you will see exactly what security and non-security pros say about their current and future cybersecurity awareness programs. But here's what stands out when you combine the storylines: Security pros and employees fundamentally agree about the quality of enterprise security posture. And they also agree on several key points:

- Employees are often just going through the motions when it comes to awareness training.
- Having rewards and consequences would improve engagement.
- Phishing simulation exercises are currently the most effective type of training.
- Phishing needs even more attention in 2023.

Sara Pan of survey sponsor Proofpoint reviewed the results — individually and combined — and weighs in with her analysis of what respondents are saying.

"While phishing and BEC or ransomware are already the most covered topics based on the survey, employees are requesting more information," she says. ***"And many security professionals rely on newsletters to communicate security initiatives to employees. But interesting finding: None of the employees consider newsletters effective."***

"So that tells security professionals that they need to utilize multiple mediums to communicate to their employees. They cannot rely on, let's say, just newsletters, or just training, or just phishing simulation. You have to take advantage of all these different mediums because people consume information from different mediums."

Read on for full results — of both surveys — and expert analysis of the results and how to put them to use to improve your own organization's awareness efforts.

SECURITY PROFESSIONALS SURVEYED

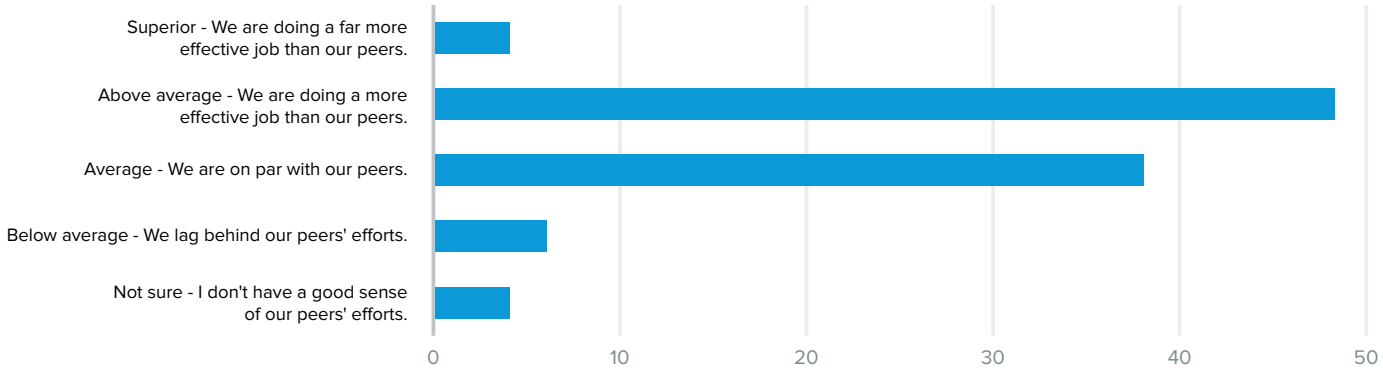
NOTE: For this section of the survey, there were 198 respondents. Twenty-eight percent were CISOs, 17% came from financial services and 13% were from government. Only *top* results are included in the charts, so not all totals for each question will add up to 100%.

PART 1 — BASELINE QUESTIONS

This opening section surveys security pros on their basic cybersecurity posture and the degree to which it is influenced by the success of their cybersecurity awareness programs.

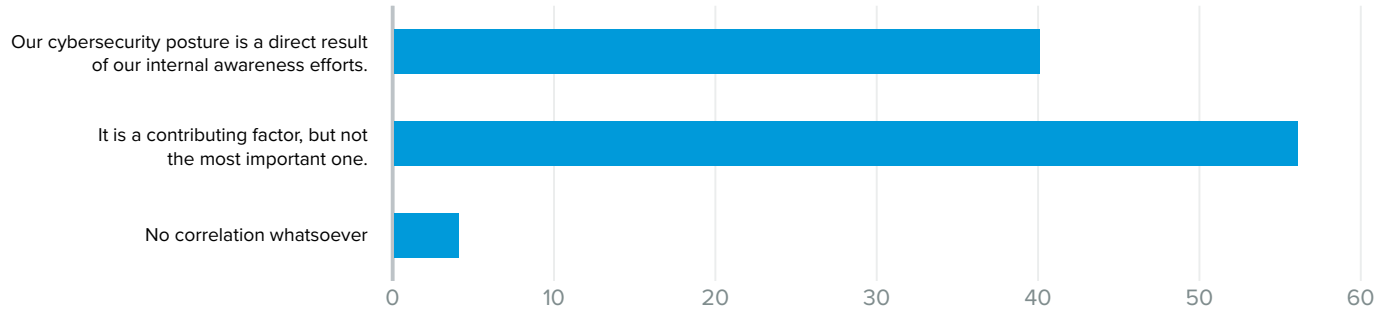
1. How do you assess your organization's relative cybersecurity posture in comparison to peers in your sector?

How are we doing compared to our peers?" This is a common cybersecurity question across sectors. Security pros tend to give what might be a statistically overoptimistic response: 52% believe their postures is above average or superior. 38% claim average, and just 6% say below average.



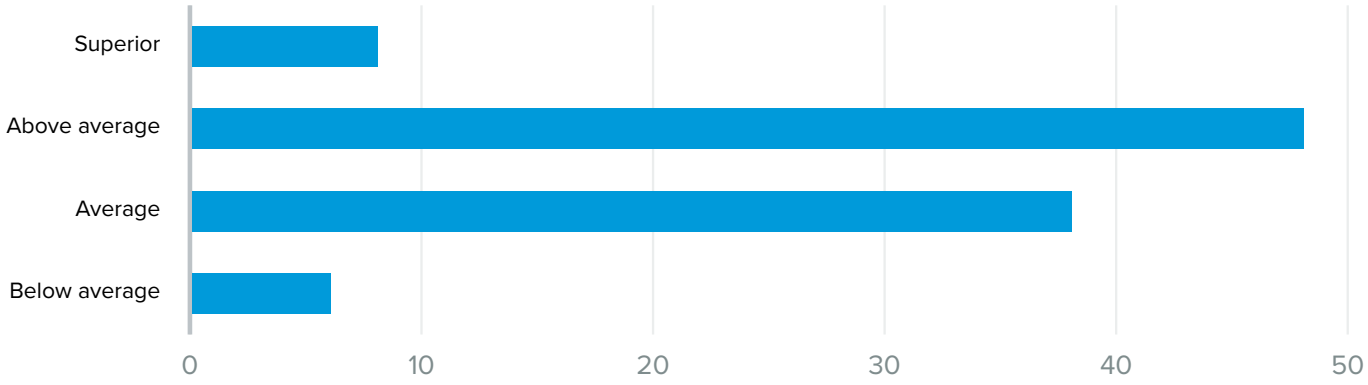
2. To what degree do you tie the strength of your organization's cybersecurity posture to the success of your internal cybersecurity awareness efforts?

Only 4% of respondents see no correlation. Meanwhile, 56% say awareness efforts are a contributing factor, and 40% say the cybersecurity posture is a direct result of internal awareness efforts.



3. If you were to assign a ranking, how would you assess your organization's current cybersecurity awareness efforts in terms of clarity, quality and effectiveness?

Again, a "glass half full" response: 56% of respondents judge their programs above average or superior. Only 6% say below average.

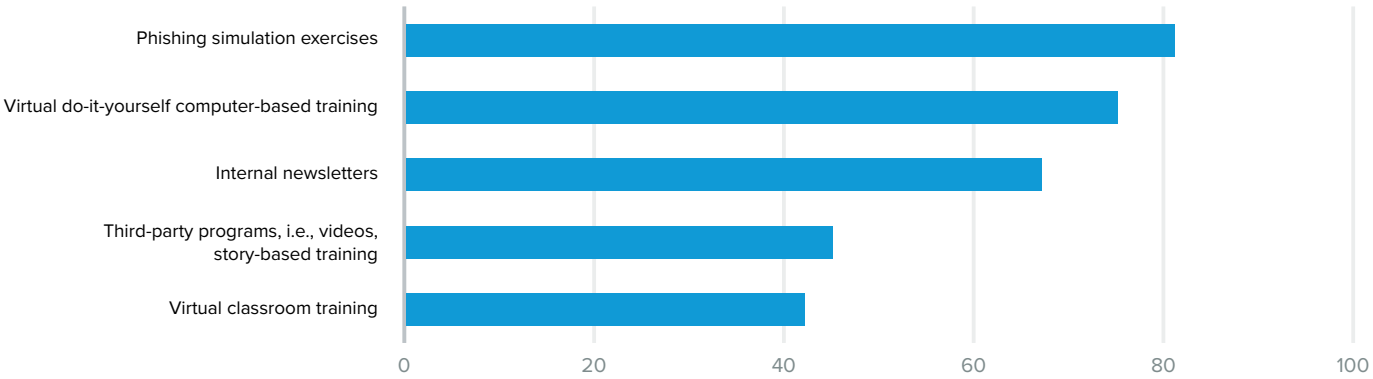


CURRENT AWARENESS PROGRAM

Here the report delves into specific awareness programs being offered, as well as the frequency and measured success of the training.

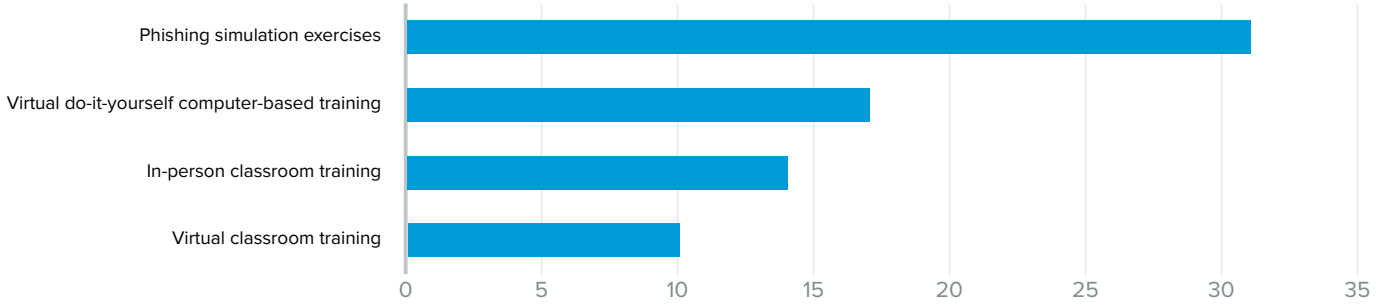
4. What types of cybersecurity awareness programs does your organization currently offer? (Select all that apply.)

Phishing simulation exercises are the most popular form of training administered, chosen by 81% of respondents. Other top vote-getters: virtual self-paced computer-based training at 75% and internal newsletters at 67%. Note: Internal newsletters do not even register on the radar of the non-security pros, as illustrated in the next section of this report.



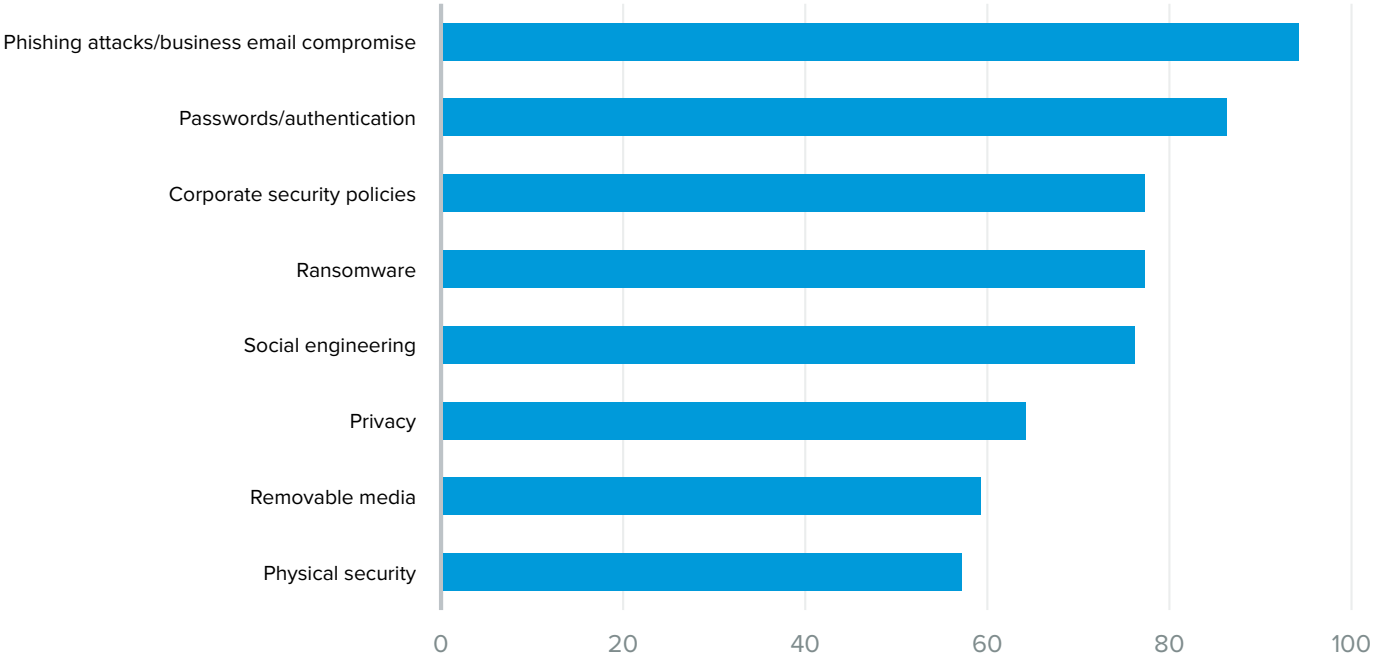
5. Which of these elements do you believe is most successful in reaching the intended audience?

What types of training are deemed most successful by security pros? Again, phishing simulation exercises place first at 31%, followed by computer-based training at 17% and in-person classroom training at 14%.



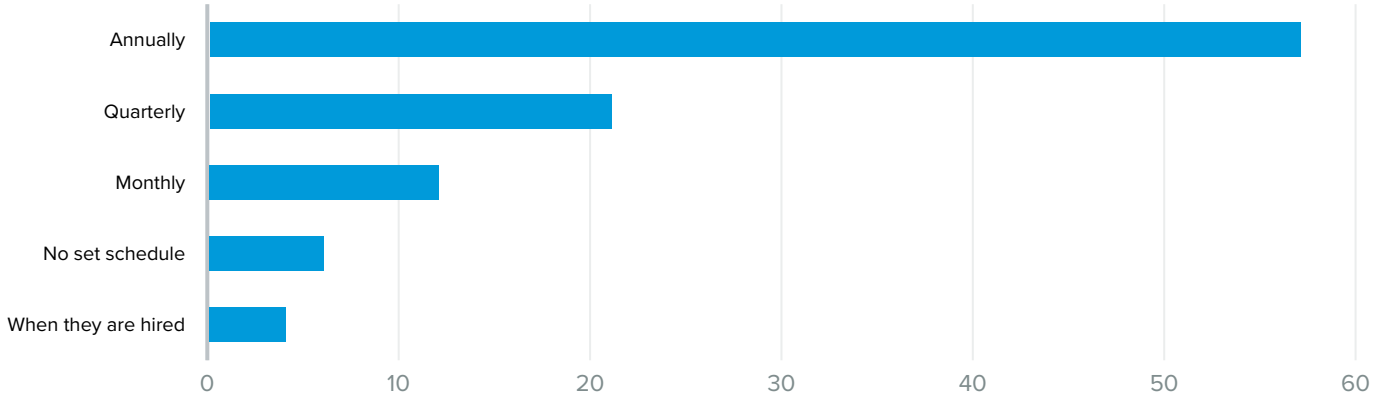
6. Which topics typically are covered in your cybersecurity awareness programs? (Select all that apply.)

There is no surprise for readers of any recent threat landscape reports. Phishing/business email compromise attacks remain hot, and they take the top spot in this poll at 94%. Other key topics are passwords/authentication at 86% and corporate security policies at 77%.



7. How frequently do employees receive cybersecurity awareness training?

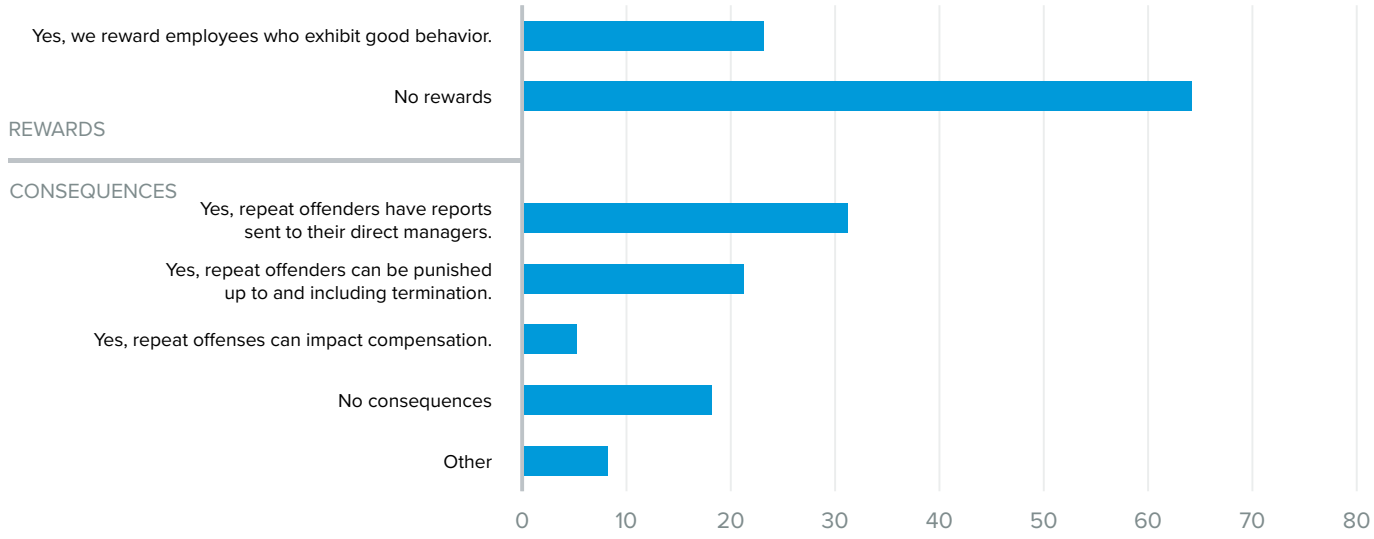
Despite the expressed criticality of security awareness programs, the majority of security pros — 57% — say their organizations only provide annual training. Roughly one-fifth (21%) offer quarterly training, and 12% say their programs are monthly.



8. Are there rewards for employees who report security incidents and/or consequences for employees who continually commit security errors even after undergoing training? (Select all that apply.)

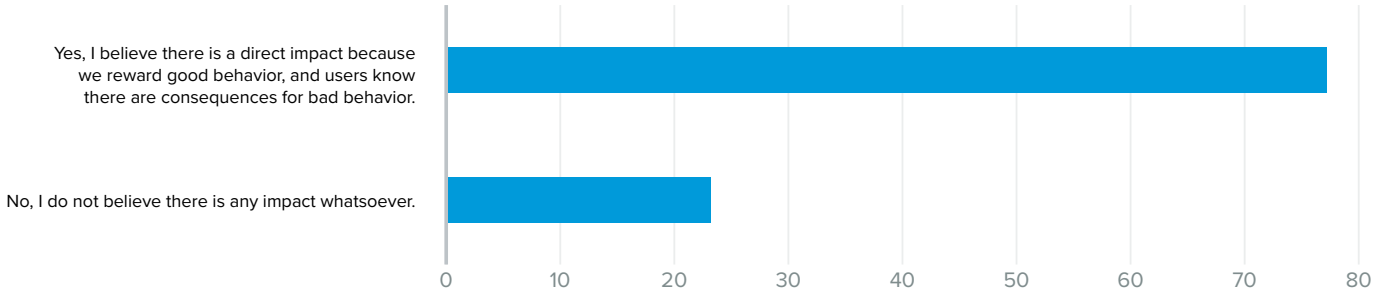
It's a common topic of discussion among security pros: Is it useful either to reward employees who report security incidents as a result of their training or to punish repeated violators of security policies?

Sixty-four percent of respondents say there are no rewards, and 18% report no consequences. Thirty-one percent say repeat offenders have reports sent to their direct managers, and 23% say their organizations reward employees who exhibit good behavior, such as reporting phishing emails.



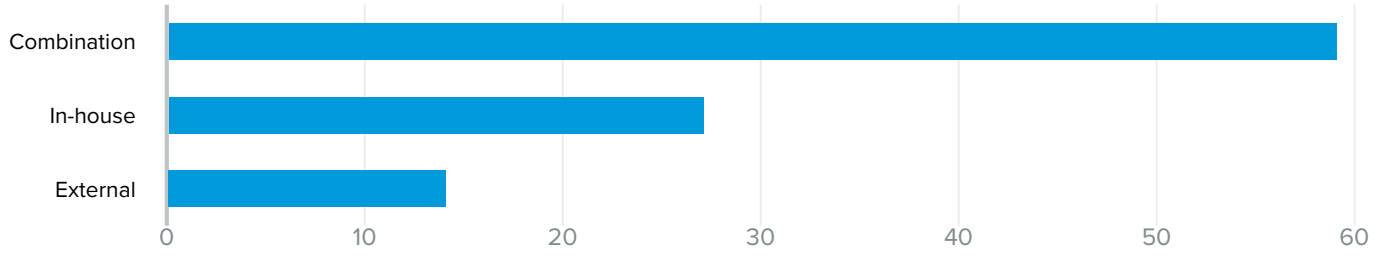
9. Do you believe the carrot/stick approach enhances — or could enhance — the success of your cybersecurity awareness programs? (Select all that apply.)

Following up on the previous question, security pros were asked whether a carrot/stick approach could enhance the success of their awareness programs. Seventy-seven percent say yes.



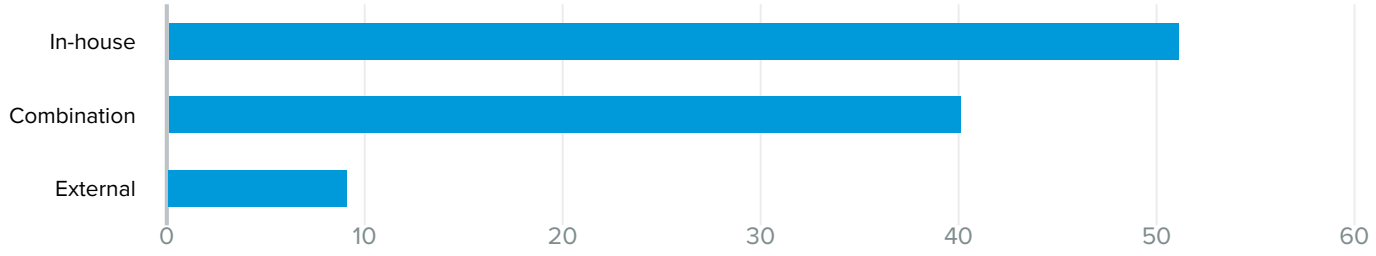
10. Are these programs created in-house or by external service providers?

Asked whether their awareness programs are created in-house or outsourced, 59% say it is a combination. Only 27% rely solely on in-house programs.



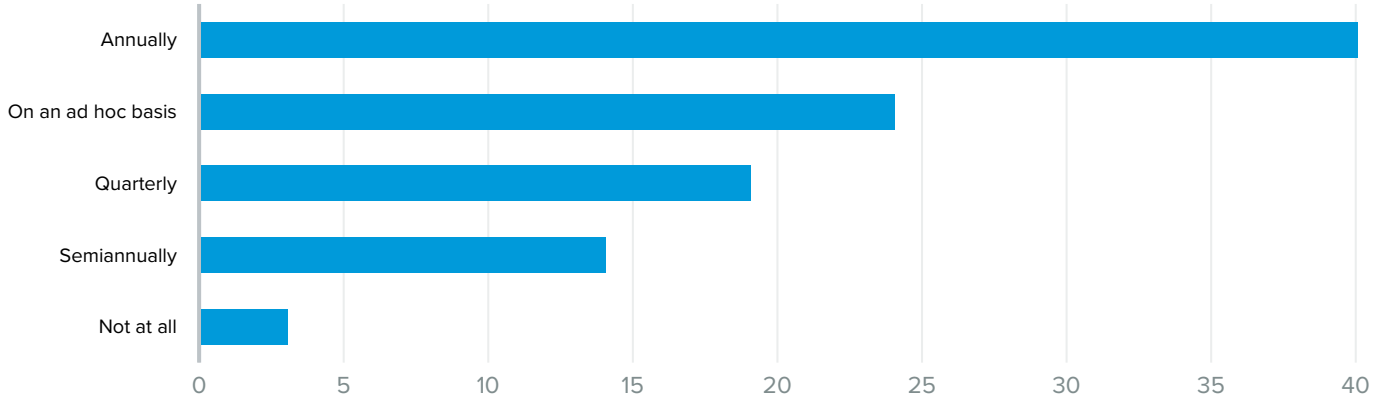
11. Are these programs run in-house or by external service providers?

Fifty-one percent of respondents say the programs are run entirely in-house, while 40% rely on a combination of in-house and outsourced administrators.



12. How frequently do you assess your cybersecurity awareness programs?

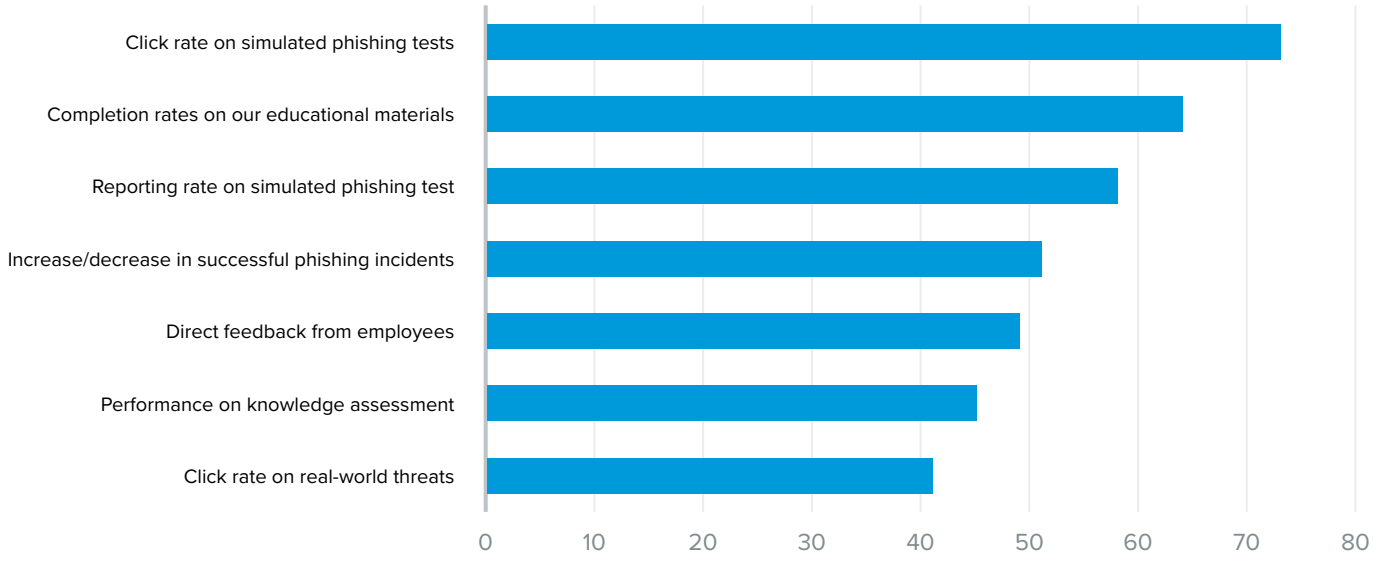
Threats evolve quickly in cybersecurity — but awareness programs do not. Forty percent of respondents say their programs are assessed annually, while 24% say it happens on an ad hoc basis.



13. When you do assess your awareness programs, what specifically do you review? (Select all that apply.)

When programs are reviewed, here are the three top metrics for security pros:

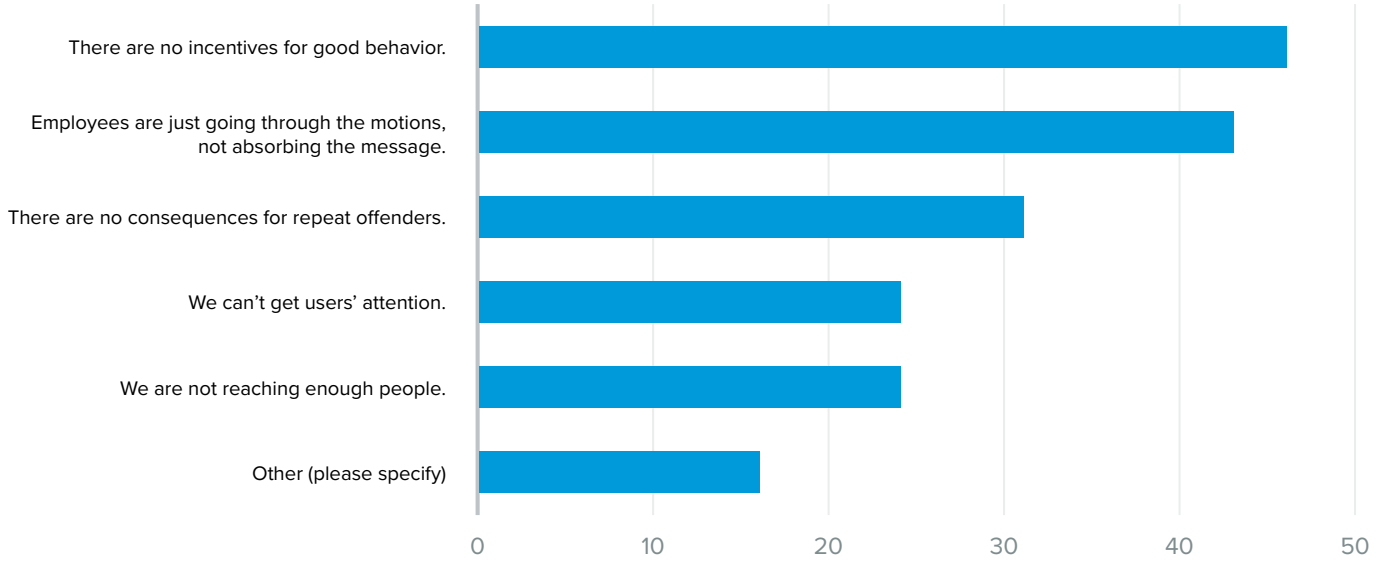
- Click rate on simulated phishing tests — 73%
- Completion rates on educational materials — 64%
- Reporting rate on simulated phishing tests — 58%



14. What do you deem to be the biggest gaps in your current cybersecurity awareness efforts? (Select all that apply.)

The biggest perceived gaps in current awareness efforts are:

- There are no incentives for good behavior — 46%
- Employees are just going through the motions — 43%
- There are no consequences for repeat offenders — 31%

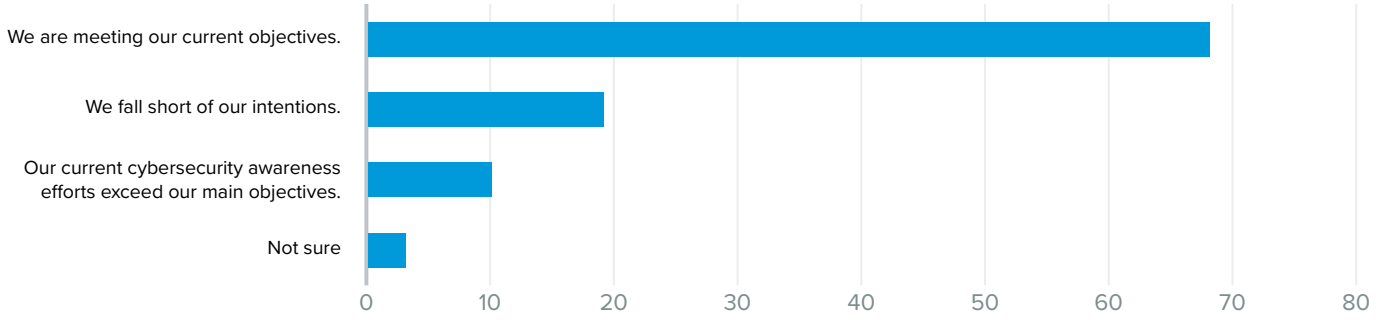


ASSESSING AWARENESS

Having described awareness in the previous section, security pros in this section discuss how to make their efforts more effective.

15. How well do you believe your organization's efforts are meeting their objectives?

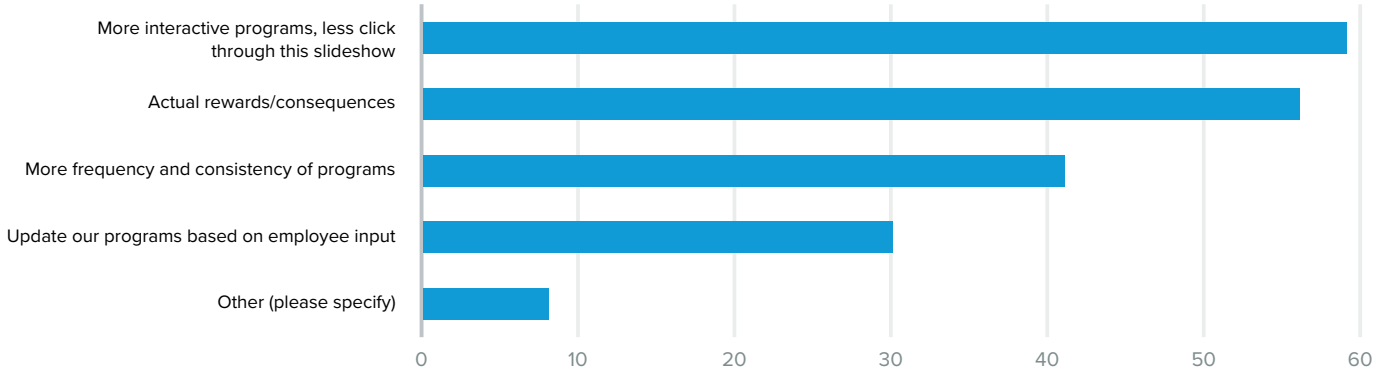
The good news: 68% of respondents believe they meet or exceed their security awareness objectives. Concerning news: Nearly one-fifth (19%) say they fall short of intentions.



16. What would make these efforts even more effective for employees? (Select all that apply.)

The biggest perceived gaps in current awareness efforts are:

- More interactive programs, less "click through this slideshow" — 59%
- Actual rewards/consequences — 56%



2023 STRATEGY

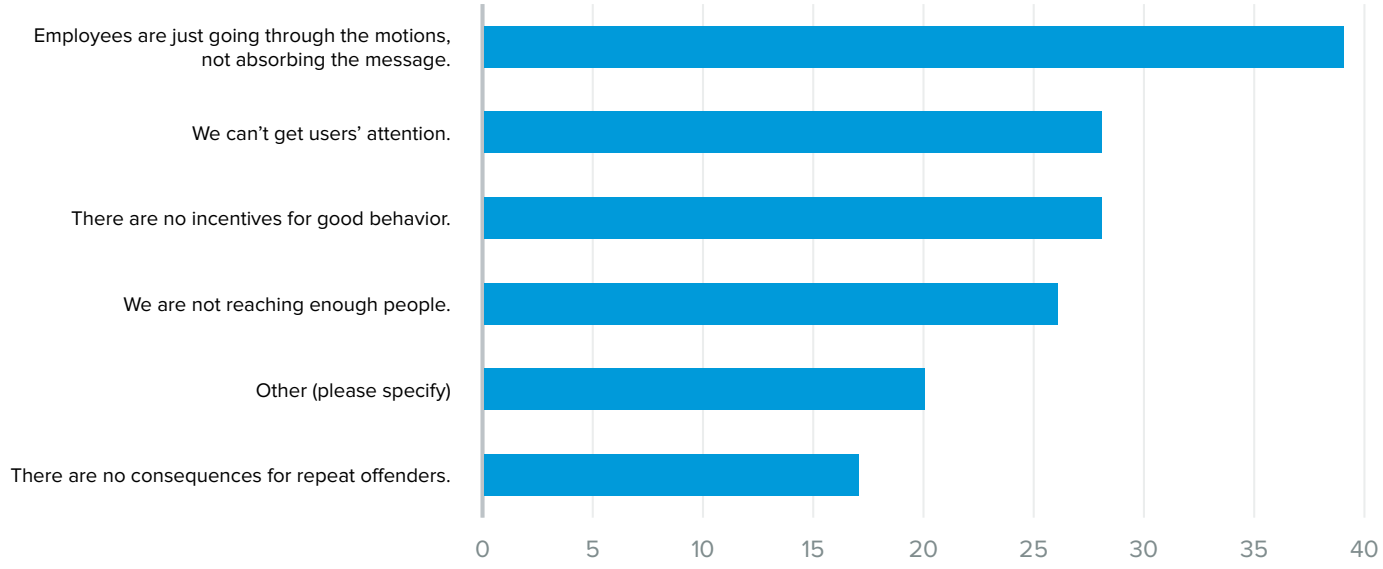
Finally, this section of the report focuses on 2023 strategies: How will organizations fill their awareness gaps, and how will associated budgets change? Given dramatic shifts in the global economic landscape since these survey results were collected in late 2022, it's not clear which budget plans will hold true through 2023, but here is the logic that set the stage for where enterprises are today.

Good news again: Only 3% of respondents have seen a budget decrease in the past year.

17. Which of these cybersecurity awareness gaps will your organization focus on addressing in 2023? (Select all the apply.)

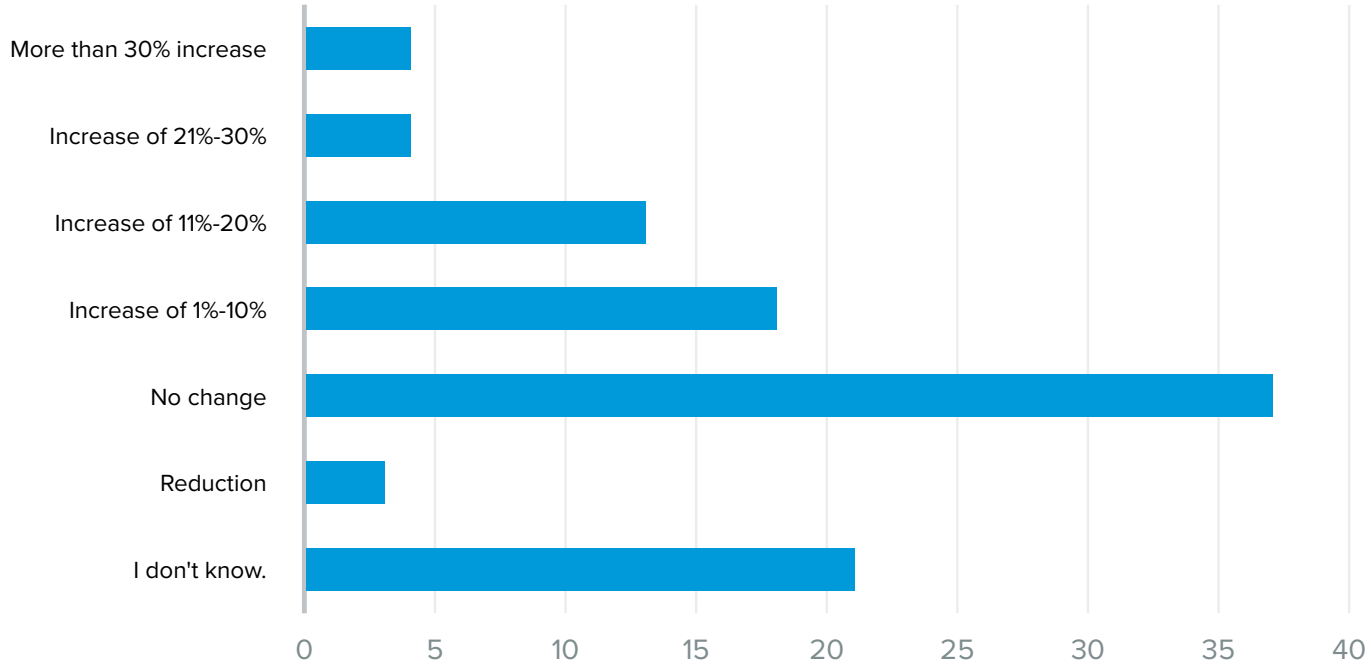
The three most important gaps to focus on in 2023 are:

- Employees just going through the motions — 39%
- There are no incentives for good behavior — 28%
- We can't get users' attention — 28%



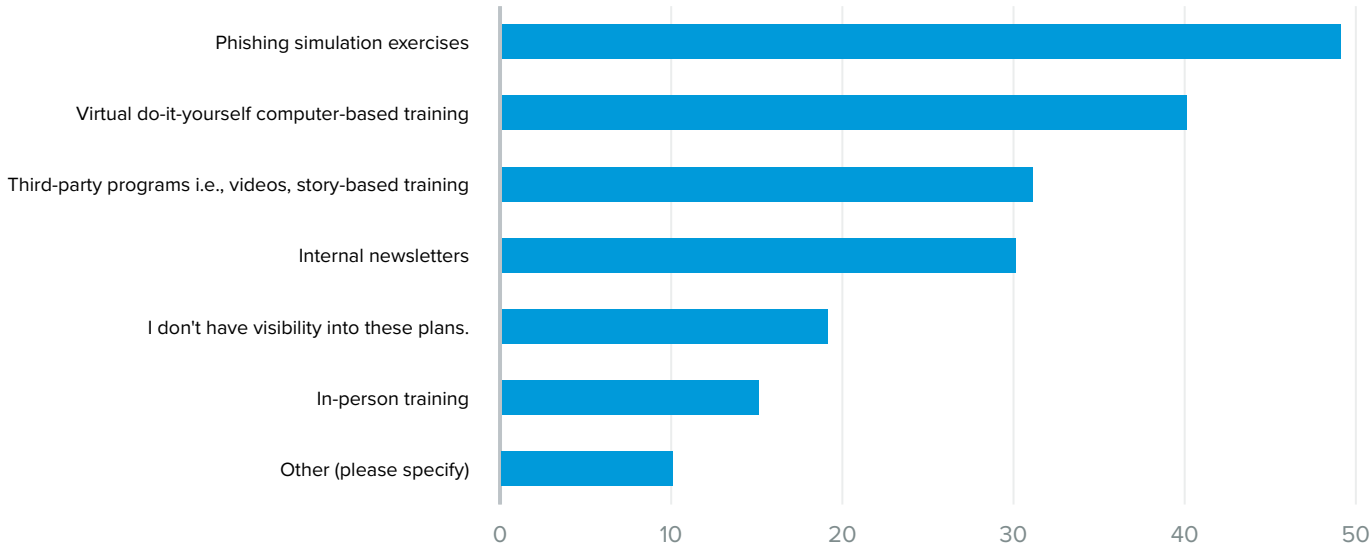
18. How has your organization's budget for cybersecurity awareness changed since 2021?

Thirty-seven percent of respondents have seen no change to their budgets for cybersecurity awareness, but an even larger amount — 39% — have seen increases of anywhere from 1% to more than 30%.



19. Which specific investments will your organization make in 2023? (Select all that apply.)

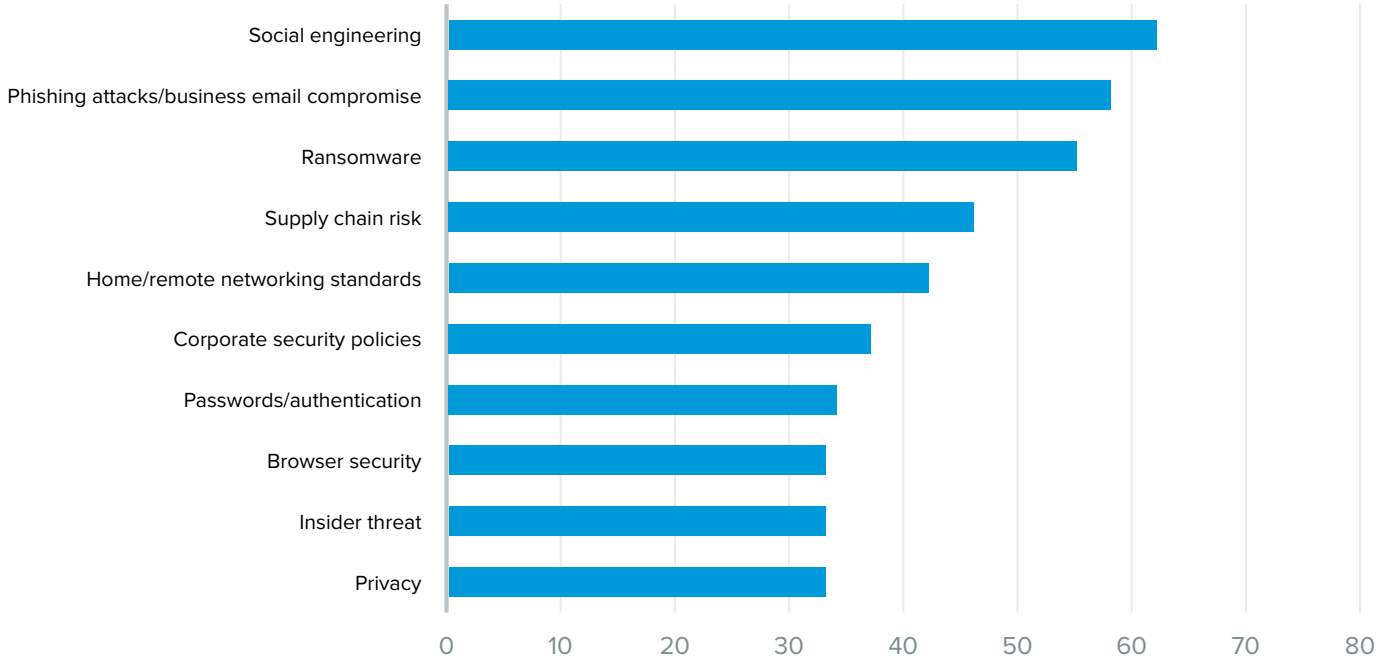
If given greater funds, where would security pros invest them? Primarily in more phishing simulation exercises, 49% of the respondents say, while 40% opt for an increase in computer-based training.



20. Which topic(s) should get greater attention in 2023? (Select all that apply.)

Finally, security pros indicate the topics that should receive greater attention in 2023. Here are their top three:

- Social engineering — 62%
- Phishing attacks/BEC — 58%
- Ransomware — 55%



NON-SECURITY PROFESSIONALS SURVEYED

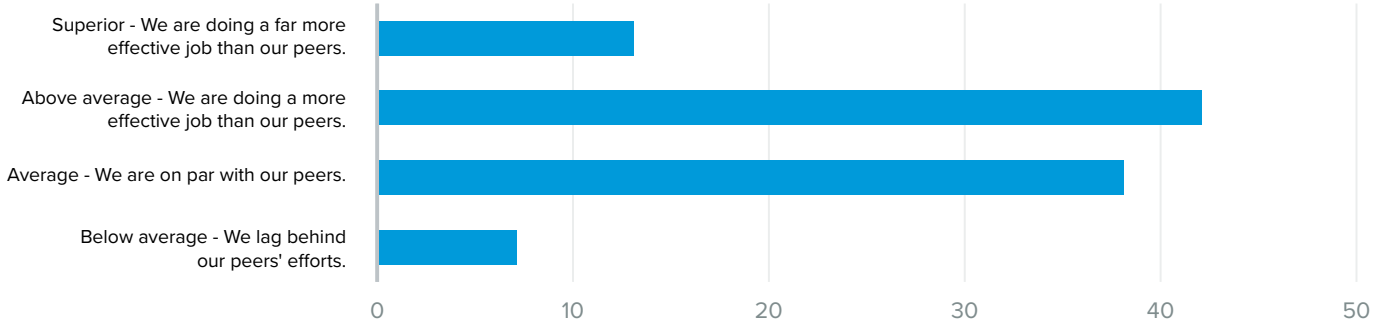
NOTE: For this section of the survey, there were 133 respondents. Twenty-two percent are business managers, 20% come from financial services, 13% from healthcare and another 13% from government. Again, only *top* results are included in the charts, so not all totals for each question will add up to 100%.

BASELINE QUESTIONS

Similar to the previous overview, this opening section surveys non-security pros on their organizations' basic cybersecurity posture, as well as their own levels of awareness.

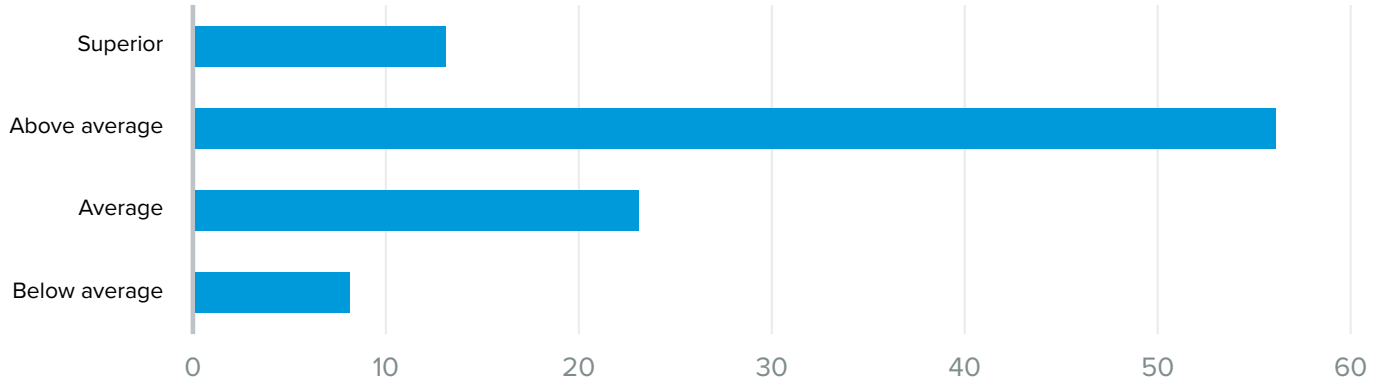
1. Based on your own observations, how do you assess your organization's relative cybersecurity posture in comparison to peers in your sector?

Non-security pros largely believe their organizations have strong security posture: 55% grade it above average or superior. Only 7% label it below average.



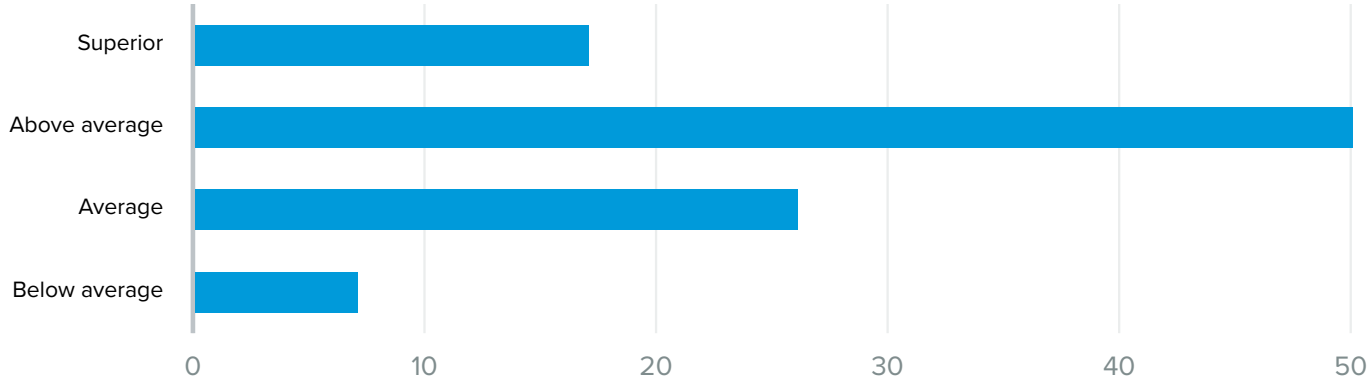
2. If you were to assign a ranking, how would you assess your organization's current cybersecurity awareness efforts in terms of clarity, quality and effectiveness?

Even more than security pros, the non-security crowd feels strongly about the quality of cybersecurity awareness efforts, and 69% say they are above average or superior.



3. Again, if you were to assign a ranking, how would you assess your own degree of cybersecurity awareness as a result of your organization's education efforts?

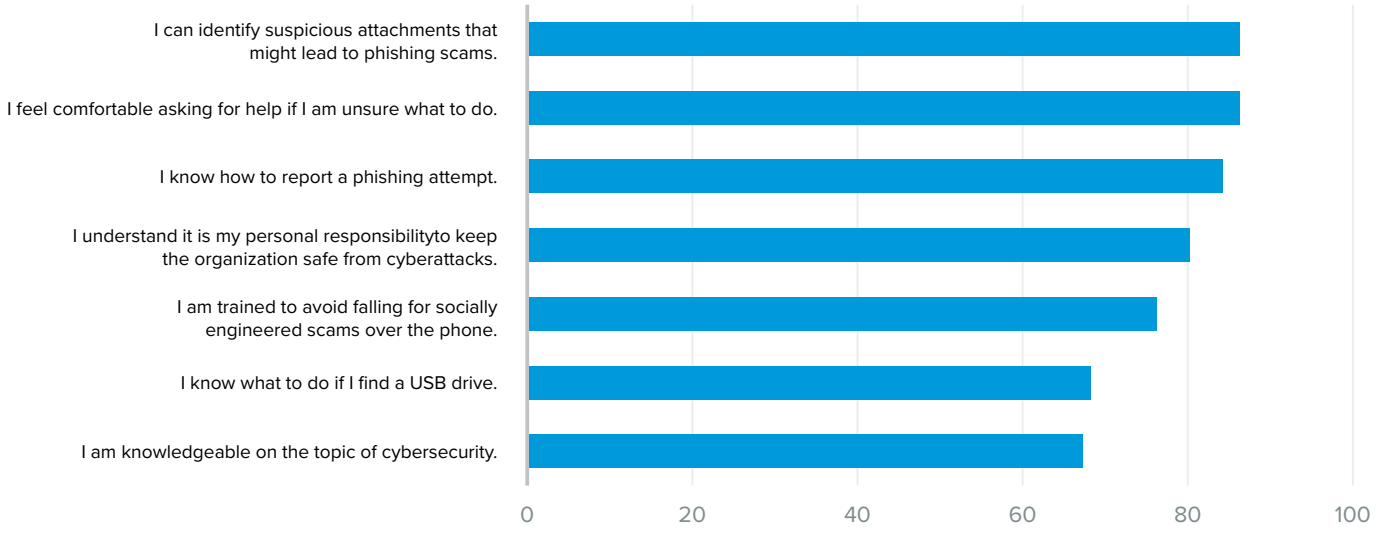
As for their own levels of awareness, 67% of respondents say they are above average or superior. That does leave, though, roughly one-third — 33% — who identity as average or below.



4. What do you believe you personally have gained from your organization's cybersecurity education efforts? (Select all that apply.)

Asked what they have gained from their organizations' awareness efforts, non-security pros offer these top three takeaways:

- I can identify suspicious attachments that might lead to phishing scams — 86%
- I feel comfortable asking for help if I am unsure what to do — 86%
- I know how to report a phishing attempt — 84%

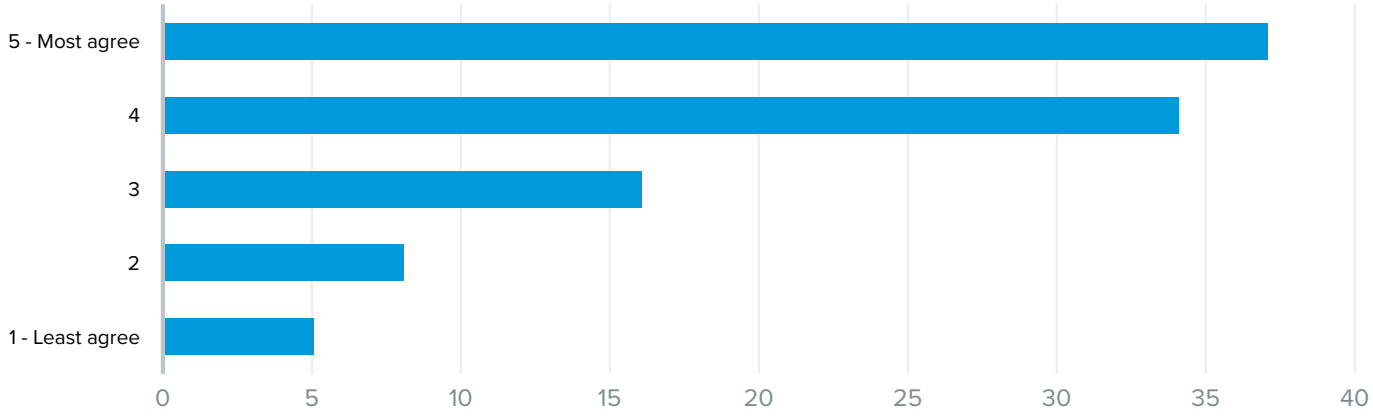


CURRENT AWARENESS PROGRAM

Here, the report delves into specific awareness programs being offered, as well as the frequency and measured success of the training.

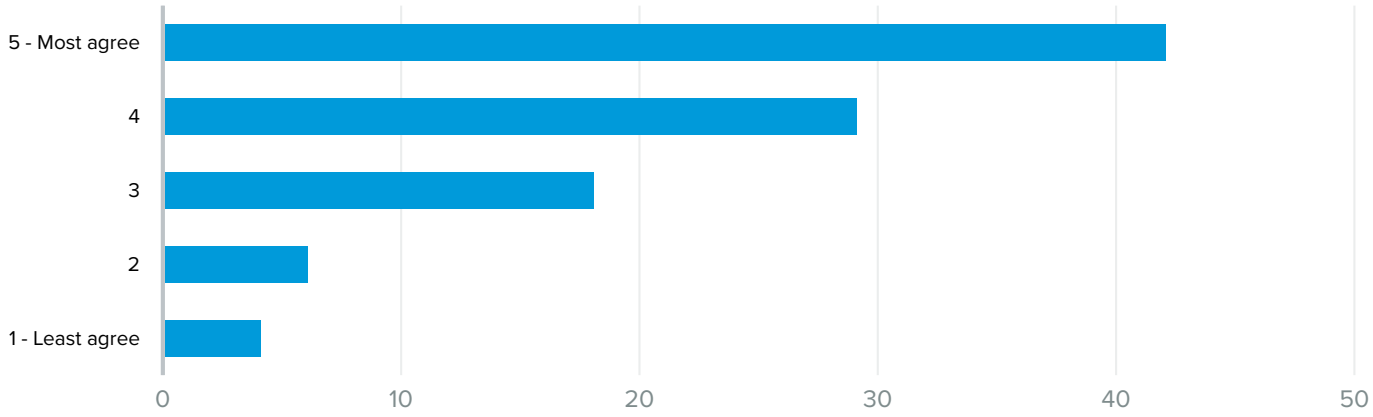
5. On a scale of 1-5 (1 being “least agree,” 5 being “most agree”), do you believe your organization puts sufficient emphasis on the criticality of cybersecurity awareness?

Seventy-one percent of respondents rate their organizations at 4 or 5 in terms of putting sufficient emphasis on the criticality of cybersecurity awareness. Only 5% say they “least agree” with this statement.



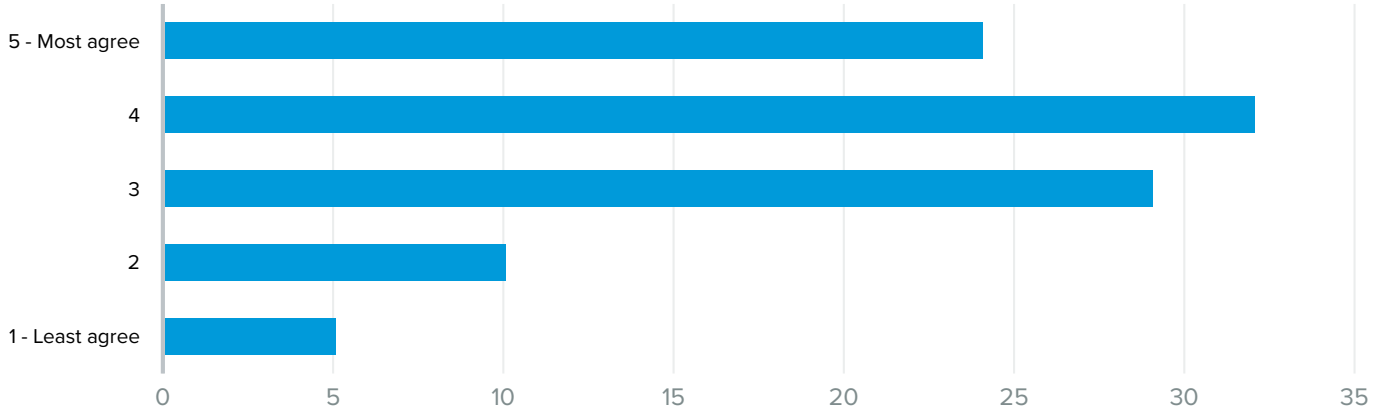
6. On a scale of 1-5 (1 being “least agree,” 5 being “most agree”), do you believe your immediate manager takes the organization’s cybersecurity awareness efforts seriously enough?

Likewise, 71% say their immediate manager is most likely to take these awareness efforts seriously.



7. On a scale of 1-5 (1 being “least agree,” 5 being “most agree”), do you believe your peer employees take the organization’s cybersecurity awareness efforts seriously enough?

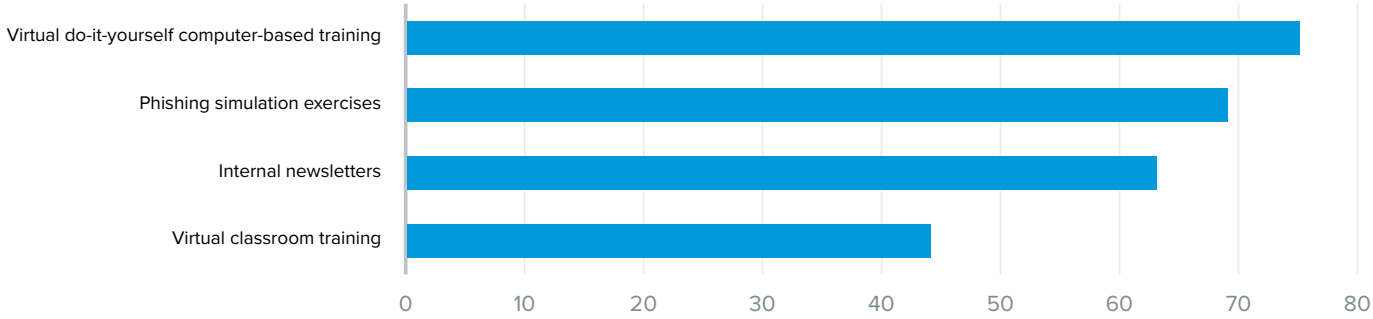
How about peers? Do they take awareness seriously enough? Fifty-six percent of respondents rate this response a 4 or 5 — (“most agree”). But 44% rate it 1 to 3, displaying less confidence.



8. What types of cybersecurity awareness programs does your organization currently offer? (Select all that apply.)

The most common forms of awareness programs identified by this group are:

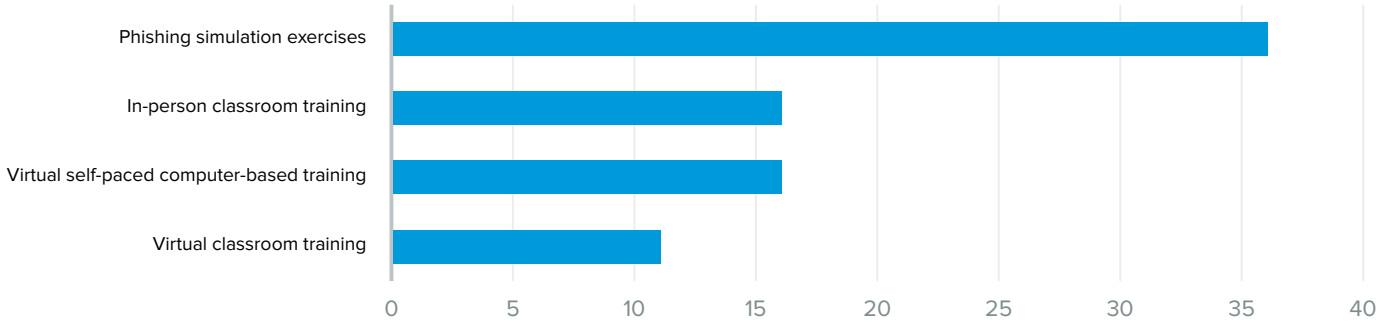
- Virtual self-paced computer-based training — 75%
- Phishing simulation exercises — 69%
- Internal newsletters — 63%



9. Which of these elements do you believe is most successful in reaching the intended audience?

Similar to their security pro counterparts, this group finds these three elements to be most successful in reaching the target audience:

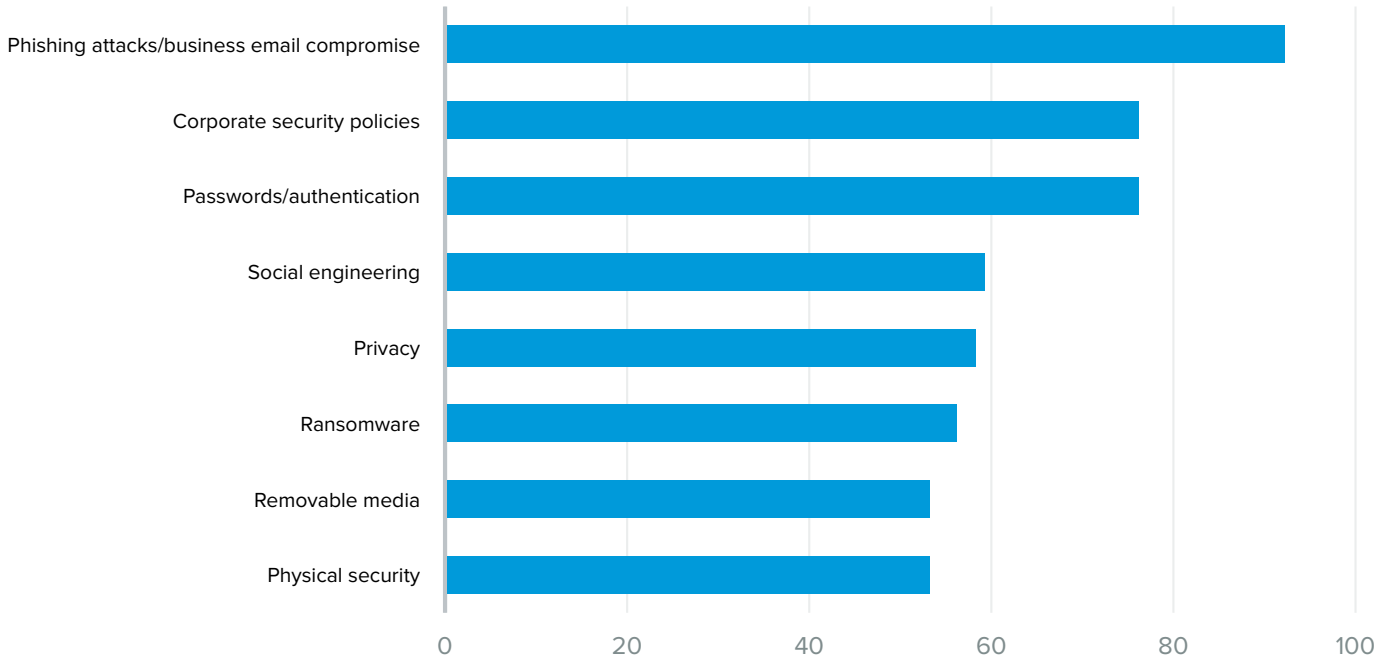
- Phishing simulation exercises — 36%
- In-person classroom training — 16%
- Virtual self-paced computer-based training — 16%



10. What topics typically are covered in your cybersecurity awareness programs? (Select all that apply.)

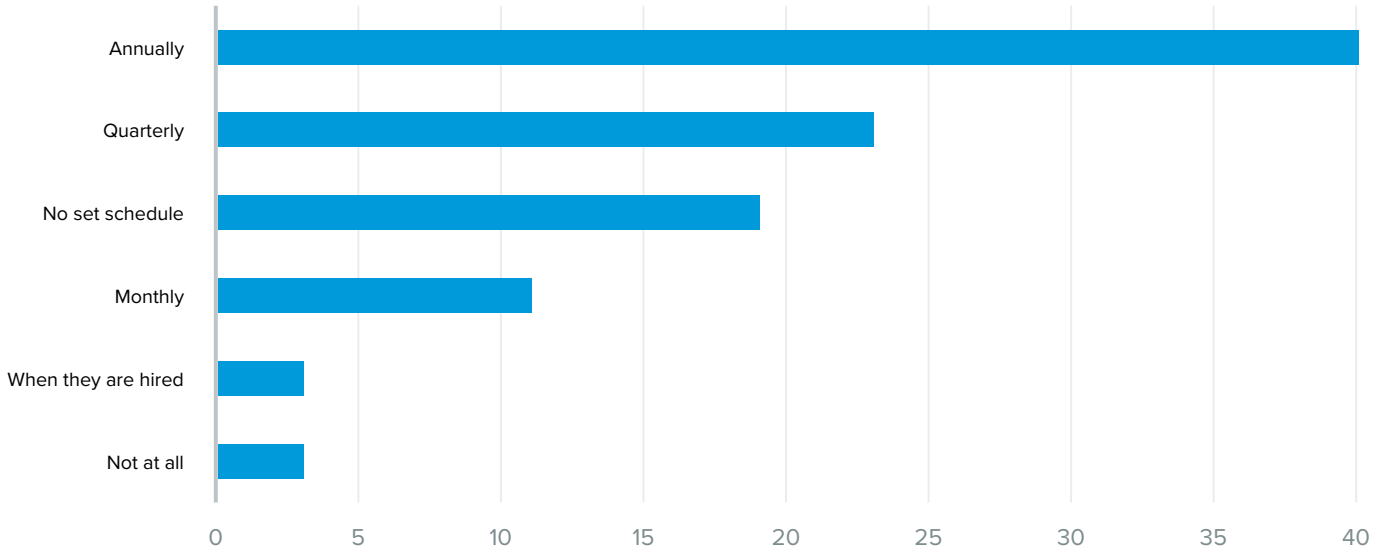
The top three topics covered in awareness programs are:

- Phishing attacks/BEC — 92%
- Corporate security policies — 76%
- Passwords/authentication — 76%



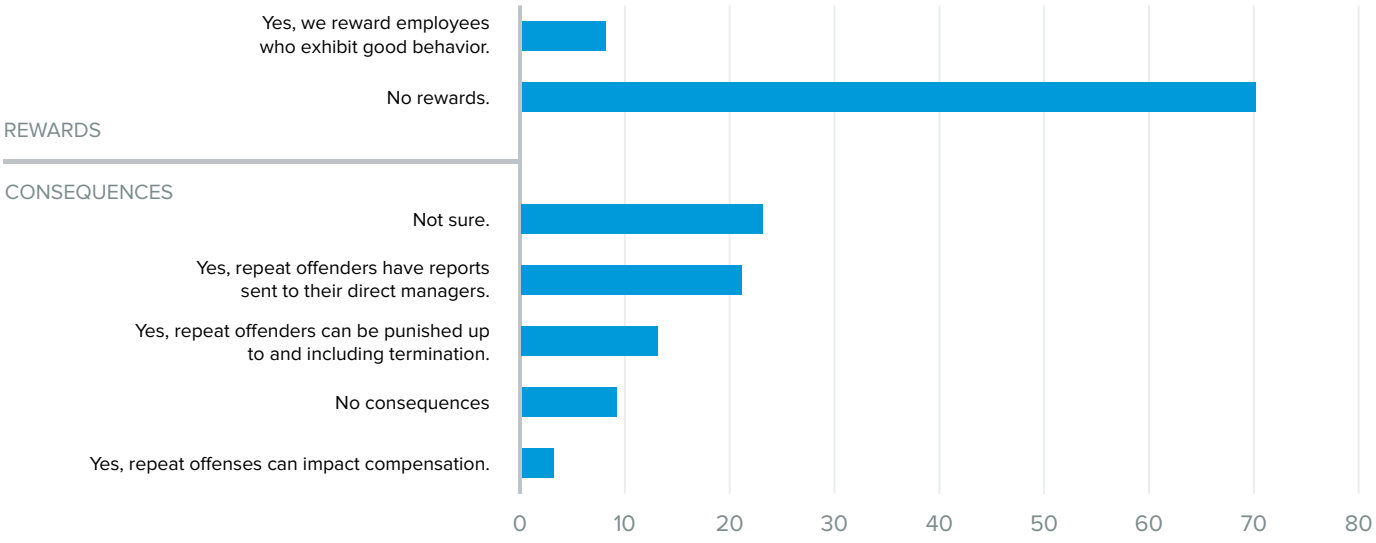
11. How frequently do employees receive cybersecurity awareness training?

Forty percent of non-security pros say awareness programs are offered only annually, while 23% say they are offered on a quarterly basis, and 19% say there is no set frequency.



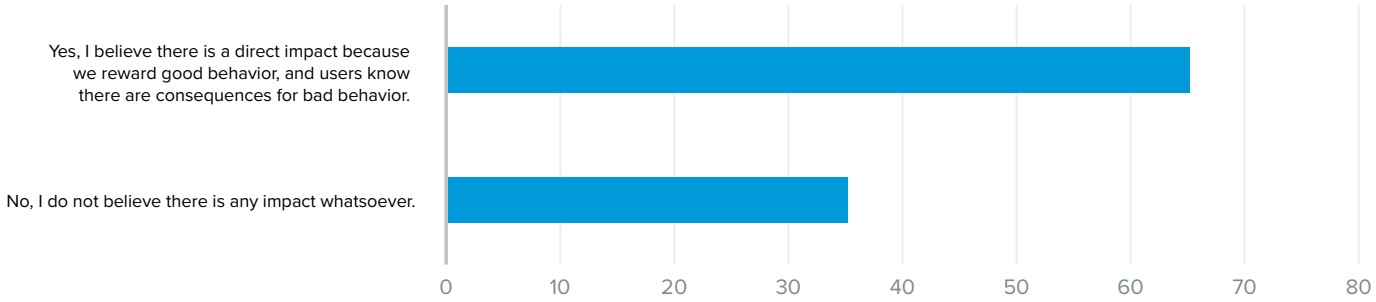
12. Are there rewards for employees who report security incidents and/or consequences for employees who continually commit security errors even after undergoing training? (Select all that apply.)

Seventy percent say no rewards are offered for employees who report security incidents, and 21% say repeat offenders have reports sent to their direct managers.



13. Do you believe the carrot/stick approach enhances the success of your cybersecurity awareness programs? (Select all that apply.)

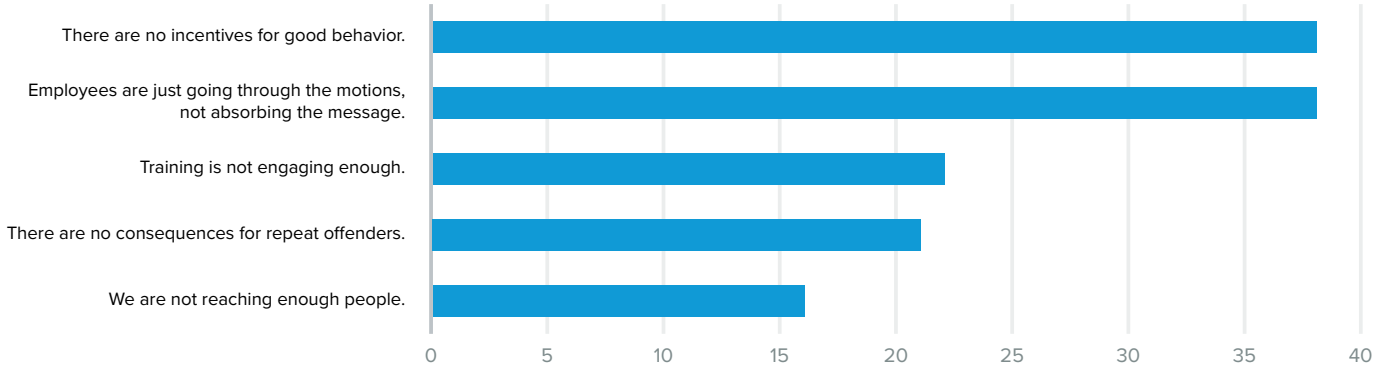
Should there be rewards and consequences? Sixty-five percent of respondents believe the carrot/stick approach enhances the success of cybersecurity awareness programs.



14. What do you deem to be the biggest gaps in your organization's current cybersecurity awareness efforts? (Select all that apply.)

The top three perceived gaps in current awareness efforts are:

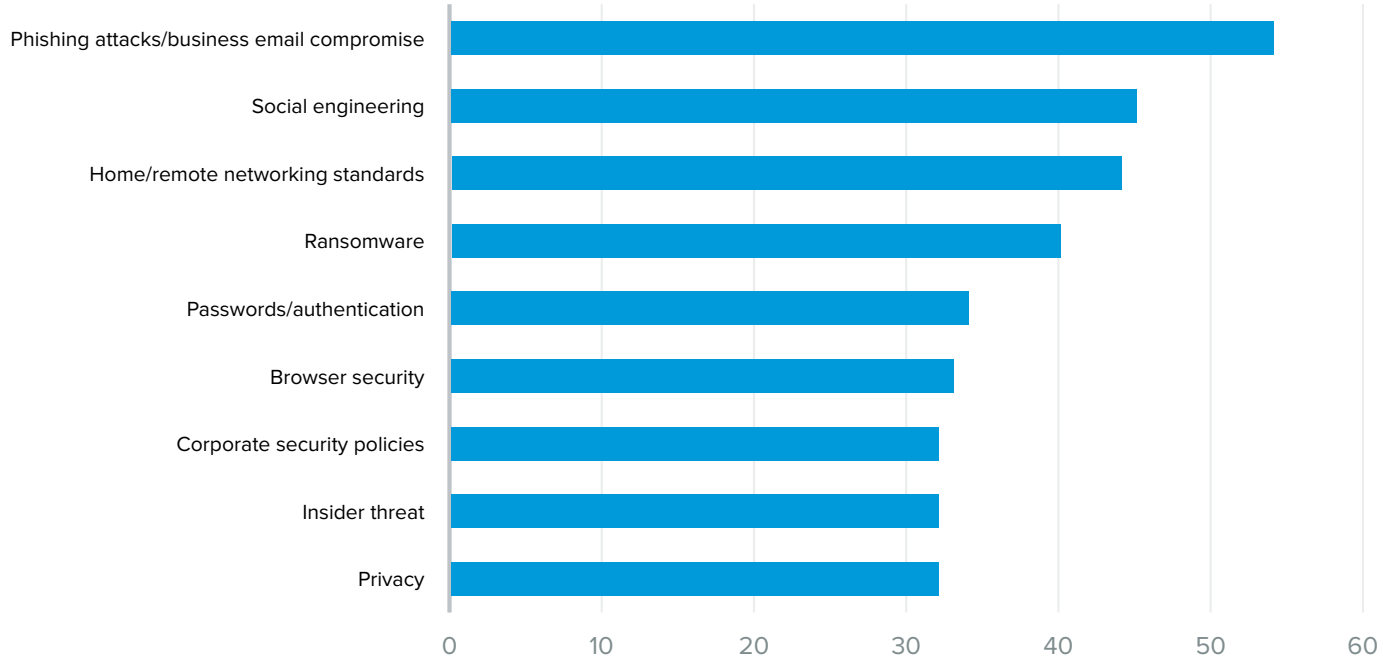
- Employees are just going through the motions — 38%
- There are no incentives for good behavior — 38%
- Training is not engaging enough — 22%



15. Which topic(s) should get greater attention in 2023? (Select all that apply.)

These are the top three topics deemed most important to address in 2023:

- Phishing attacks/business email compromise — 54%
- Social engineering — 45%
- Home/remote networking standards — 44%



CONCLUSIONS

In concluding this survey report, it is useful to return to some of the opening statistics shared:

- Security pros:
  - 56% say their enterprise's cybersecurity awareness efforts are above average or superior.
  - 64% say there are no incentives for good cybersecurity behavior.
- Non-security pros:
  - 67% say their own awareness is above average or superior.
  - 38% say "Employees are just going through the motions" when it comes to training.

The message is clear that even when there is agreement on the high quality of cybersecurity posture and awareness training, there are gaps that need to be addressed. These gaps include:

- Frequency of awareness training — A majority of security pros and rank-and-file employees say it is given only annually.
- Type of training — Security pros favor in-house newsletters, but non-security pros show no interest in them.
- Topics — Phishing/BEC training is good, but non-security pros also want guidance on how to secure their home networks.
- Rewards/Consequences — Security pros and non-security pros disagreed on consequences. But they both agreed rewards motivate good behavior.

With these points in mind, the report draws the following conclusions.

NO MATTER HOW WELL YOU DELIVER AWARENESS, DO MORE

Security and non-security pros alike may agree that current cybersecurity awareness programs are strong and result in bolstering a strong enterprise cybersecurity posture. But they also agree that the majority of current programs are delivered only annually. That is nowhere near frequent enough. As fast as the threat landscape evolves today, and with the critical role end users play in defense, awareness training must be constant. As Sara Pan, team manager of product marketing at Proofpoint, says in the analysis that follows: ***"Seventy-five percent of organizations have less***

than two hours per year to train their users. So within limited time, you want to provide short trainings but do it more frequently. And rather than do it annually, you want to try to educate them at least on a quarterly basis."

WHATEVER YOU'RE DOING NOW, DO IT BETTER

Annual training webinars and occasional newsletters may have been sufficient in a previous generation, but a more effective security awareness program should incorporate various mediums to reach end users. Newsletters do not even register with these users. Security pros need to be in synch with users' needs and get immediate feedback on what works and what still needs work in awareness programs.

MAKE THE PROGRAMMING CURRENT

Phishing and BEC are huge topics and always relevant. But in an age where the hybrid workforce is the rule, not the exception, awareness programs need to shift and start talking about home/remote networking standards. Help users secure their workspaces. Then give them additional training in defending against ransomware and other socially engineered attacks that now focus on "divide and conquer" with the remote workforce.

INCENTIVIZE GOOD BEHAVIOR AND REMEDIATE BAD

A common theme from both sets of respondents: There are no incentives for good cybersecurity behavior, and there are not enough consequences for repeat offenders who ignore the principles of awareness training. Some enterprises do send reports to direct managers when there are repeat offenses, and others even tie cybersecurity behavior to salary and bonus programs. Another approach favored by many enterprises and highlighted by Proofpoint's Pan: Build a network of cybersecurity champions. ***"A lot of times what we hear from security professionals is that they have limited resources and the team is pretty lean,"*** she says. ***"So you want to gather your allies, build a champion network, leverage people who can help you get the word out, and get executive sponsors and buy-in from your leadership team to make your security awareness program more successful and get more attention from your general employees."***

To Proofpoint, it comes down to ACE: Assess, Change behavior, and Evaluate. ***"You have to establish a baseline by finding out what your users know, what they will do when they're faced with potential threats, and what they believe and how they feel about the security program,"*** Pan says. ***"We utilize threat intelligence to help our customers identify vulnerable users and the most attacked users."***

Ultimately, Pan says, ***"Timely education is considered one of the best ways to improve learners' learning effectiveness, and then reinforce that positive behavior. When your end users report suspicious email, let them know that they're doing the right thing by proactively keeping the organization safe."***

To learn more about how to put these survey findings to work, please read the Expert Analysis that concludes this report.

EXPERT ANALYSIS

SARA PAN

2023 SECURITY AWARENESS STUDY

Executive Insights on What Survey Results Mean – and How to Put Them to Work

NOTE: ISMG's Anna Delaney discussed the survey results with Sara Pan, team manager of product marketing at Proofpoint. This is an excerpt of that conversation.

SURVEY GOALS

ANNA DELANEY: What were your goals in conducting this survey?

SARA PAN: To uncover any gaps between security professionals and general employees regarding how they perceive a security awareness program. Before we went into this survey, we made some assumptions and we were trying to validate them. For example, we assumed that average employees do not perceive security awareness the same way as security professionals think they do. Another assumption was that the objectives of a security awareness program are not always aligned with how the program is perceived by general employees. The goal was to help organizations and security professionals identify those discrepancies so they can better assess and modify their current program.

"We assume that average employees do not perceive security awareness the same way as security professionals think they do."

"People will forget 90% of the things that they learned after seven days."

UNDERSTANDING NON-SECURITY PROFESSIONALS

DELANEY: Why have you surveyed non-security professionals as well as security professionals?

PAN: We talk to security professionals all the time, and we're trying to understand their pain points and talk about the solutions. And when we say "our customers," it's really the security professionals. But *nonsecurity* professionals are the *consumers* of your security awareness program. So if you want to improve your security awareness program, you need to understand their pain points, like how you can keep them engaged, or what needs to be modified. So it's important to also learn about how your general employees feel about security and what they believe about your current security awareness program.

KEY FINDINGS

DELANEY: Which findings stood out or even surprised you?

PAN: Quite a few things jump out. The thing that surprised me the most is the mixed signals that we're getting from the security professionals survey. There is an interesting data point: While 78% say that they are meeting or exceeding objectives, 57% say the training was done annually. Now, talking to a lot of security awareness practitioners, most of these security professionals understand that annual training is not enough because there's the forgetting curve. People will forget 90% of the things that they learned after seven days. So you have to provide frequent training or education in order for your security awareness program to be effective.

But the fact that a majority is saying that they are meeting or exceeding objectives while 57% say the training was only done annually tells us either they set the bar low or they believe annual training is sufficient. But either way, that's alerting.

And even though nearly 80% say that they're exceeding objectives, only 56% say that their awareness training efforts are a contributing factor to their security posture. So what does that tell us? That implies that they don't see their security awareness program can make an impact on the overall security posture.

Also, we see some consistent results between security professionals and general employees. They both agree that there are no incentives for positive behavior. When we're talking to security professionals, we know that not every organization has the resources to provide a rewards system. They feel like there's no budget and no way to incentivize their employees. And employees see that. Also, employees are just going through the motions, and both security professionals and employees themselves see that.

"You always have to come back and evaluate your program to continue to identify if there are other gaps that you need to address, what works and what needs to be changed, and to track behavioral metrics that help you understand what users know."

MOST EFFECTIVE TYPES OF TRAINING

DELANEY: What are the most effective types of training?

PAN: Organizations need to take a holistic approach. You need to start from knowing the current gaps of your program and understanding your users' vulnerabilities and knowledge gaps. And then once you identify those gaps, identify who your vulnerable users are.

The next thing is how you change their behavior. One of the challenges for organizations is that people are always fighting for end users' attention. Security awareness practitioners are always thinking about how to keep users engaged and the most effective way to convey a certain concept. Use just-in-time education or provide some contextual nudges. Keep it interactive and do it more frequently. Ultimately, that's how you can build a strong security culture that not only helps protect your own organization, but at the same time motivates your users to help secure the organization as well.

Last but not least, you always have to come back and evaluate your program. Continue to identify if there are other gaps that you need to address, what works and what needs to be changed and track behavioral metrics that help you understand what users know and evaluate what they will do when they're faced with real-world threats.

TRAINING FREQUENCY

DELANEY: You mentioned that training should be administered more frequently. How and when should it be administered?

PAN: As a security professional, we want to do it more frequently, but there are some challenges. Seventy-five percent of the organizations have less than two hours per year to train their users. So within limited time, you want to provide short trainings but do it more frequently. Rather than do it annually, you want to try to educate them at least on a quarterly basis.

"Seventy-five percent of organizations have less than two hours per year to train their users."

"If you want to take a step further, think about building a security champion network."

MORE EFFECTIVE TRAINING

DELANEY: What can and should security pros learn from what non-security professionals are telling them?

PAN: While phishing and BEC or ransomware are already the most covered topics based on the survey, employees are requesting more information. And many security professionals rely on newsletters to communicate security initiatives to employees. But interesting finding: None of the employees consider newsletters effective.

AWARENESS TRAINING IN 2023

DELANEY: What else can be done to make 2023 better than 2022 in terms of awareness training?

PAN: More frequent communication provides the way to get feedback from employees. It has to be two-way communication. You have to provide a platform or even a network tool to gather feedback from your employees — something interactive. In the old days, when people came into the office, organizations put up posters and webinars, inviting security professionals and authorities to come and present information about the current threat landscape, plus newsletters, in-person education — taking full advantage of multiple mediums. The industry started to talk about how to build a strong security culture.

If you want to take a step further, think about building a security champion network. What we hear from security professionals is that they have limited resources and the team is pretty lean. So you want to gather your allies, build a champion network, leverage people who can help you get the word out, and get executive sponsors and buy-ins from your leadership team to make your security awareness program more successful and get more attention from your general employees.

THE PROOFPOINT APPROACH

DELANEY: What is Proofpoint doing to address these challenges with its customers?

PAN: Proofpoint provides a holistic approach to security awareness education. We have a framework called ACE. A stands for "assess," C stands for "change behavior," and E stands for "evaluate." You have to establish a baseline by finding out what your users know, what they will do when they're faced with potential threats, and what they believe and how they feel about the security program. We utilize threat intelligence to help our customers identify vulnerable users and the most attacked users.

From there, we try to change those unsafe behaviors by providing just-in-time education. Timely education is considered one of the most effective ways to improve learners' learning effectiveness, then reinforce that positive behavior and how you engage with your employees, and let them know that this is the behavior that you love to see from them. When your end

users report suspicious email, let them know that they're doing the right thing by proactively keeping the organization safe.

Last but not least, evaluate your program. If you want to see the impact of your program, go beyond tracking the completion rate or the click rate of phishing simulation. Start tracking some behavioral metrics, such as reporting rate, and then the reported email accuracy rate. Is your user reporting random spam or questionable email — or do they even have the ability to identify potential risk or email accuracy rate? Those are the things that Proofpoint can do to help security professionals address security awareness.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center Princeton, NJ 08540 www.ismg.io