ThriveDX

Lucy
Powered by ThriveDX

2022 Global Cybersecurity Awareness Training Study

Research and findings based on data collected by Lucy Security in collaboration with ThriveDX

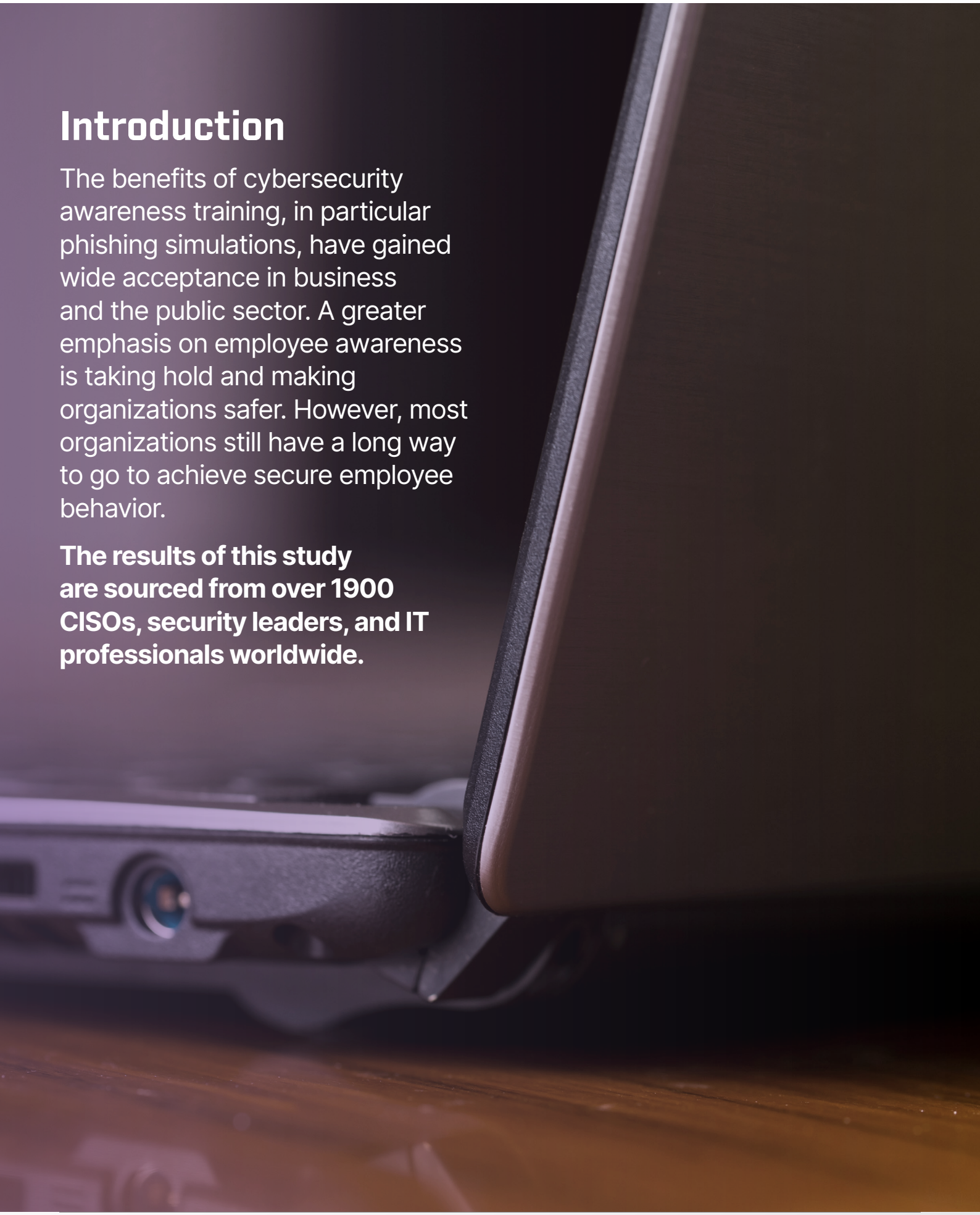
August 2022

Table of Contents

Introduction

The benefits of cybersecurity awareness training, in particular phishing simulations, have gained wide acceptance in business and the public sector. A greater emphasis on employee awareness is taking hold and making organizations safer. However, most organizations still have a long way to go to achieve secure employee behavior.

The results of this study are sourced from over 1900 CISOs, security leaders, and IT professionals worldwide.



97% of respondents are convinced that cybersecurity awareness training leads to greater corporate security

The “human factor” remains in the crosshairs of cybercriminals, with 91% of successful attacks starting with a lack of employee understanding or awareness. Unfortunately, this figure has hardly changed over the last few years, even though the majority of medium-to-large-sized organizations have now adapted security awareness training measures.

Today, IT security systems and hardware are without a doubt part of the basic equipment of every organization, regardless of size. Based on this foundation, successful cybersecurity awareness focuses on the general protection of the company against the damages of cybercrime. It also provides employees with tools, such as the ability to report suspicious emails and have them analyzed. This study shows that properly implemented awareness training programs make a company significantly more secure. As many as 87% of the study participants stated that without employee training, effective IT security is not possible.

The first Cybersecurity Awareness Training Study in 2020 found that cybersecurity awareness has more benefits than just better trained employees or fewer security incidents. This year's report confirms that the impact of cybersecurity awareness is more diverse and goes further than expected. Whats more is that 97% of respondents claim to be convinced that cybersecurity awareness training leads to greater corporate security, 54% of those respondents saying the impact on security was significant.

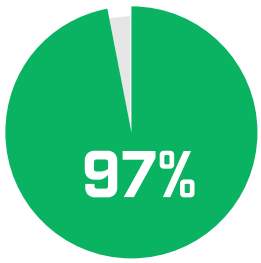
When it comes to challenges, the technical environment is rather immune. Instead, first and second among the challenges are user acceptance and resource scarcity. Ensuring the ongoing operation of an awareness program comes in third. Further, it can be seen that the implementation of cybersecurity awareness continues to pose increased challenges to leadership and is an innovation task. The goal remains to achieve secure behavior among the workforce.

One of the most common challenges a CISO faces is ensuring a training program is properly implemented. However, awareness concepts that are more autonomous should be taken and standardization should be taken with caution here. The security awareness industry sometimes tries to present cybersecurity awareness as a simple problem. However, the data of this study shows that individualization, specific company context, and personalization are the most important success factors of employee awareness training measures.

Since cybersecurity awareness measures are part of the everyday work within many companies and are carried out on an ongoing basis, smart and entertaining implementation is also highly relevant. If the phishing simulations are too clumsy or too simple, or if the training modules are not engaging and lack variation, then employee sensitization falls by the wayside and the security of the company suffers.

Key Results 2022

Reaching the state of adolescence



97% of the organizations surveyed have implemented cybersecurity awareness measures

Almost all of the organizations surveyed have implemented cybersecurity awareness measures (97%). In doing so, the use of phishing simulations has caught up with the use of awareness training (both are now at 88%). Fifty-eight percent of the companies now have awareness policies in place and only 42% of the companies surveyed use a "phishing button".

These results are not surprising considering the target group of more than 1,900 IT security professionals globally. It is worth noting, however, that not even half of the organizations involve their employees in their security arrangements. Only 42% of the companies have a Phishing Incident Button in use. Such a button activates the “human firewall” and gives the insecure employee a simple but powerful tool that offers great support in the daily handling of emails. Just as importantly, the security department benefits from the accelerated reporting and analysis of suspicious emails that comes with the implementation of a phishing button.

Awareness measures among staff clearly increase corporate security: 96% stated that awareness measures have been increased and as many as 97% of those surveyed stated that IT security has been improved as a result. On the same note, 87% of the study participants stated that the security level cannot be maintained if only technical security measures are implemented without security awareness.

There is an increased maturity of awareness programs: the use of mission statements, policies, guidelines, metrics, and systematic training show a higher degree of institutionalization. Fifty-eight percent of respondents now have some form of regulations for security awareness in place. Furthermore, 65% believe their cybersecurity awareness training programs need to be expanded, and no one indicated a desire to reduce the level of awareness.

Once the awareness program is in place, a large majority of respondents (72%) said they refrain from pre-announcing a phishing campaign. Unfortunately, only 20% of participants conduct more than seven simulations per year and 67% invest up to 12 hours / year in awareness training, which is in line with the "people-centered" approach.

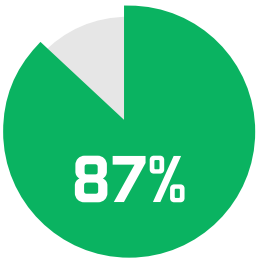
Currently, the most popular training topics are courses on phishing and malware, password security, email security, social engineering, and ransomware.

The results of employee awareness efforts are impressive: Better awareness (19%), greater vigilance (14%), strengthened human firewall (12%), and increased corporate security (9%) are cited as the greatest benefits.

In order to achieve this, the most important success factors were course duration (21.2%), entertaining nature of the training courses (19.2%), and customization of the courses (13%). For phishing simulations, the most important success factors were contextualization (30.9%), customization (23%), recognizability (15.1%), realism (12.9%), and individualization (11.5%).

No topic is without challenges. The biggest challenges cited in implementing an awareness program are achieving user acceptance (25%), workload and resources (22%), and program execution (14%).

Furthermore, for the second time, cybersecurity awareness training has been shown to deliver benefits beyond IT security: 99% of respondents indicated that security awareness has a positive impact on the company's error culture. Further, 96% noted a positive influence on the working atmosphere. It can be concluded from these results that there is a very high level of acceptance for security awareness training among employees in the surveyed companies, even though achieving user acceptance was cited as one of the greatest challenges in implementing an awareness program.



87% of the participants state that corporate security cannot be maintained if only technology is used.

Greatest benefits of employee awareness efforts:

19%
BETTER AWARENESS

14%
GREATER VIGILANCE

12%
STRENGTHENED HUMAN FIREWALL

Summary of Key Results

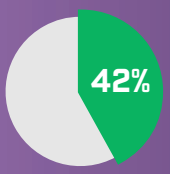
2022 Global ThriveDX Cybersecurity Awareness Study

97% implement cybersecurity awareness measures

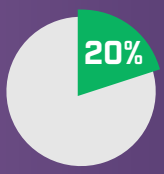
72% of participants do not inform in advance about a phishing simulation

87% of the participants state that the level of safety cannot be maintained by relying only on technology

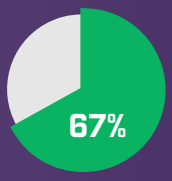
99% recognize a positive influence on the culture of errors in the company



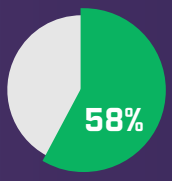
42% offer their employees a "phishing button"



20% do more than 7 simulations per year



67% invest up to 12 hours in awareness training



58% have a cybersecurity awareness policy in place

65% of participants want to expand their awareness measure

96% of the participants indicate a neutral to strongly positive influence on the working atmosphere

Source: 2022 TDX Global Cybersecurity Awareness Study

Summary
2022 Global ThriveDX Cybersecurity Awareness Study

Cybersecurity awareness has increased significantly in the last year (96%) and has led to a higher level of security in companies (97%)

Still, **65%** believe cybersecurity awareness programs need to expand. **87%** agreed that advancement cannot be based on technology alone, but must also focus on people

Increased maturity of cybersecurity awareness programs: mission statements, policies, metrics, and systematic training show higher levels of institutionalization. **58%** now have an awareness policy

67% invest up to 12 hours in awareness training, consistent with the "focus on people" approach

Phishing, malware, social engineering, ransomware, password security and email security are the most important topics covered

A large majority (72%) do not announce phishing simulations in advance. Only 20% conduct more than 7 simulations per year

The biggest benefits of cybersecurity awareness:

- Higher awareness (19%)
- Vigilance (14%)
- A strong(er) human firewall (12%)
- Increased security (9%)

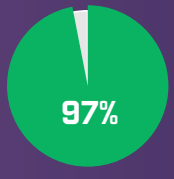
Significant challenges include:

- User acceptance (25%)
- Workload and resources (22%)
- Program execution (14%)

99% see a somewhat to strongly positive impact of cybersecurity awareness on error culture. The same (96%) see a neutral to strongly positive influence on the working climate

42% provide their employees with a "phishing button" for reporting and analysis

Program duration (21.2%), entertainability (19.2%), and personalization (13%) are the most important success factors for training modules

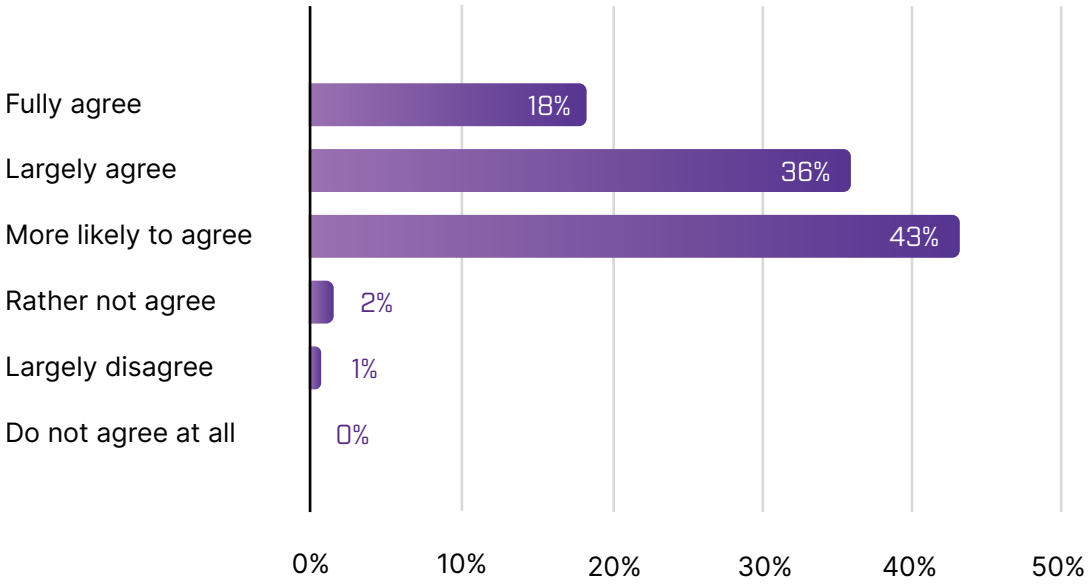


97% of respondents are convinced that cybersecurity awareness training leads to greater corporate security

Results in Detail

The results of the survey indicate that there's a need to go beyond awareness in end-user security training.

The Security Awareness Training Led To Increased Security In Our Organization

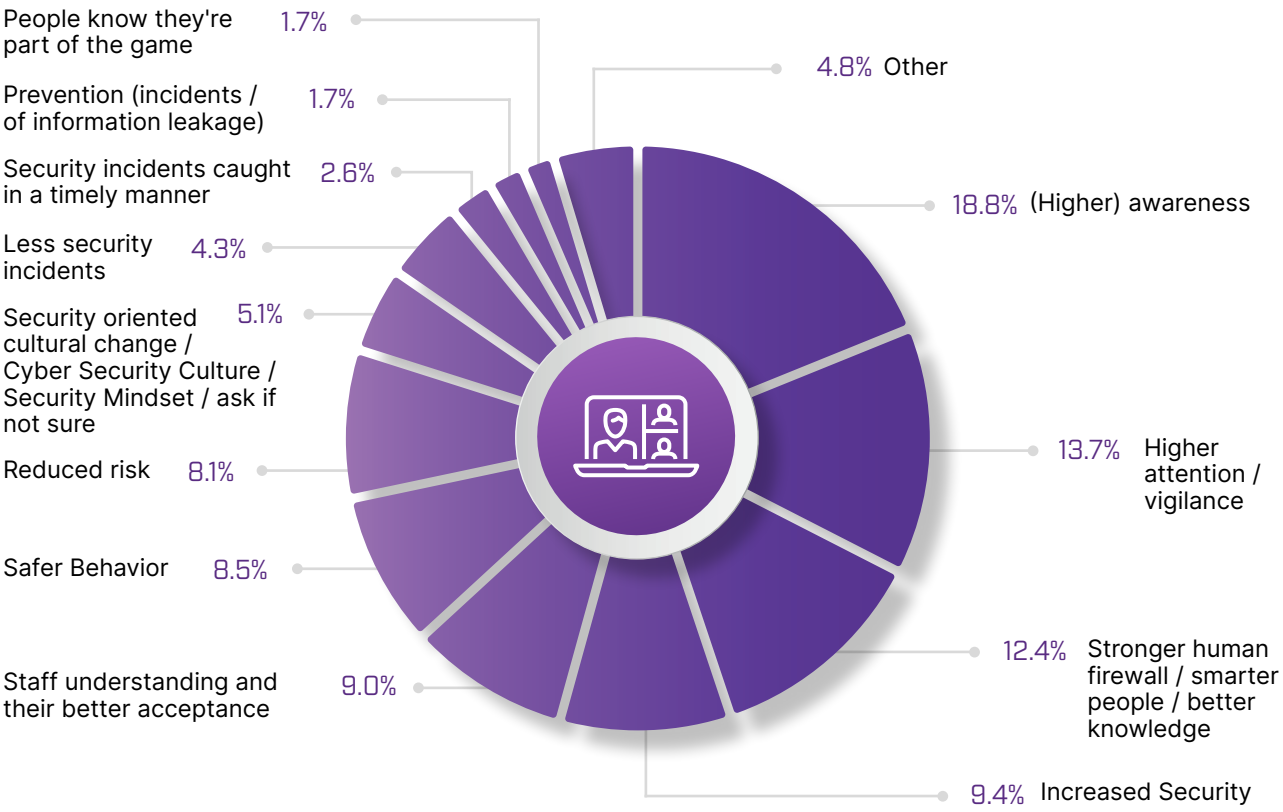


97% of respondents are convinced that cybersecurity awareness leads to greater corporate security. Well over half of the respondents (54%) stated that awareness had even significantly increased corporate security.

SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

Benefits of Cybersecurity Awareness Training

Benefits To The Organization Due to Cyber Security Awareness Training



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

ANALYSIS

Multiple answers were possible. As expected, the evaluation of the free responses revealed consistencies in various statements. The top benefit was clearly attributed to the employee. The most frequently mentioned benefits were:

1. Higher awareness (18.8%),

2. Greater vigilance (13.7%), and

3. Increased human firewall (12.4%), all clearly relate to the user.

The top three responses regarding benefits combined accounted for 44.9%. Strengthening the human firewall refers to the involvement and commitment of the employee in the company's alert chain in the event of potential security incidents.

Improved overall IT security of the organization was ranked 4th. Employee understanding, safer behavior, and reduced incident risk were cited with similar frequency. The change to a security culture fell at position 8 of the benefits mentioned, with 5.1% of the mentions. This is followed by fewer security incidents with 4.3% of mentions. Next, security incidents caught in a timely manner at 2.6%. After that is incident prevention at 1.7%, and also people know they are part of the game at 1.7%.

Other Benefits

The combined total of the other benefits mentioned is 4.8% of all statements:

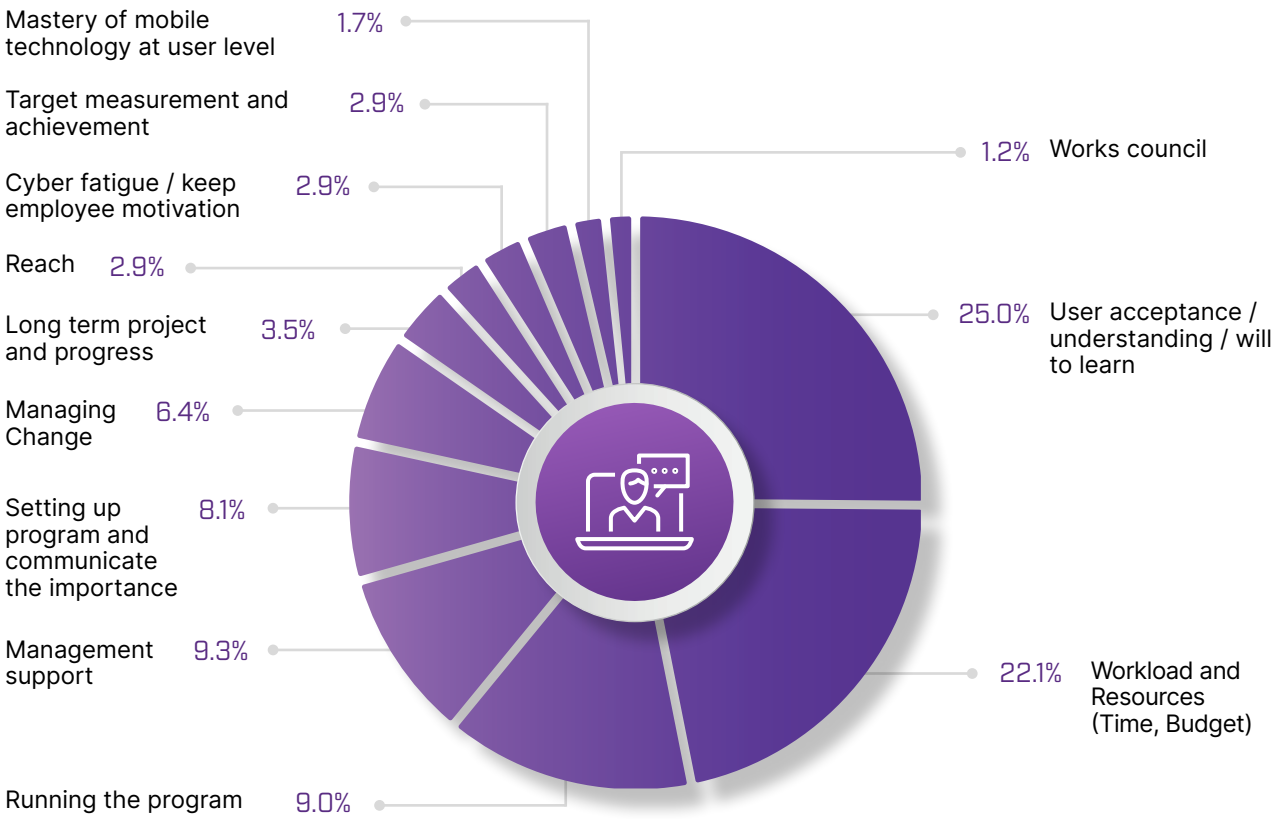
- Private use of what is learned
- Sense of responsibility among employees
- Respect and fair error culture
- Lower costs
- Compliance (with the guidelines)
- Laying the foundation for a functioning Infosec infrastructure, basis for effectiveness, and applicability of technical measures

Study director's note:
With so few mentions of cost, it is reasonable to assume that the financial impact is either unmeasured, difficult to measure, or non-existent.

Challenges in Cybersecurity Awareness

The complexity and multi-dimensionality of the subject matter became readily apparent in the cybersecurity awareness challenges.

Challenges Associated With Cyber Security Awareness Training



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

The six main topic areas received around 85% of the mentions:

1. User acceptance, understanding, and the will to learn received a quarter of the mentions (25%).
2. Scarcity of resources (time, budget, staff) was the second most cited (22.1%).
3. Running the program and keeping it focused, attractive, and effective was the third most cited challenge at 14%.
4. Ensuring management support was fourth, with 9.3%.
5. Setting up and communicating the program was fifth, with more than 8% of nominations.
6. Managing change came in sixth, with 6.4% of mentions.

Other Challenges

Other challenges cited in implementing cybersecurity awareness measures were:

- The long-term nature of the measures and ensuring progress
- Ensuring the reach of the program
- Dealing with cyber fatigue
- The measurement and achievement of goals
- The technology skills of employees, especially in handling mobile devices
- The staff representative / works council

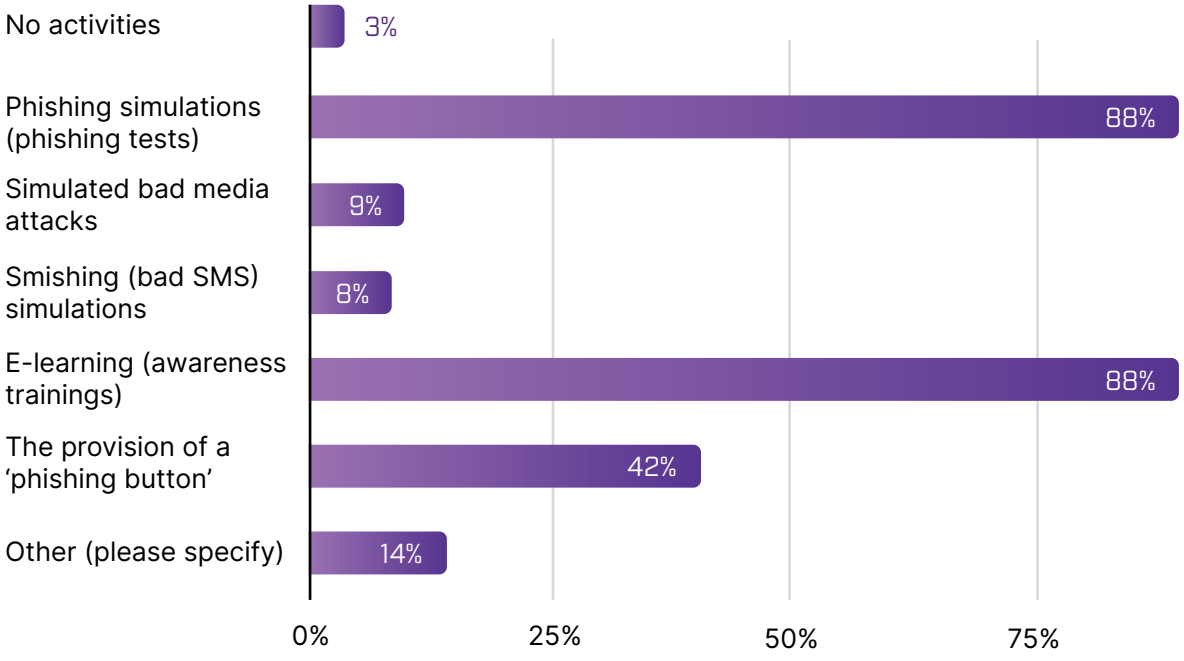
The combined sum of these answers is 15.2% of all statements about the challenges of cybersecurity awareness.

The fact that the works council was mentioned in only 1.2% of the responses suggests that, in most cases, the buy-in of staff representatives is not or is only a minor challenge in the implementation of cybersecurity awareness programs.

Deployment of Cybersecurity Awareness Programs

- Awareness as a whole has increased. In addition to traditional training, phishing simulation has become an accepted tool for increasing employee awareness.
- There is an advanced maturity of cybersecurity awareness in the market. However, significant weaknesses in implementation are also evident. Fifty-eight percent of organizations now have awareness regulations in place.
- ISO27001 as a standard was mentioned most frequently.
- The need for cyber risk insurance does not seem to be an overly significant driver for awareness programs.
- Almost two-thirds (65%) of the participants want to expand their awareness programs further in the future.

My Organization Applies the Following Measures to Increase Employee Awareness



Smishing and bad media / USB hack simulations have minimal impact, with less than 10% of respondents using these awareness measures.

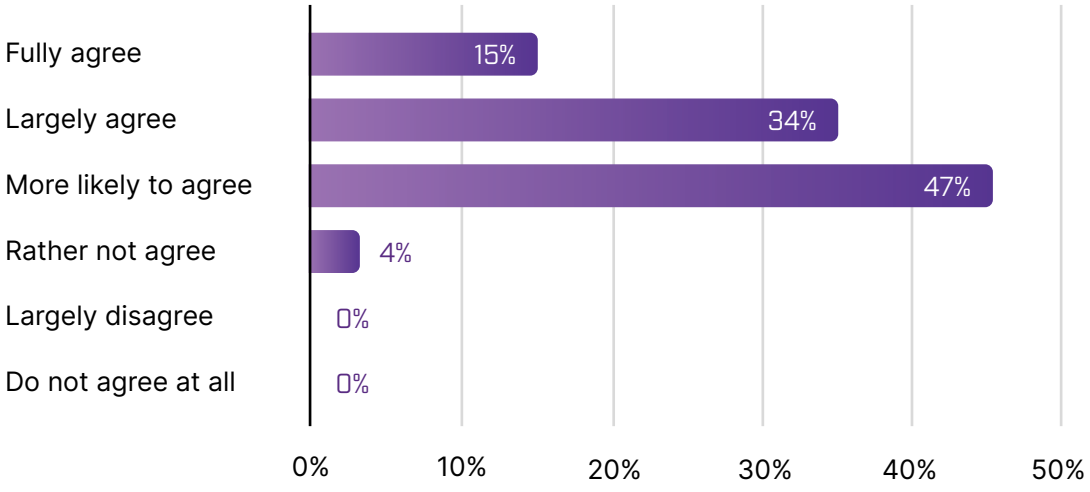
Only 42% of respondents use a phishing button. A lot of protection potential and user motivation is still being wasted here.

SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

Other Elements - Other elements of awareness programs mentioned were:

- Poster
- InfoSec news site / security intranet / newsletter (commenting on public hacks)
- Email banner
- Penetration testing
- Life-hacking / informational cybersecurity demonstrations
- Flag as "unsolicited email" / "external email"
- Set of rules / rules of conduct (guidelines) / guideline / code of conduct
- Topic on the introduction day / New Joiner Onboarding / InfoSec sessions for new employees
- Offline activities and games
- Cybersecurity Culture Survey
- Discussion of practical examples in management meetings
- Team awareness sessions
- Compliance trainings
- Security consultancy for managers

The Cybersecurity Awareness Level Increased Amongst Our Workforce Over The Past Year



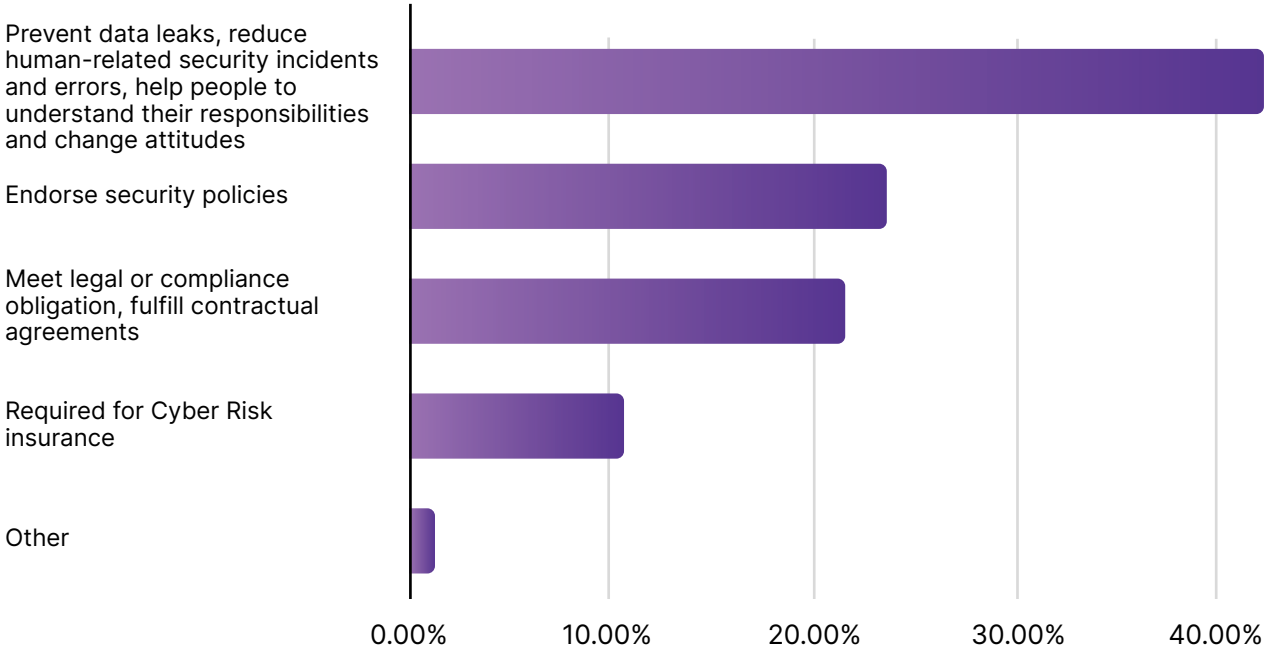
SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

- 96% of all respondents stated that the level of awareness in their organization has increased.
- Only 4% of all respondents stated that the level of awareness has remained the same or has decreased somewhat.

MOTIVATION, NORMATIVE FOUNDATIONS, AND EXPANSION OF AWARENESS PROGRAMS

The main motivation of cybersecurity awareness is still based on the intention to make employees smarter and, thus, companies safer from cyber attacks.

What Was The Main Reason Your Organization Implemented Security Awareness Measures

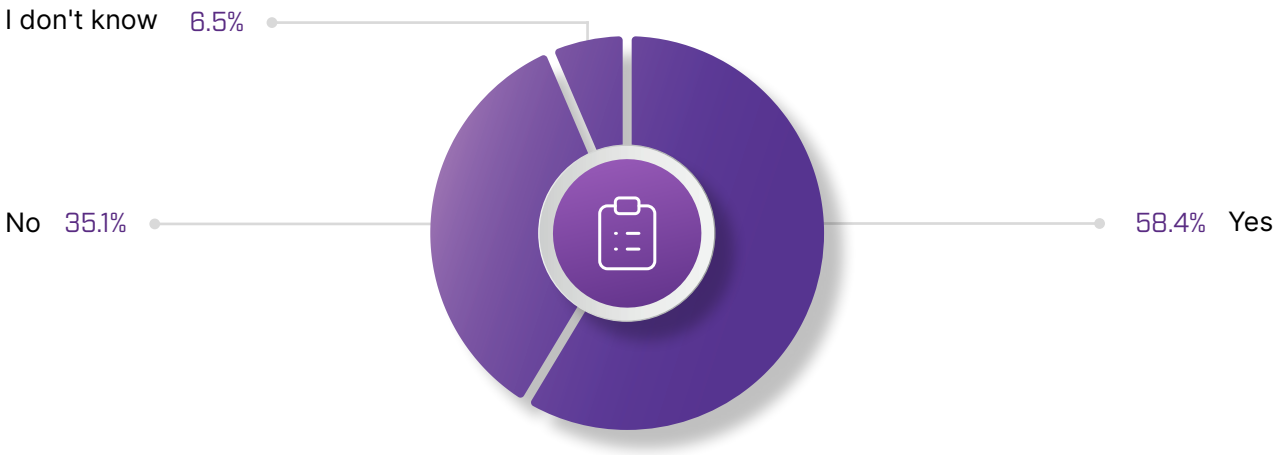


SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

Only 10.6% of the participants stated that awareness activities are necessary for their cyber insurance.

Almost a quarter of the respondents (24%) stated that they have to perform awareness activities due to some standards or legal obligations.

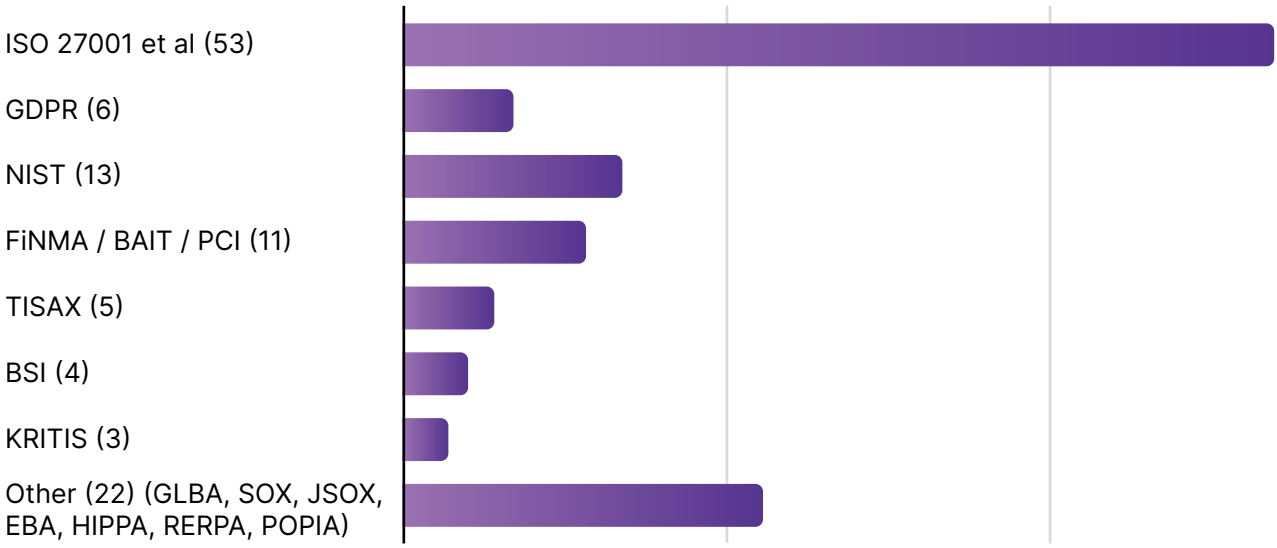
Our Organization Has a Cybersecurity Awareness Mission Statement or Policy



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

Which Regulation(s) Requires Your Compliance

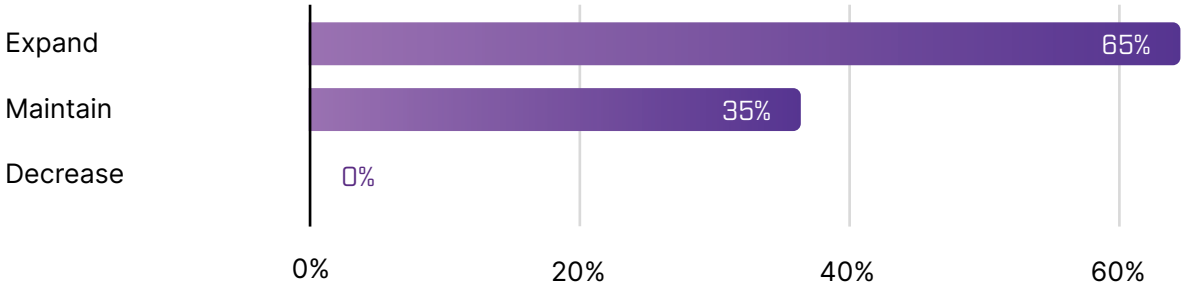
If applicable



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

With regard to guidelines and standards, ISO 27001 is the most widespread. It is also clear that in the financial world regulators specify concrete cybersecurity awareness measures. NIST is the second most frequently mentioned framework (often used in the global financial industry as well, e.g. FINMA is based on NIST). TISAX is a new standard in the automotive industry, which also specifically requires the implementation of Awareness programs.

In The Future We Want Our Cybersecurity Awareness Program To:



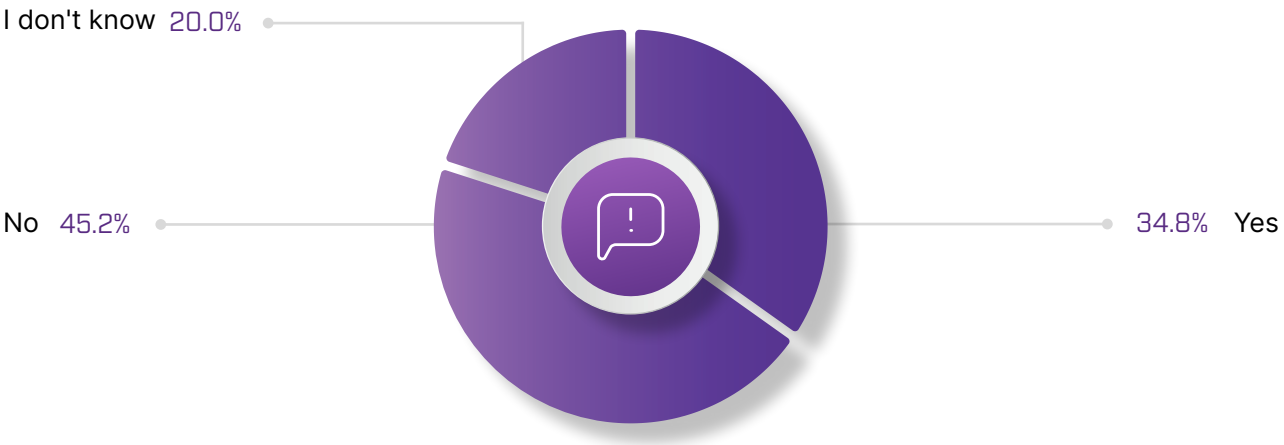
This chart clearly shows that there is still a need to catch up in terms of cybersecurity awareness. Almost two-thirds of the respondents stated that they want to further expand the IT-security domain.

SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

DISCIPLINARY ACTION

Mistakes made do not often have consequences for the employee. About two thirds of the participants (45.2% No and 20% Don't know) said they refrain from holding their employees accountable for mistakes made when using computers and the internet. The participants who answered “yes” to this question are mainly from the security, financial, and manufacturing industries.

Security Incidents Unintentionally Caused By Employees Can Have Disciplinary Actions



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

Almost two-thirds of the participants (65%) send 2-5 phishing simulation emails per year

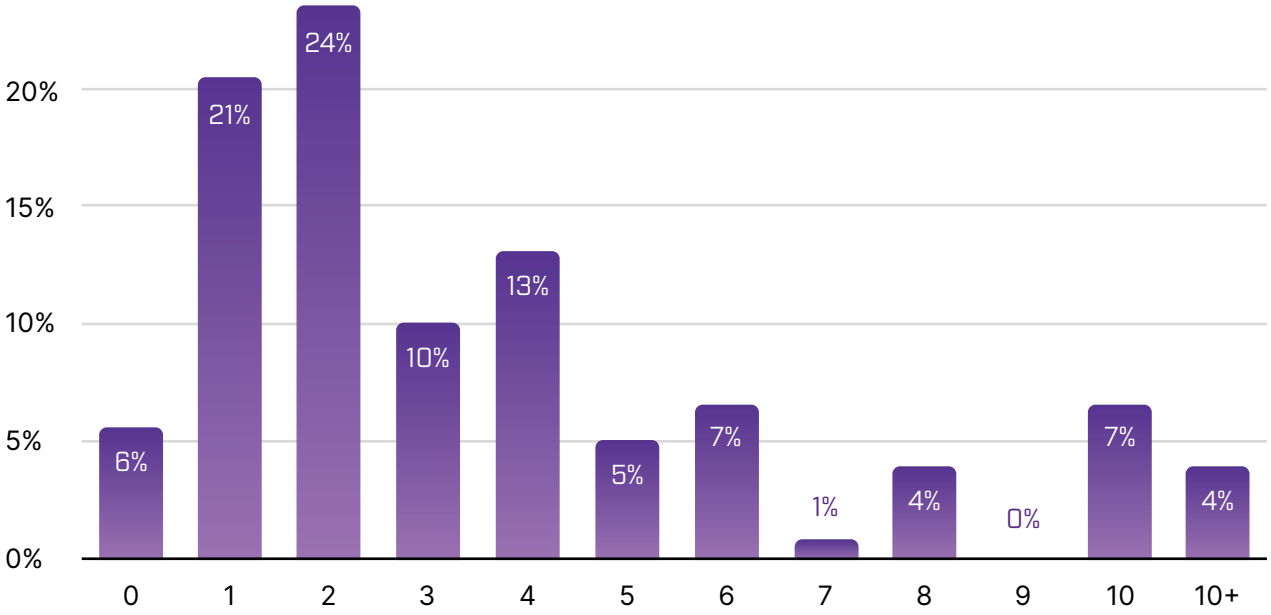
QUANTITIES AND METRICS

The question of how much time is available for training generates a considerable range of responses.

- A detailed examination reveals that 6% of the participants do without training altogether. However, if training is dispensed, it is most often in the form of attack simulations.
- One-fifth of the participants conduct only one training course per year (21%) and just under a quarter of the participants conduct two courses (24%).
- 11% of participants conduct 10 or more courses per year.
- Almost two-thirds of the participants (65%) send 2-5 phishing simulation emails per year. The best practice is three to four campaigns with 3-5 scenarios per campaign; i.e., one employee should receive around 12 phishing simulation emails or more per year.
- From the point of view of the study management, only 15% of the participants send a reasonable amount of 10 or more phishing emails per year.

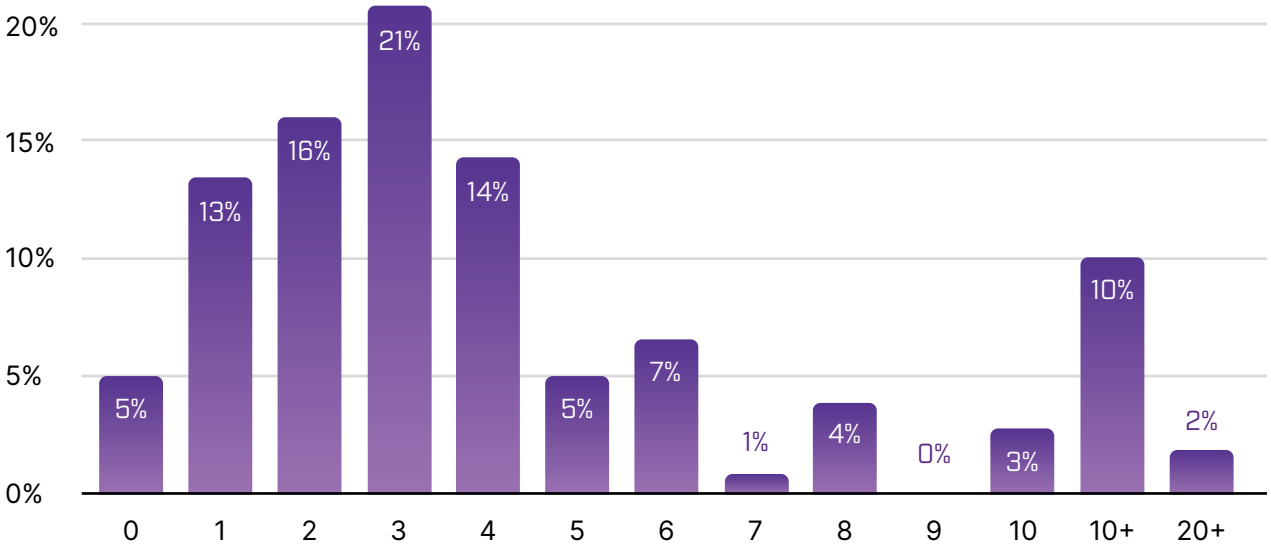
In contrast to the amount of phishing simulations performed, valuing the data on the amount of training completed makes little sense. The quantity of courses without knowledge of the course content and the available time budgeted has no significance.

On Average, How Many Security Training Modules Do Your Employees Complete Yearly?



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

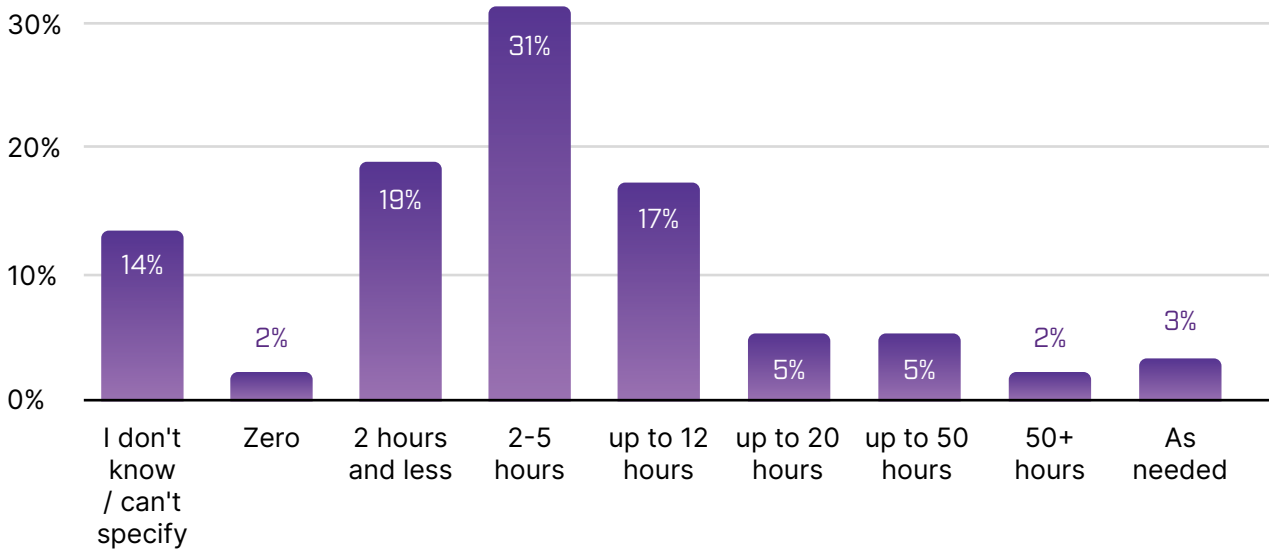
On Average, How Many Phishing Simulation Emails Do Your Employees Receive Yearly?



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

Around two-thirds of participants (67%) stated that between two and 12 hours are budgeted for IT security training. It is notable that only 10% of participants have an annual training budget of 21 hours or more. Only 2% of the participants stated that no training budget is available at all in their organization.

On Average, How Much Time Do Your Employees (Per Person) Spend On Security Awareness Training Yearly?

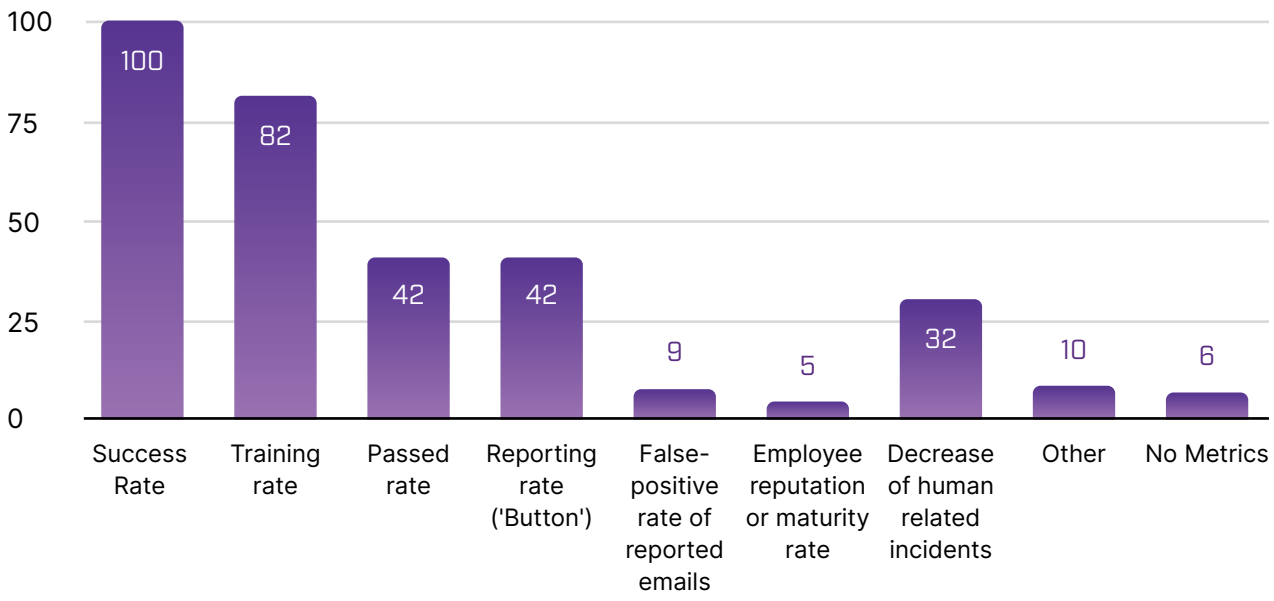


SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

As expected, all participants measure the click and success rates, as was the high index of 82 of the training courses conducted.

The pass rate and the reporting rate, which refers to the phishing button, both come in at a relatively low index of 42.

What Security Awareness Metrics Are Tracked At Your Organization?



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

The detailed analysis shows that the KPI systems in the awareness market are not yet mature. The low reporting rate, with an index value of 42, is certainly also related to the low use of the phishing button in the companies (42%).

Detailed Insights Around Awareness Campaigns

IT Security Training Content

Most companies train their employees on the following topics:

1 PHISHING AND MALWARE

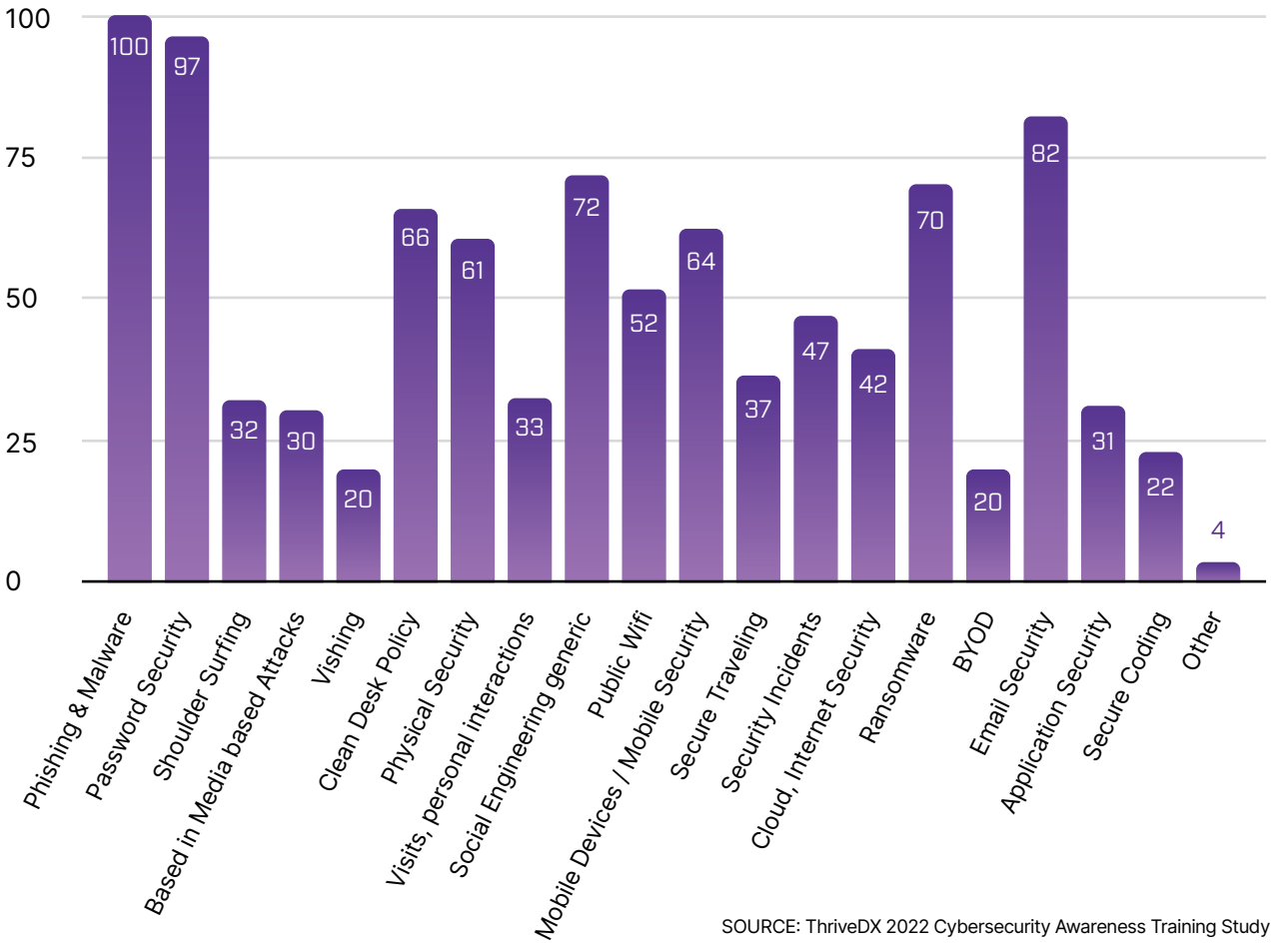
2 PASSWORD SECURITY

3 EMAIL SECURITY

Other significant training areas include clean desk, physical security, social engineering, public wifi, mobile devices, security incidents, and ransomware.

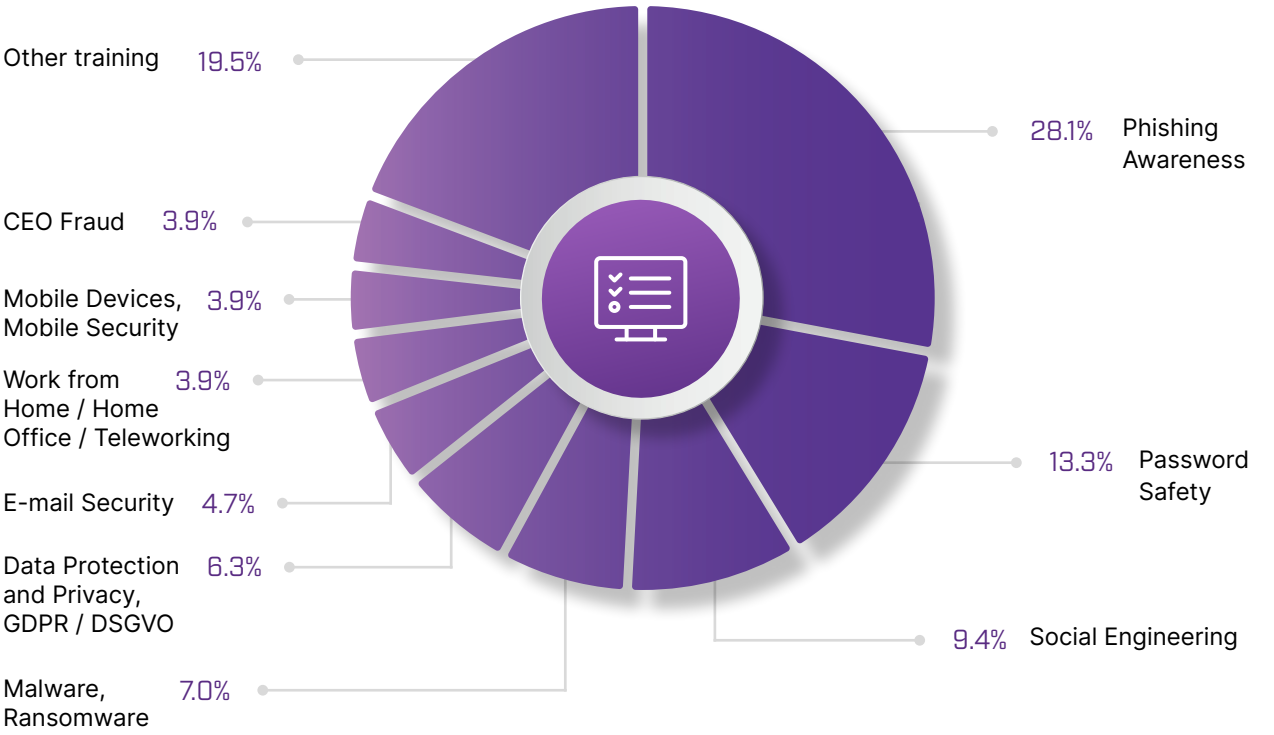
Niche training conducted in the market includes courses such as Shoulder Surfing, USB Attacks and the Like, Vishing, Dealing with Visitors and Personal Interactions, BYOD and Work from Home, Application Security / Secure Coding, and Internal Security Policies.

Which Cybersecurity Topics Are Covered In Training At Your Organization?



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

What Awareness Training Topics Have You Conducted Recently?



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

The responses to the question of which training courses have been carried out in the first half of 2022 show a high degree of variability: 9 training areas account for over 80% of the training courses.

IT Security training areas covered in 2022:

1. Phishing mail detection
2. Password security
3. Social engineering in general
4. Malware, especially ransomware
5. Data protection, data security, and GDPR/DSGVO
6. Email security
7. Security in the home office / Secure work from home
8. Security for mobile devices (Mobile IT Security)
9. CEO fraud

FREQUENTLY USED SCENARIOS FOR PHISHING SIMULATIONS

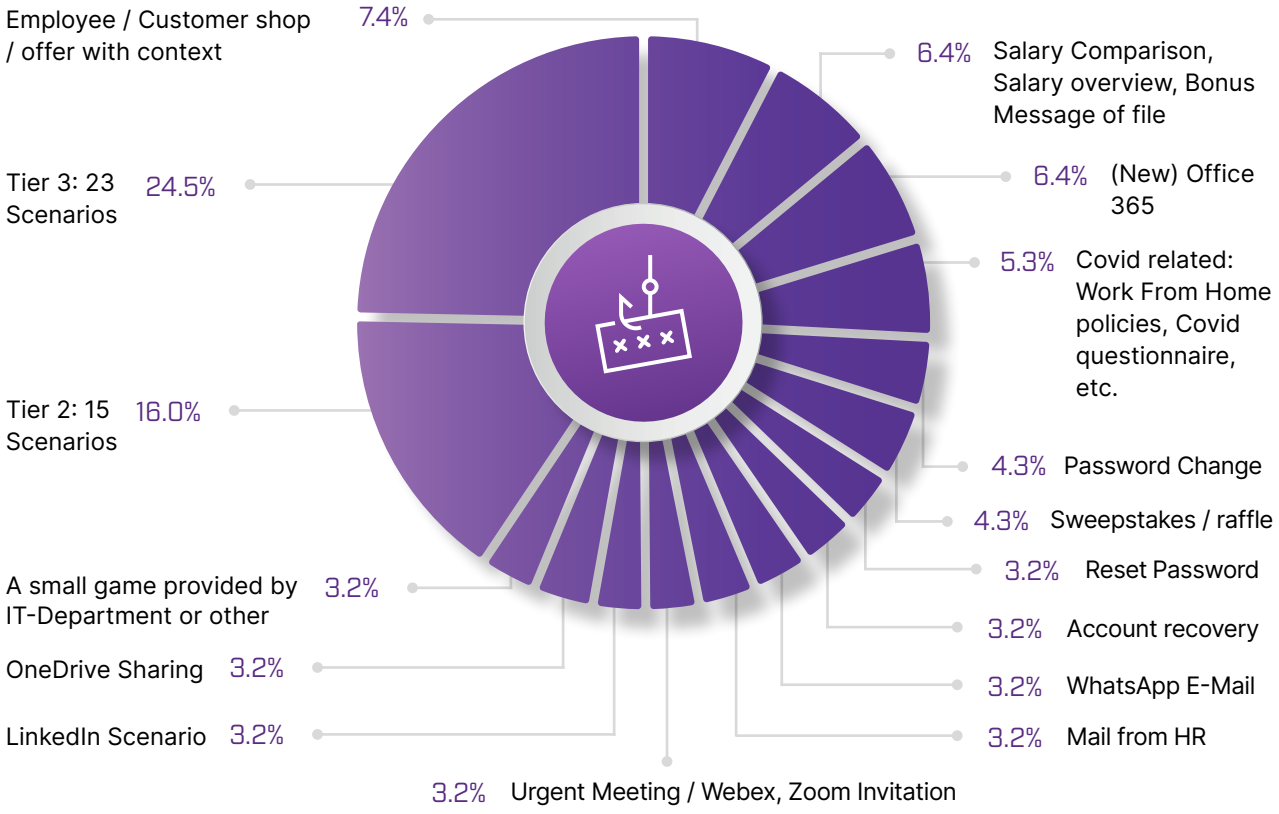
Business-related, accurate spelling and language, as well as emotionality

Supposedly trustworthy senders or senders with high authority

Discount offers, payroll-related messages, and system messages

The question regarding the most successful phishing scenarios yielded a considerable amount of variability. It was often mentioned that "all" phishing simulations seem to work if a plausible corporate context can be established in the attack scenario, combined with the right language. The most successful scenarios have been those that appeal to the emotional level: curiosity, sense of duty, urgency, helpfulness, greed, profit, empathy, and personal addressing. Senders who are supposedly trustworthy or who exude a high level of authority also increase the click rate.

Which Phishing Simulations Have Been The Most Effective At Your Organization?



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

These tier 1 scenarios make up the bulk of popular phishing simulations, at just under 60%:

- Discount offers
- Scenarios related to payroll (wage comparison, canceled bonus, payroll)
- Office365 system messages (migration, password)
- Covid related scenarios and home office policies
- Password change
- Sweepstakes and raffles
- Account recovery calls
- OneDrive scenarios (file sharing, etc.)
- A small game provided by the IT department

Tier 2 phishing scenarios include:

- Shipping confirmation
- Google / iCloud / O365 Account access
- Microsoft OneDrive downloads
- Document shared via Teams
- SharePoint collaboration invitations
- Event registration
- Password check / Strength test
- Sign-in alerts (Google, Microsoft)
- Notification from the IT Department
- Social media notification / Violation / Login / Activity

Less frequently mentioned tier 3 phishing scenarios include:

- Business event / upcoming event
- Fake Microsoft email
- SAP Success Factors email
- Email in Quarantine
- WFH / Back to Office policies
- Dropbox scenario
- Mail from Mastercard
- Apple device employee offer
- Software update scenario
- Link to important documents (with login)
- Fax Message
- Microsoft data leak information
- IT Security survey

SUCCESS FACTORS IN AWARENESS TRAINING

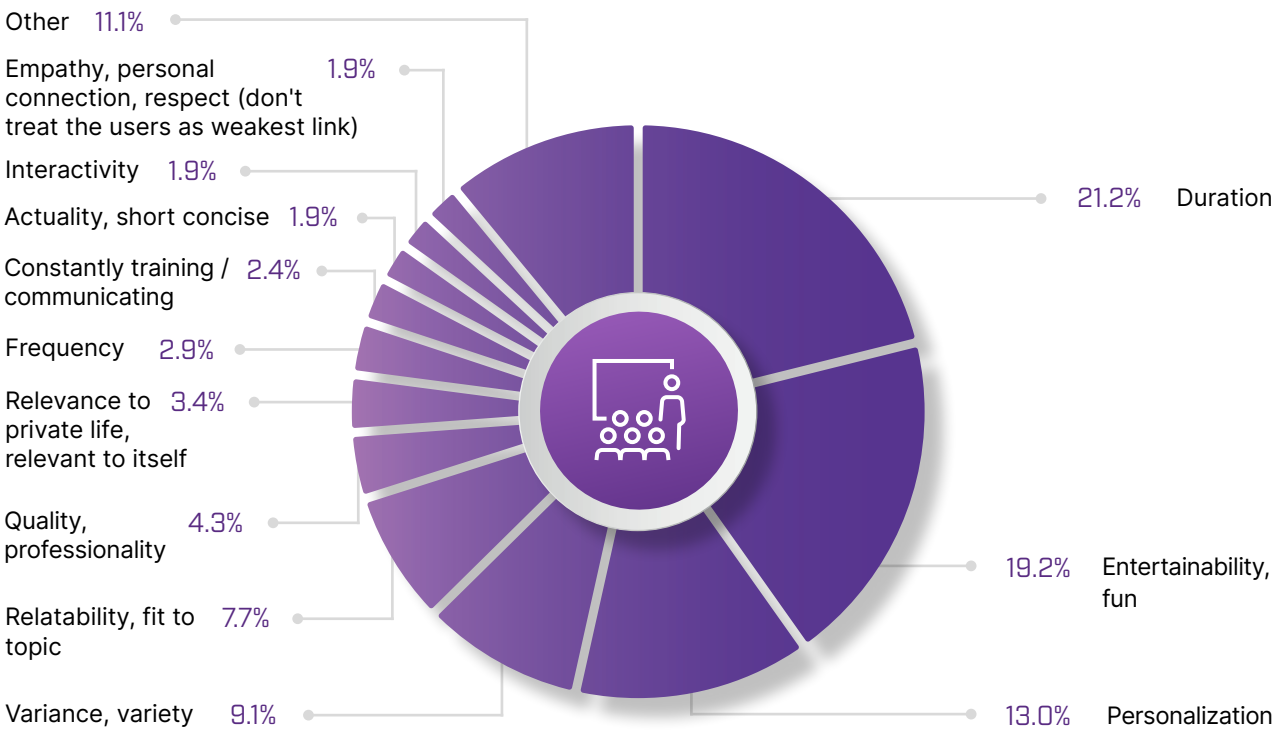
The top 3 success factors, with a share of 53.4% of the mentions for IT security awareness training, are duration, entertainment value, and personalization. Personalization is the ability to customize training and adapt it to specific needs.

Second group of success factors:
(24.5%): Variance, relatedness, and topic fit; quality and professionalism; and relevance to personal life or job function

Third group:
(11%): Frequency, continuity, timeliness, interactivity, empathy, and respect.

Other:
Sporadically mentioned success factors with 11.1% share of the mentions include optically appealing, good to look at; real-life examples; gamification; inclusiveness; easy to understand; culturally appropriate; learning new things; pace can be individualized; must be recognized as meaningful; playfulness; and time allocation by management.

Which Factors Determine Whether A Training Is Successful At Your Organization?

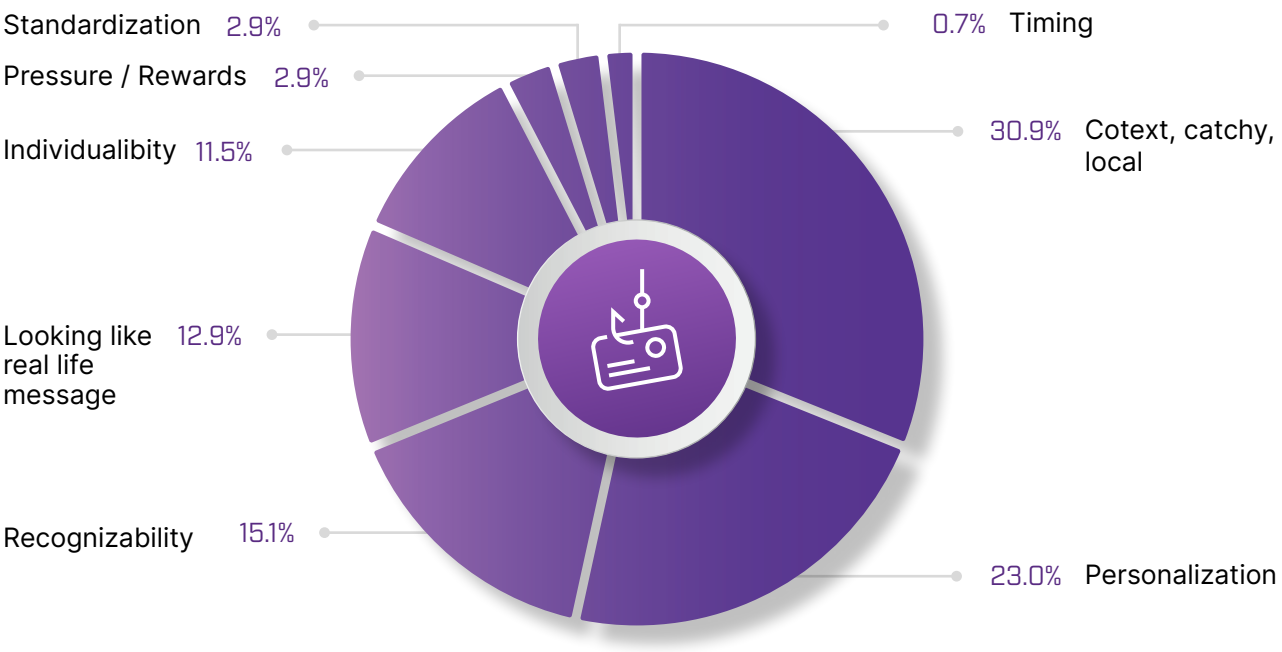


SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

SUCCESS FACTORS IN PHISHING CAMPAIGNS

- The five most important success factors are context, adaptation, recognizability, plausibility / reality, and individualization.
- The question of what constitutes a “good” phishing simulation was taken up and answered controversially by the participants.

Which Factors Determine Whether A Phishing Simulation Is Successful At Your Organization?



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

Five factors determine a good phishing simulation:

1
The scenario must fit into the (corporate) context or have a local reference and / or arouse the reader's interest (catchy)

2
The phishing simulation must be customizable in terms of appearance and content

3
The scenario must still be identifiable as a phishing email. Users should be able to recognize that a phishing attempt has been made

4
The phishing scenario should appear real, legitimate, and plausible at first glance and should contain the correct operational language

5
Individualization (i.e., the concrete and correct user address) is also very important for a successful simulation scenario

> "What is a good phishing simulation? One where as many as possible 'fall in' or a simulation with the highest possible reporting rates."
>
> **Study participant**

Other success factors mentioned were:
Work with pressure, rewards or similar; standardization; the right timing; and constant repetition.

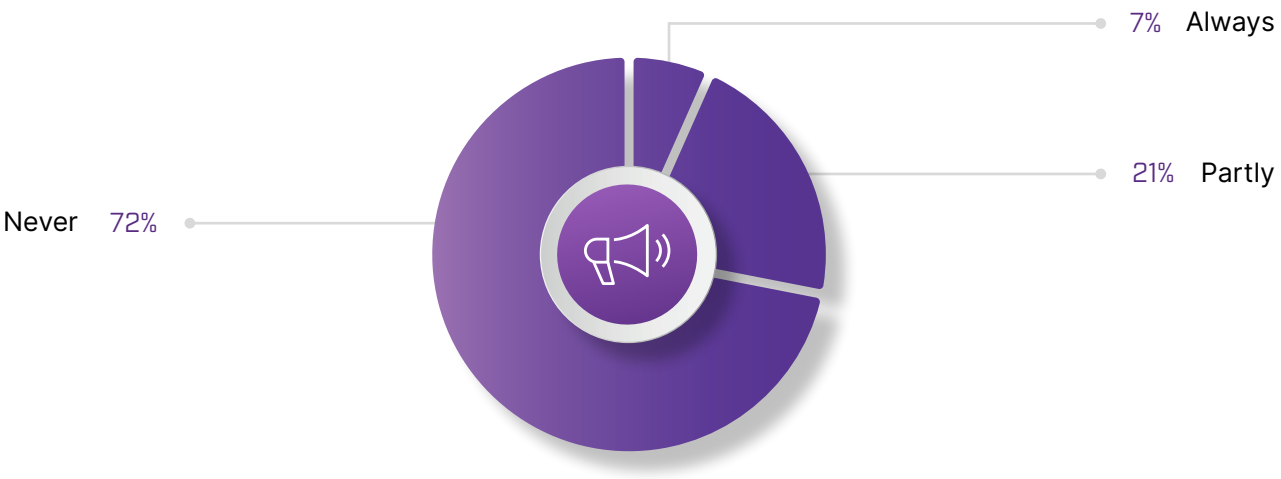
Controversy:
The responses revealed controversial attitudes about what constitutes a successful phishing simulation. The reality is that the learning effect of campaigns that are optimized for the highest possible reporting rates is smaller. If many employees "fall in", it also means that many employees have not noticed the phishing simulation and, thus, no learning effect is created. This is why the "detectability" factor was mentioned so often by the survey participants. The tension between simple simulation and highly personalized simulation is best resolved by providing the user with both simple and highly personalized phishing scenarios.

PRE-NOTIFICATION OF PHISHING CAMPAIGNS

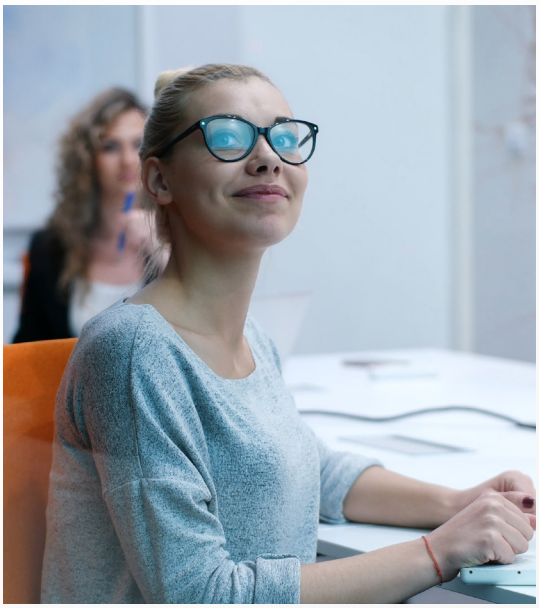
Only 7% of the participants stated that they inform their employees about phishing simulations before they are planned. At 72%, a large proportion of participants do not give advance notice of a phishing simulation. Of course, it is highly recommended that when the awareness program is introduced, all stakeholders — including staff — are fully informed about which cybersecurity awareness measures (e.g., phishing simulations) will be used.

Once this initial communication has taken place and the awareness program is in regular operation, pre-announcement no longer seems necessary.

Planned Phishing Simulations Are Announced In Advance



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study



Cybersecurity Awareness Training in Terms of Strategy and Culture

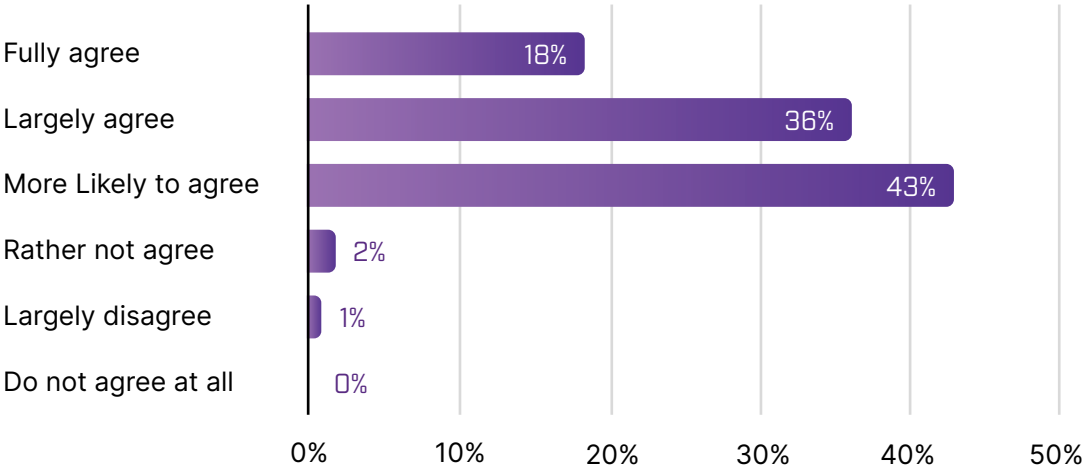
For 58% of the participants, cybersecurity awareness training is part of the IT strategy.

99% see a strong positive influence of cybersecurity awareness training on the culture of errors. The same (96%) see a neutral to strongly positive influence on the working atmosphere.

97% of the respondents stated that cybersecurity awareness training leads to a higher level of corporate security.

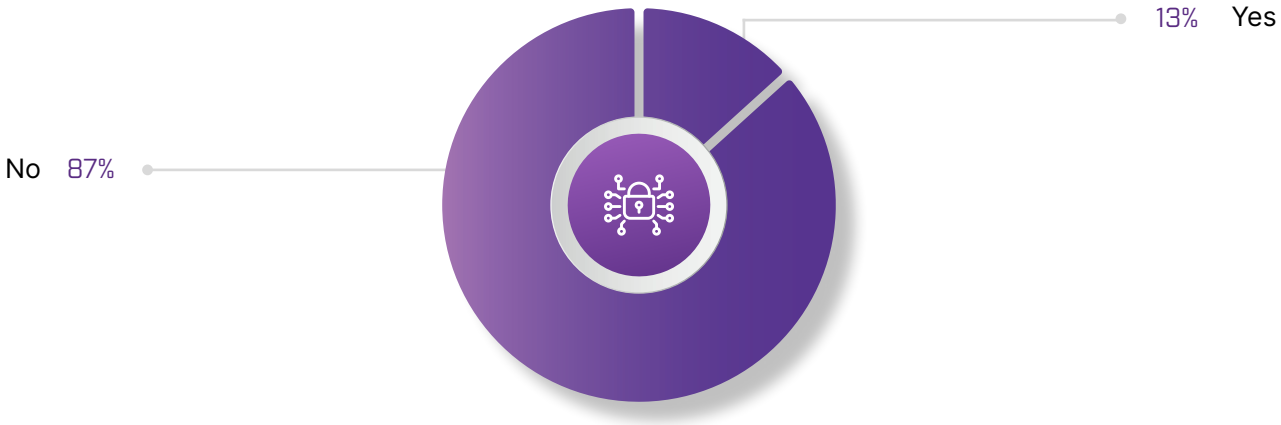
87% of respondents stated that a decent level of IT security cannot be maintained in the company if employees are not made aware of cyber risks.

Security Awareness Activities Led To A Higher Level Of Security At Our Organization

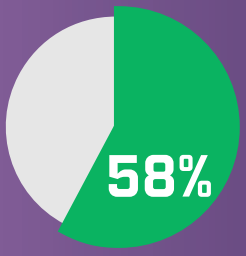


SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

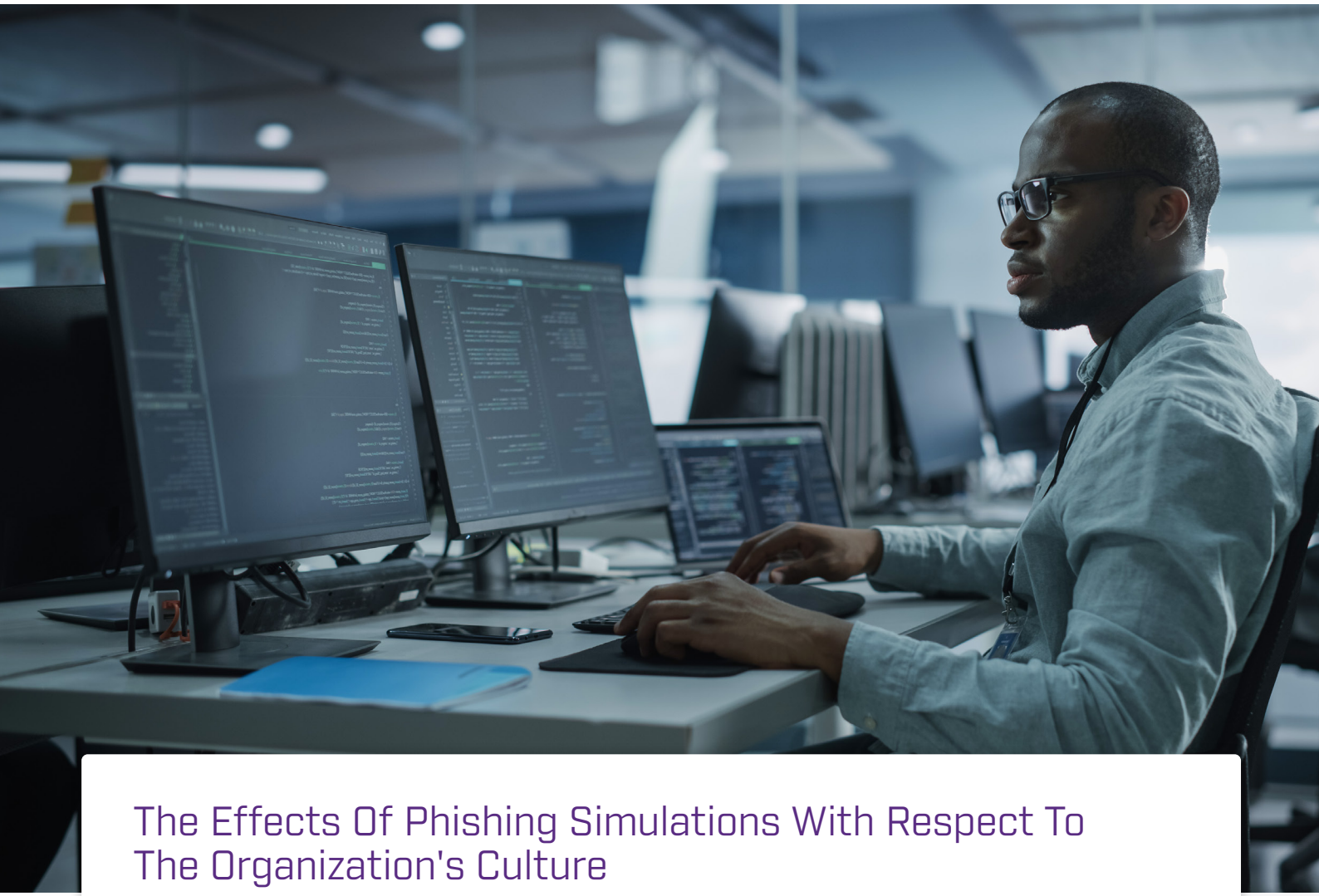
Can You Maintain A Decent Security Level In Your Organization By Investing Only In Technology?



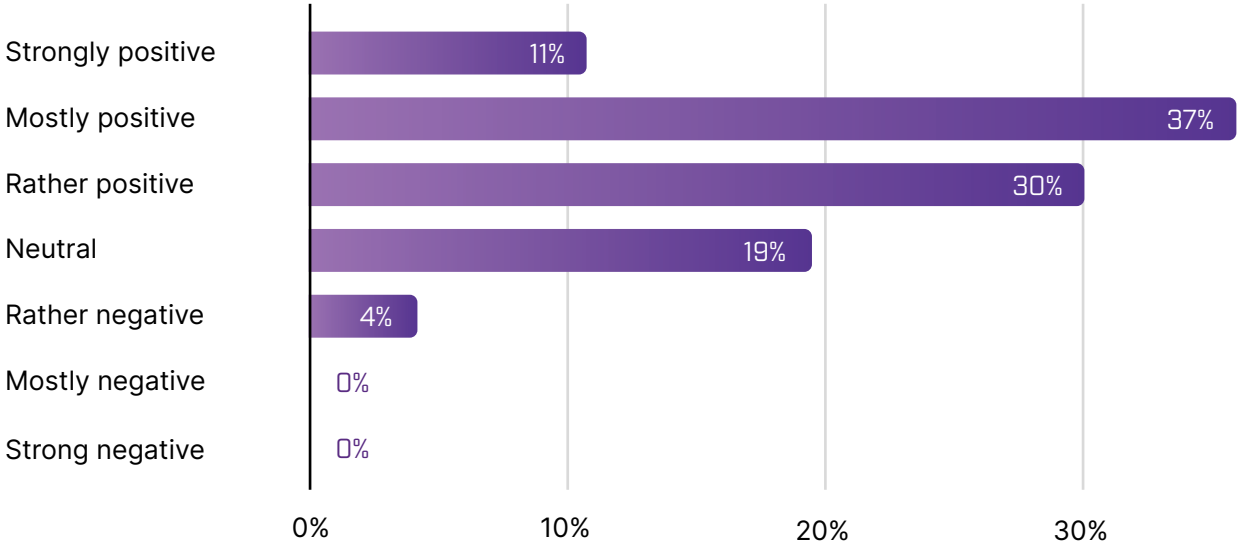
SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study



Cybersecurity awareness training is now increasingly embedded in IT strategy, with 58% of respondents having an awareness policy in place.

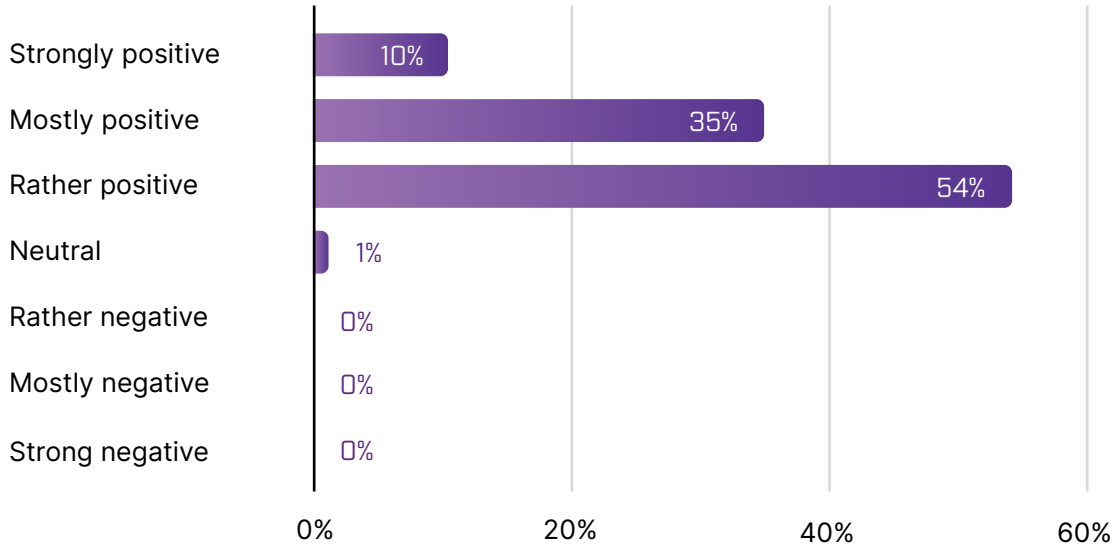


The Effects Of Phishing Simulations With Respect To The Organization's Culture



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

The Influence Of Cybersecurity Awareness Training On The Culture Of Errors



SOURCE: ThriveDX 2022 Cybersecurity Awareness Training Study

96% of the participants stated that phishing simulations make a neutral to strongly positive contribution to the work atmosphere. Almost half of all respondents (48%) were even convinced that cybersecurity awareness training and phishing simulations make a significantly positive contribution to the work climate.

A resounding 99% confirmed that cybersecurity awareness training makes a positive contribution to the error culture of an organization.

96% of the participants stated that phishing simulations make a neutral to strongly positive contribution to the work atmosphere

Concluding Statements

Ninety-one percent of successful cyber attacks start with the employee. Cybersecurity awareness training measures should always start with the people. The results of the study validate the positive effects that practical, ongoing cyber training has on IT security in an organization.

Ninety-one percent of successful cyber attacks start with the employee

Virtually all survey participants reported an improvement in their error culture and 96% confirmed a better working atmosphere thanks to cybersecurity awareness training. The greatest outcomes are achieved when the human factor is prioritized, going beyond awareness to reach understanding. A robust and effective cybersecurity awareness training program is one that includes both engaging content as well as attack simulations. Phishing simulations are now used as an awareness measure with the same frequency as awareness training. The biggest challenges faced by IT professionals are achieving user acceptance, a lack of resources (staff, time, money), and ensuring the continued operation of the awareness program.

Fifty-eight percent of organizations now have awareness regulations in place and two-thirds of respondents said they want to continue to expand their awareness programs. The same amount said they provide their employees with up to 12 hours of training budget per year. Course duration, entertainment, and personalization (including for job function) are considered to be the three most important success factors for a cybersecurity awareness training program. The success of phishing simulation scenarios is largely based on the corporate context, the personalization, and the recognizability of the simulation.

Research Methodology

The global online study "Benefits and challenges of Cybersecurity Awareness 2022" was conducted in April, May, and June 2022, among more than 1,900 qualified security specialists. Close to 8% of the respondents answered the extensive questionnaire. During the same period, the survey was also publicly available and was advertised on LinkedIn [10] and Social Media. 4.5% of all answers have been collected through this channel. Of the respondents, 87% stated that they were security awareness specialists. And finally, 89% of the respondents indicated that they use LUCY / ThriveDX Software for security awareness activities.

Footnotes and References

[1] https://lucysecurity.com/wp-content/uploads/2020/12/Cyber-Security-Awareness-Study-2020.pdf

[2] IBM Cyber Security Intelligence Index Report

[3] https://www.linkedin.com/search/results/content/?keywords=global%20awareness%20survey%202022&sid=j%2Cc&update=urn%3Ali%3Afs_updateV2%3A(urn%3Ali%3Aactivity%3A6927145204630089729%2CBLENDED_SEARCH_FEED%2CEMPTY%2CDEFAULT%2Cfalse)

ThriveDX

Lucy
Powered by ThriveDX

Thank you!

We appreciate your support in reading our 2022 Cybersecurity Awareness Training Study. For more information about our products and solutions, please visit thrivedx.com/for-enterprise.