10 YEAR ANNIVERSARY

SANS

Embedding a Strong Security Culture

SANS 2025 Security Awareness Report®

Workforce Security and Risk Training

Table of Contents

Executive Summary

We are excited to have you join us for the 10th anniversary of the SANS Security Awareness report. This report is designed to enable organizations to better manage their human risk and ultimately drive a stronger security culture.

The report is divided into three sections:

1 Program Benchmarking

This section provides an overview of security awareness and culture programs, enabling you to benchmark your organization against others in a variety of different areas.

2 Program Maturity and Growth

This section provides data-driven steps to grow and mature your security awareness program.

3 Professional Development

This section guides security awareness and culture professionals in developing their skills and grow their careers.

This report does not have to be read straight through, feel free to jump to the sections that interest you the most.

In this report, we use the term ***security awareness*** program to describe a structured effort to engage, train, and secure your workforce and ultimately build a strong security culture. However, many organizations refer to such efforts using different terms, including ***security behavior and culture***, ***security engagement and influence***, ***security training and education***, ***security communications***, or ***human risk management***. There is no single right or wrong term. We are less concerned about what you call your program and more concerned about enabling you to secure your workforce and ultimately your organization. Wherever you see the term security awareness in this report, simply replace that term with whatever term or description you and your organization use.

Key Findings

Maturing Your Program

Similar to past years, the 2025 survey found one of the most important variables that correlates with mature programs is the size of your security awareness and culture team. Unsurprisingly, the larger your team, the more mature your program. New this year is that it's not just the size of the team that is important, but how long you have had a structured program focusing on the human side of cybersecurity. We found that organizations that were effectively changing their workforce's behavior had a team of at least 2.8 dedicated full-time employees (FTEs) and could take 3-5 years to have an impact organization-wide. To go beyond behavior and embed a strong security culture requires a larger team of at least 3.9 FTEs and can take up to 5-10 years for organization-wide impact. The most mature programs often had over 6 dedicated FTEs and had been operating for more than 10 years.

Growing Your Career

This year's report presents an in-depth analysis of compensation and pay rates, with the average salary of security awareness professionals at $116,091 globally. We found big differences in pay based on region, background, and industry, which we detail later in this report.

Sharing Your Thoughts

As part of our 10th anniversary, we asked five new open-ended questions about you and your program. What we learned surprised us, and in other cases confirmed what we already knew. One of the biggest findings is just how passionate our community is, but also how overwhelmed everyone is!

Data From Around the World

Not only are we excited that we now have ten years of data to share with you, but this report is based on our largest survey ever, with feedback from over 2,700 security awareness practitioners from more than 70 countries. Participants from North America, Europe, Asia, Africa, Australia, and South America shared their unique perspectives to create our most comprehensive and revealing report yet.

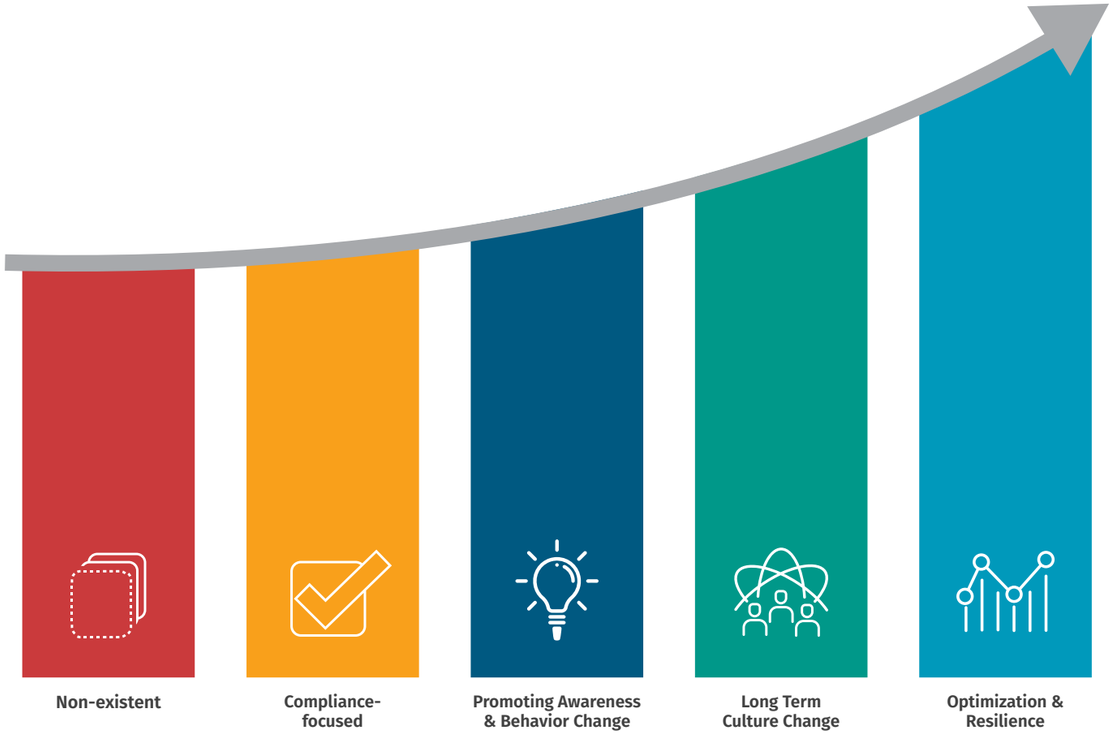
Section 1
Benchmarking Your Program

We would like to start by providing you background on the security awareness and culture industry, specifically what the typical program looks like and how your program compares.

Security Awareness & Culture Maturity Model

To determine the maturity of an organization's program, we leverage the Security Awareness & Culture Maturity Model. First created in 2011 through a coordinated effort by more than 200 awareness officers, this model enables organizations to identify and benchmark the current maturity level of their security programs and identify a path for improvement. The most mature programs go beyond behaviors and embed a strong security culture throughout the organization.

Security Awareness & Culture Maturity Model



As outlined in the model, the levels of maturity are as follows:

Non-Existent
No formal program is in place. Employees have no idea they are targets, that their actions have a direct impact on the security of the organization, do not know or follow organization policies, and easily fall victim to attacks.

Compliance-Focused
The program is designed primarily to meet specific compliance or audit requirements. Training is limited to an annual or ad hoc basis. Employees are unsure of organizational policies and/or their role in protecting their organization's information assets.

Promoting Awareness and Behavioral Change
The program identifies the top human risks to the organization and the behaviors that manage those risks. It goes beyond annual training and includes continual reinforcement throughout the year. More mature programs in this stage identify additional roles, departments, or regions that represent unique risks that require additional or specialized role-based training. Content is communicated in an engaging and positive manner that encourages behavior change. As a result, employees understand their role in cybersecurity, follow organizational policies, and exhibit key behaviors to secure the organization.

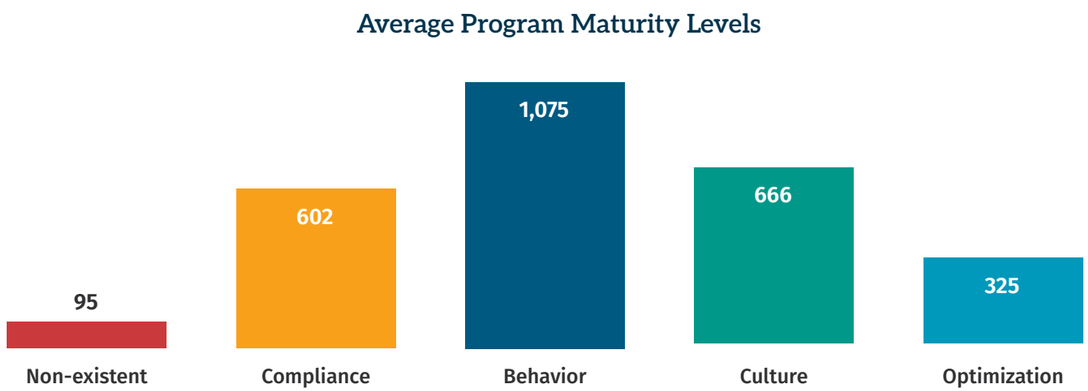
Long-Term Sustainment and Culture Change
The program has the processes, resources, and leadership support in place for a long-term sustainment. In addition, the security team has moved beyond continuous training and is focusing on additional human related drivers, such as simplifying security policies and workforce communications, supporting incentive programs, or improving how the security team partners with and enables other departments. As a result, security is an established part of the organization's culture and the workforce believes in, supports, and prioritizes security in their actions and processes.

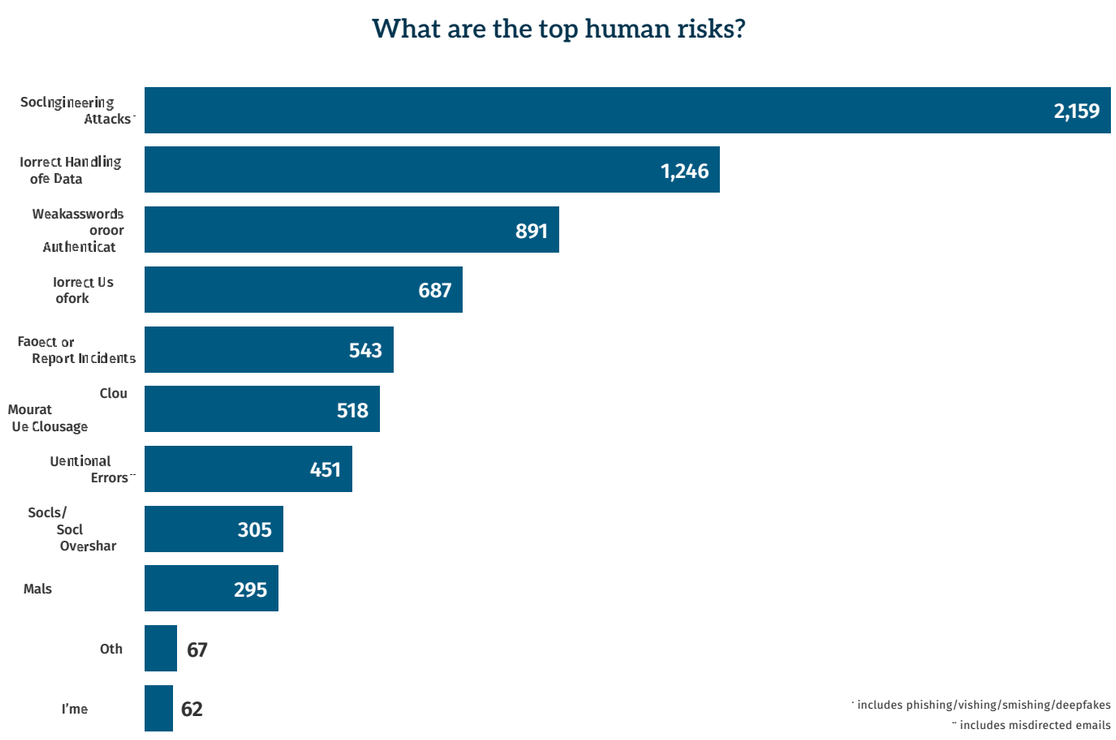
Optimization and Resilience
The program has a robust metrics framework aligned with and supporting the organization's mission and business goals. It no longer just measures and reports on changes in behavior and culture, but ultimately how these changes reduce risk and enable leadership to achieve their strategic priorities. As a result, the program is continuously improving and demonstrates return on investment.

This report includes a copy of the Security Awareness & Culture Maturity Model Indicators Matrix (**Appendix A**), which enables you to easily identify your program's maturity level, the metrics for each stage of the model, and the steps to achieve the next stage in the model.

Benchmarking the Maturity of Your Program Against Others

So, what are the average maturity levels for organizations, and how does your program compare against others? Overall, the results look like a typical bell curve, with a slight emphasis on more mature programs. These maturity level findings are like the past five years. However, we are seeing a consistent but slow growth in the "Optimization" stage and a similar reduction in the "Non-Existent" stage.





Top Human Risks

If security awareness programs focus on human risk, which human risks are organizations most concerned about? This year's findings show that organizations identify one human related risk above all others as their top concern: social engineering (phishing, vishing, and smishing).

1 Social Engineering

This category refers to the three most common social engineering attacks: email-based phishing, text-based smishing, and voice-based vishing. While phishing remains the primary social engineering attack method, we are seeing a rise in both number of and sophistication in smishing and vishing. This is in part due to organizations getting better at detecting and stopping phishing attacks, but also because fewer organizations have control over and visibility into employees' mobile devices. Social engineering was by far the top human risk identified by respondents, as technology alone can only go so far in stopping them. In addition, with the growth of Artificial Intelligence (AI), it is becoming easier for cyber threat actors to create customized social engineering attacks, to include voice cloning vishing attacks.

2 Incorrect Handling of Sensitive Data

It seems like more people are handling more data in more complex ways, and with more rules regulating how that data must be handled. Add the complexity of different sensitivity levels, the different ways data can and cannot be shared and then connect it all with cloud-based solutions, and you can see just how complex secure data handling can be. This is one of the highest rated risks simply because it is also one of the most complex risks to manage, both from the technology and human perspective.

3 Passwords/ Authentication

How people authenticate and manage their passwords is a top risk, but to be honest, we were expecting this to be ranked a higher risk, closer to social engineering. One reason we believe passwords are perceived as a much lower risk is the active deployment of numerous strong authentication controls, to include identity access management (IAM), single sign-on (SSO), multi-factor authentication (MFA), biometrics, and passkeys (a relatively new type of phishing-resistant MFA). Organizations know that authentication is a primary attack vector and as a result they are investing heavily in technical controls to support strong authentication.

4 Artificial Intelligence

This is the second year we see AI as a top risk, and unsurprisingly so. The issue we see with AI is not that it is inherently vulnerable or unsafe, but that AI is so new that organizations are struggling to figure out not only how to use it, but what policies and controls should be in place to manage those risks. For many organizations, addressing the risks of AI will be similar to software as a service (SaaS) cloud-based models. Specifically, what data are people sharing with AI, and what are people doing with the outputs? In many cases, security teams struggle to determine what exactly they should be telling and training their workforce on. While this risk was ranked fourth both last year and this year, we expect to see this risk grow in coming years as adoption (and the advancement of AI) increases.

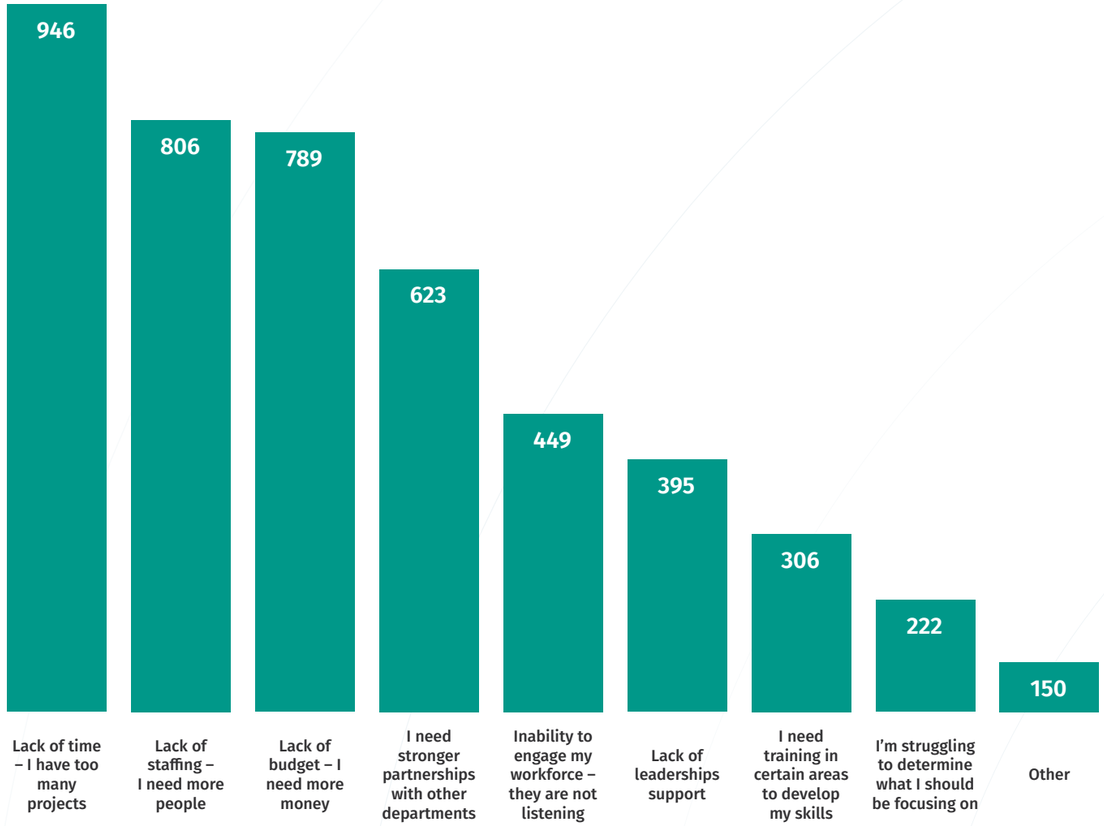
Most Common Program Challenges? – Lack of Time and Staff

In addition to understanding the cyber-based threats that our industry is focusing on, it is important to understand the most common challenges in building and managing an effective program. Like the past five years, the top two challenges are lack of time and people. Securing your workforce and building a strong security culture is ultimately a people problem and requires people as part of the solution. It takes time to:

- Build trust and partnerships with other departments
- Collaborate with the security team to identify top human risks
- Engage and train your workforce
- Track and measure impact
- Coordinate with leadership

You cannot simply purchase a tool and solve these problems. It takes people with a wide variety of skills to secure your organization's workforce and ultimately drive culture change. This is why, later in the report we emphasize the use of tools like Generative AI to help security teams accelerate their impact at a global scale.

What do you feel are the biggest challenges limiting your ability to succeed?



Program Name

We asked respondents what they call their program. We are interested in this question since the name of a program can often impact various elements of that program, such as who it reports to, budget, priorities, etc. 2,673 people answered this question. Like 2024, we found no real consistency in naming convention. Names included everything from Cyber Safety to Organizational Change Management. We struggled to determine the most common names. So instead, we identified the most common words used in the naming of the programs. Below is what we call the Top Ten Breakdown.

> "Securing your workforce and building a strong security culture is ultimately a people problem and requires people as part of the solution."

Top Ten Breakdown

Rank	Word	Count
1	Security	1,134
2	Awareness	1,100
3	Training	272
4	Cyber	260
5	Cybersecurity	241
6	Information	125
7	Culture	56
8	Education	56
9	Compliance	47
10	Risk	40

Long story short, don't worry about the name of your program, as long as it works for you.

To Whom Do Security Awareness Programs Report?

We wanted to understand which department or team security awareness and culture professionals report to. Which department these teams report to can have a huge impact on their ability to secure the workforce and ultimately impact culture.

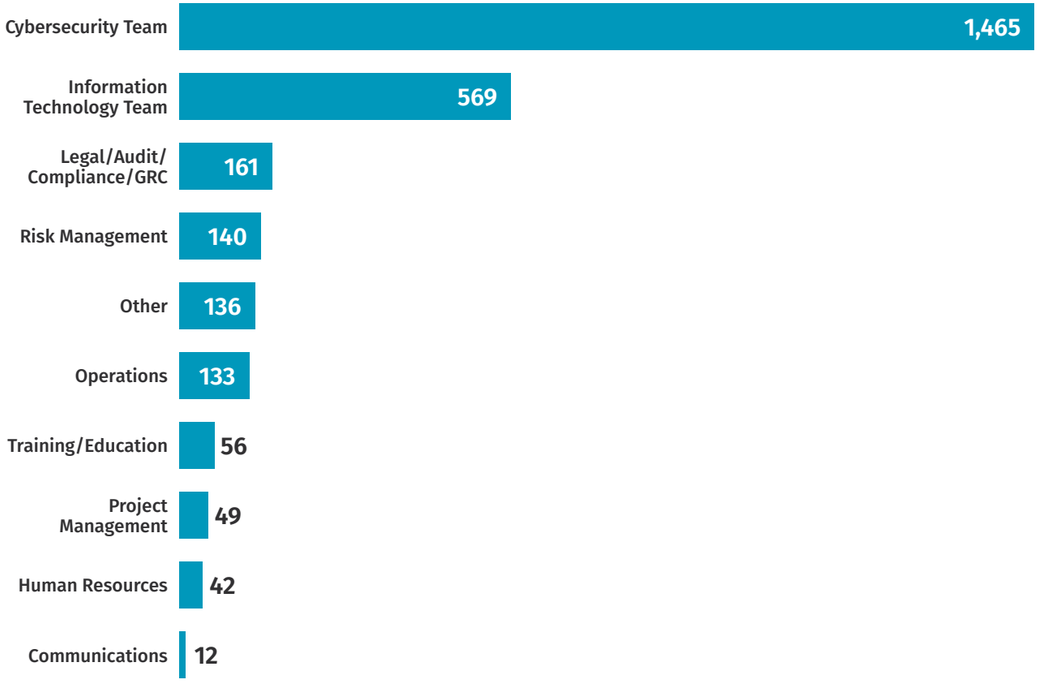
Our concern is teams that report to Legal, Audit, Human Resources, or Training may be focused solely on compliance, i.e., checking the box. These teams are often siloed from and do not interact with the security team. The ability to actively partner with the security team is critical. The security team is not only the primary source for identifying and prioritizing your top human risk, but it is also commonly involved in:

- Policy development
- Security tool rollouts
- Communicating security initiatives to the workforce

The more security awareness and culture integrates and partners with the security team on these activities, the more effective their impact. In fact, security awareness and culture should be just one part of every Chief Information Security Officer's (CISO's) overall risk management strategy.

Similar to years past, most security awareness teams report to the Cybersecurity, Information Technology, or Risk teams, which we consider a good thing

Which department best describes where your security awareness program reports into?



Supporters and Blockers

Similar to 2024's findings, the top three blockers to successful security awareness efforts remain:

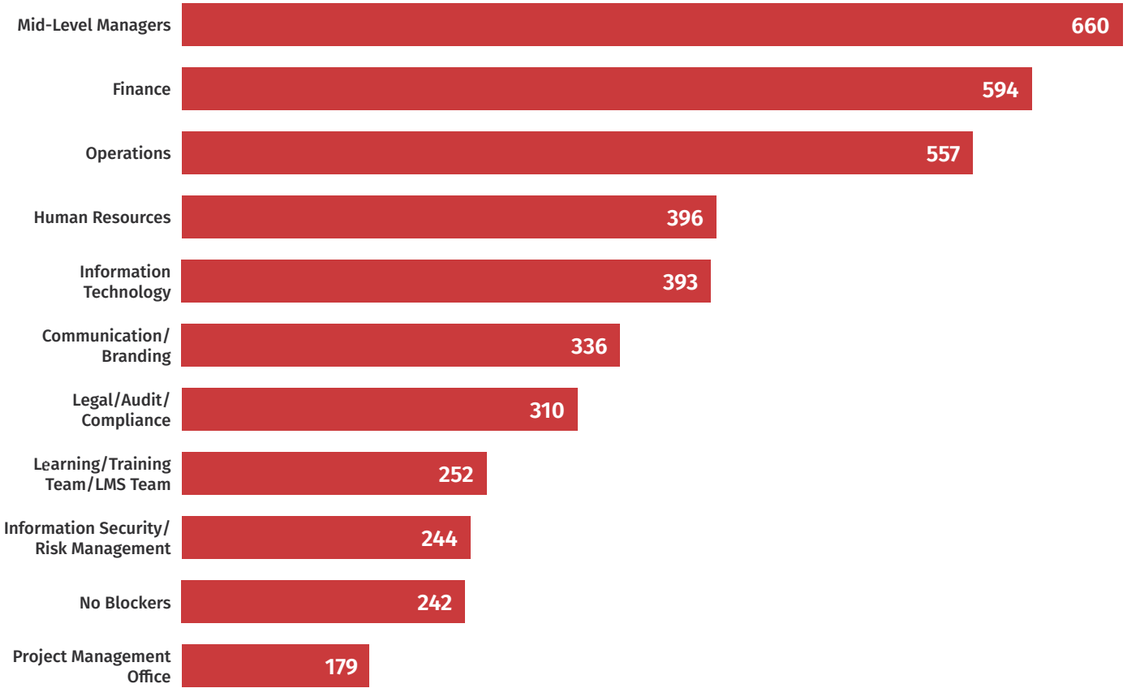
1. Mid-level managers
2. Finance
3. Operations

Mid-level managers manage teams of people and are focused on meeting business objectives, with cybersecurity often perceived as a blocker. They can be a very challenging group to reach as there is no direct line of communication between them and the security team. You may want to consider a targeted training initiative designed specifically for mid-level managers that focuses on why they should care about cybersecurity, how it benefits their team, and how to build a culture of security within their team.

Finance was a close second, most likely as this group is concerned about the costs related to effective training and support of the workforce. Finance may see security awareness programs as budgetary burdens rather than risk-reduction investments.

Operations is most likely concerned about how security training, policies, and changing behaviors affect daily operations. As such, they may view security training, policy updates, and behavioral changes as disruptions to operational efficiency.

Which departments are the biggest blockers to your program's success?



Section 2
Maturing Your Program

Now that you have a better understanding of the security awareness and culture landscape, and how your organization compares to others, we need to identify the key drivers of program maturity and what you can do based on that information.

We identified two key drivers:

1. The size of your security awareness and culture team
2. The age of your program

In addition, we found what we would call an inverse factor. Specifically, the data showed us that the less leadership support you had, the more likely you would have an immature program. This makes sense; if you lack leadership support, you most likely do not have support for the key drivers of success, e.g., the team you need and the support to sustain a long-term, dedicated program.

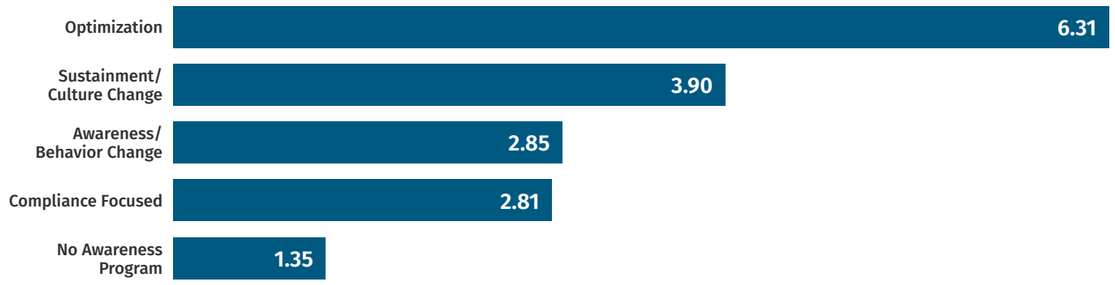
Your Team Size

For the sixth year in a row, we found a strong correlation between the size of a security awareness and culture team and program maturity. The larger your team, the greater your program's maturity level. To determine size, we asked respondents to report how many FTEs supported their awareness program. By full-time, we mean individuals who spend 75% or more of their time on security awareness efforts.

This finding makes sense: securing your workforce and ultimately driving a strong security culture is a people problem, so it requires people to drive the solution. Organizations with the largest security awareness and culture teams can most effectively partner with multiple departments, understand and address their top human risks with relevant resources and engaging content, and frequently communicate with, train, and enable their workforce.

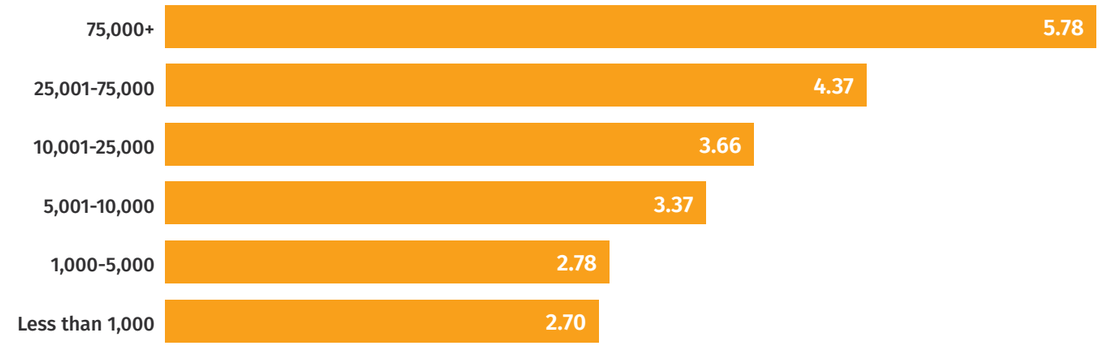
To have an impact on people's behavior, most programs need at least a combined effort of 2.8 FTEs, this means at least 2.8 people who focus 75% or more of their time on the program. Moving from a behavior focus to a culture focus is one of the most challenging. To have an impact on an organization's culture on average requires at least 4 dedicated FTEs. The results have been consistently the same for the past five years. The more people dedicated to or working on your program, the more mature your program.

Average Number of FTEs Needed per Maturity Level



The question we are often asked is, how many FTEs do I need? Unfortunately, we don't have a simple answer. We tried to see if there was some type of linear approach organizations should take, such as one FTE on your awareness team for every 10,000 or 20,000 employees. What we found is the scale is not linear. In part, it's because every organization is different in their goals, mission, and tolerance for risk. Also, it does not matter if you have 50,000 employees or 250,000 employees. In many ways it takes a similar effort to partner with Human Resources or Communications, launch and track Computer Based Training, create and push out engaging emails, develop infographics, or work with the security team to identify your top human risks.

Average Number of Security Awareness FTEs by Organization Size



Quite often, the challenge large organization's face is simply scale and localization, especially trying to reach larger numbers of people in different regions, roles, cultures, or languages. So, the larger your organization, the larger your team needs to be, but not at a linear scale. On the flip side, even relatively small companies (say 1,000 employees) still need that baseline of at least two people dedicated to their security awareness team. If you are looking for a more linear approach to sizing your security awareness and culture team, one approach may be for every ten people on your security team, at least one should be focused on the human side of cybersecurity.

How Old Is Your Program? – Change Takes Time

The importance of team size is something we have known for years. What is new is team size will only get you so far, that the team must be supported and sustained long-term. The longer you have a structured program focusing on the human side of cybersecurity, the more likely you will succeed.

This makes sense, the longer your program has existed, the more likely you are maturing your processes, developing your partnerships, improving your ability to engage, and becoming more effective in how you motivate and enable your workforce. We found that, on average, it takes:

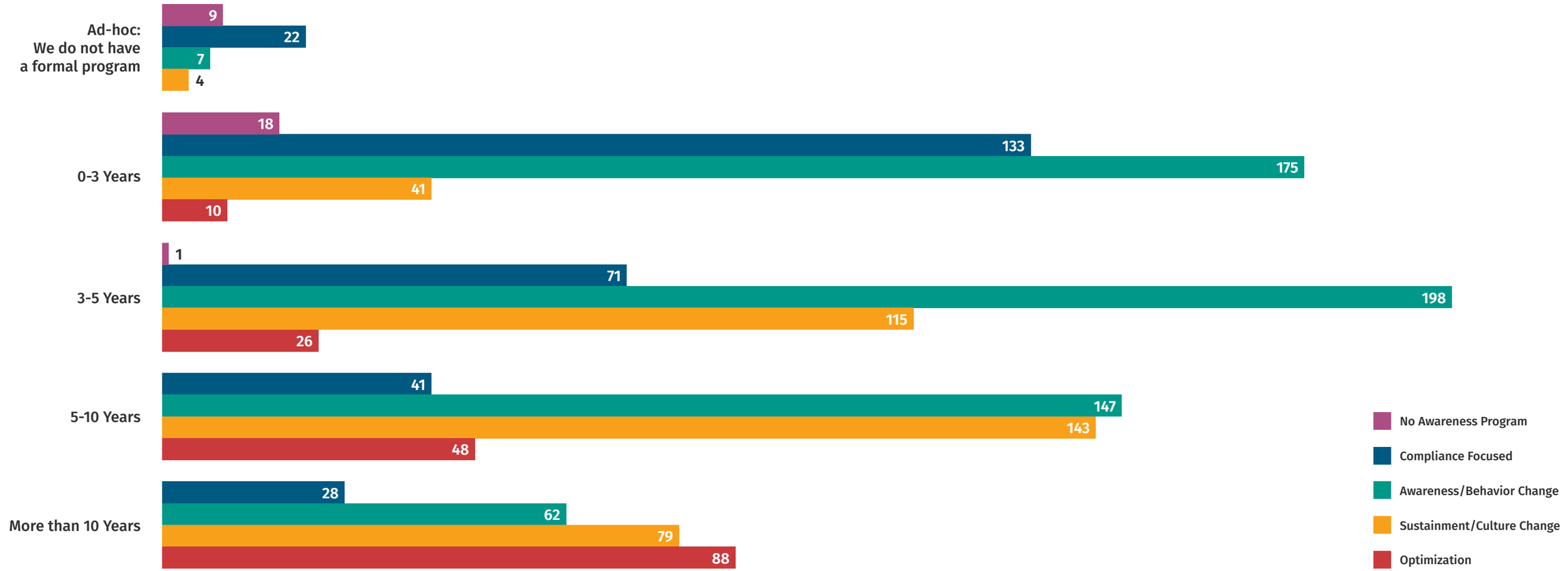
- 3-5 years to begin to truly impact behavior change organization-wide
- 5-10 years to impact culture organization-wide
- 10+ years to reach program optimization

In many ways, these numbers strongly correlate with findings and research into organizational change. Keep in mind the numbers vary for every organization. The larger your organization, the more international your organization, the more diverse your organization, or the older your organization, the longer change takes.

These findings also help explain why so many organizations struggle to have a long-term impact. A large security awareness and culture team is great, but if you are changing that team every year, or dismantling that team every several years, you do not give the team the opportunity for success. What we are learning is that building a strong security culture not only requires people, but time. This is why long-term leadership support is so critical.

> "What we are learning is that building a strong security culture not only requires people, but time."

Program Maturity by Program Age



Action Items to Increase Your Team Size and Sustain Long-Term Leadership Support

Building a strong security awareness and culture program requires both a dedicated team and sustained leadership backing. Below are six actionable strategies to help you achieve both.

1 Talk to Leadership and Security Teams in Terms of Risk or Culture

Leadership and security teams often perceive security awareness as not being part of security, but rather as a compliance effort that has little relevance to managing risk. To help change that perception, focus on and speak in terms of risk management and organizational culture. These terms are far more likely to align with most organizations' strategic security priorities, gain leadership buy-in, and resonate with a security team.

Help the members of your security team understand how you can help them. For example, demonstrate how effective communications, training, and engagement can change key behaviors and ultimately build a stronger security culture. Partner with your Security Operations Center (SOC), Incident Response, and Cyber Threat Intelligence teams to better understand not only what they do but also but how you can help them solve their human-risk-related challenges.

Below are examples comparing two different ways a security awareness officer could describe their role. The first example is how many awareness officers describe their job, in terms of what they are doing. All the actions this individual describes are good actions to be taking; they are effectively engaging their workforce. The problem is one of perception, as leadership may perceive the role being in the entertainment business. Notice how in the second example, the job description is much more risk focused and therefore far more likely to connect with leadership and gain their support.

Example 1 *Hi, my name is Renan, and I'm the security awareness officer. I manage all of our security training activities. I helped lead the new micro-videos we just released and the recent security awareness posters and organized the guest speaker we hosted last month. We are even more excited about next month as we start a new series of security memes and interactive webcasts. Our goal is to increase workforce participation by 26%.*

Example 2 *Hi, my name is Renan, and I'm the security awareness officer. I manage our human risk and ultimately drive a strong security culture. Did you know that our employees were responsible for over 75% of our security incidents last year? I work with the security team to engage, train, and change our workforce behaviors to reduce risk and create a stronger security culture. Our goal is to dramatically increase our ability to securely make the most of technology, including adopting AI as part of our innovation initiative.*

2 Demonstrate the Investment Gap Between Technical and Human-Focused Security

Explain that while your organization has become very effective at securing technology, it has under-invested in the human side, leaving its workforce (and your culture) vulnerable. A simple but effective way to demonstrate this is to count how many people are on your security team. Then count how many of those people are dedicated to the technology side versus the human side. Quite often, we see 50-person security teams with 49 of them focused on technology and maybe one focused on the human side. And then we wonder why people are the primary attack vector. As a starting point, consider having a 10:1 ratio of technical security professionals to human-focused security professionals.

3 Leverage AI

2024 was the first time we recommended leveraging Generative AI to help you. In 2025, due to all the incredible advances of this technology, we have moved this up in our recommendations. If you don't have the budget to hire someone for your team, leverage Generative AI. In many ways, Generative AI can act as an intern or subject matter expert to help with all your needs, from creating engaging emails and content to data or risk analysis. You and your team are still responsible for the results, but Generative AI is becoming extremely powerful in giving you back your most precious resource: time. One example is the **Security ea**, a customized GTP agent designed to help any security team create highly engaging emails for their workforce.

4 Develop Partnerships

You can't do everything yourself. The more you can partner with other departments in your organization, the more effective your team will be. Partner with:

- **Communications to help engage and communicate with your workforce**
- **Human Resources to help with new hires or to measure and build a strong culture**
- **Business Operations to help analyze metrics and data points**

Developing partnerships is something you do not accomplish overnight. It takes time to build trust. Try to take key people out for a coffee once a month or ask if you can sit in on one of their monthly team meetings. Listen and learn what their challenges are and how to best support and work with them.

5 Maintain Regular Communications with Leadership

Set aside four hours a month to collect metrics and success stories, then share these with leadership. By regularly updating them on the value security awareness is providing and how you are supporting the organization, you are far more likely to sustain their support long term.

6 Break Down Your Needs

To bring new people on your team, document all the different steps and initiatives you need to undertake to make your program effective. One approach is to align your initiatives with your leadership's strategic security priorities. Is it improving detection and reporting capabilities, enabling cloud or AI adoption, leading a DevSecOps initiative for developers, or reducing policy violations? Then identify and document the number of FTEs needed for each of these efforts, and at the same time, demonstrate the value of those efforts. Leadership will have a better understanding of why you need more help. If you can't hire new employees on your team, see if you can hire short-term contractors to take on and help manage specific initiatives.

Section 3
Compensation and Career

The goal of this section is to enable security awareness and culture professionals to grow their skills, advance their careers, and increase their compensation.

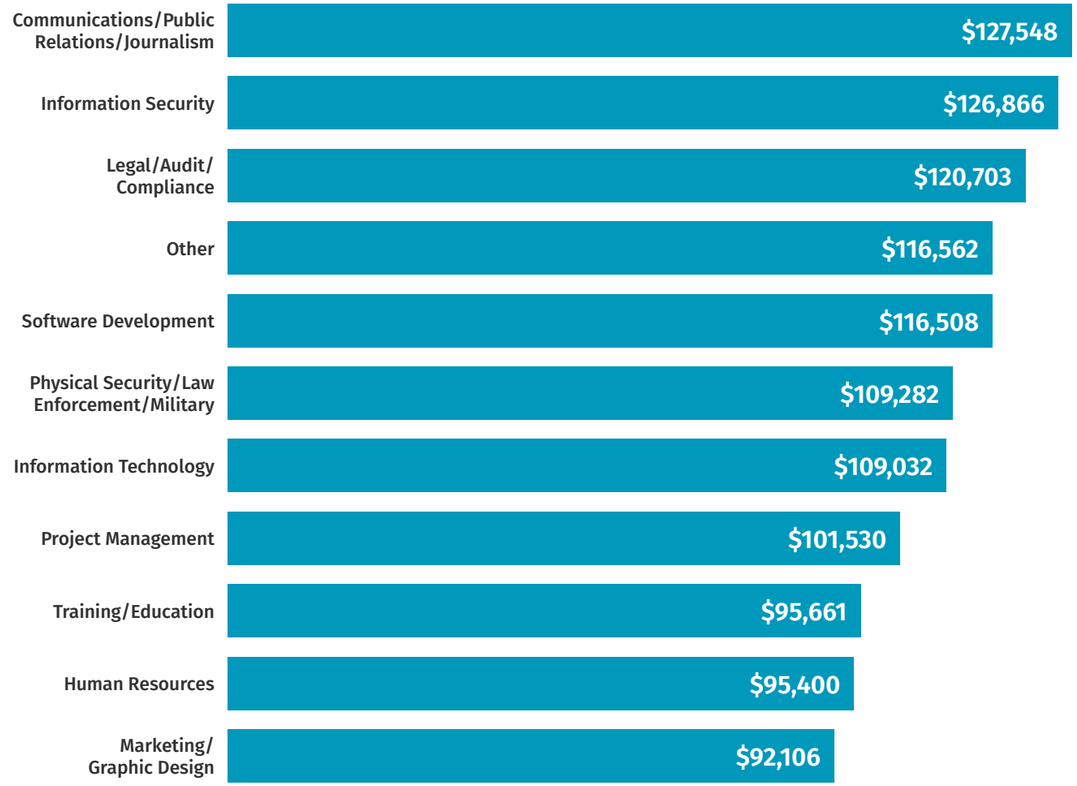
Compensation

Similar to past years, we wanted to know what the average salaries are for people in this field. In 2025, the average annual salary for individuals working in security awareness is $116,091. Keep in mind this draws on responses from all industries and all global regions. In terms of geography, North America has the highest average annual salary at $129,961, almost identical to 2024's findings.

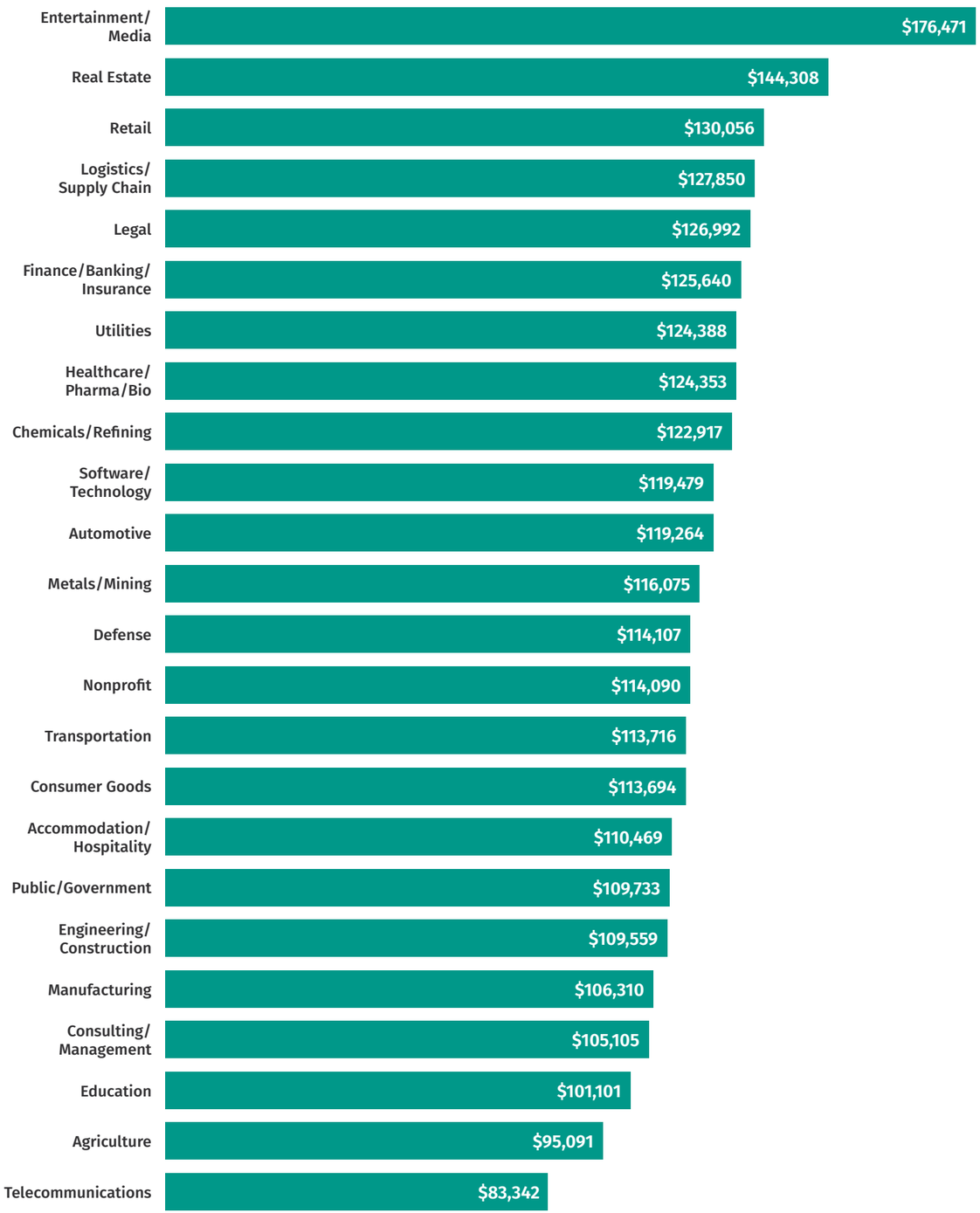
Average Salary by Region

We looked at a variety of other variables to determine which had the greatest impact on pay. In 2025, the two biggest variables in 2025 were ***industry*** and ***background***.

Average Salary by Professional Background



Average Salary by Industry



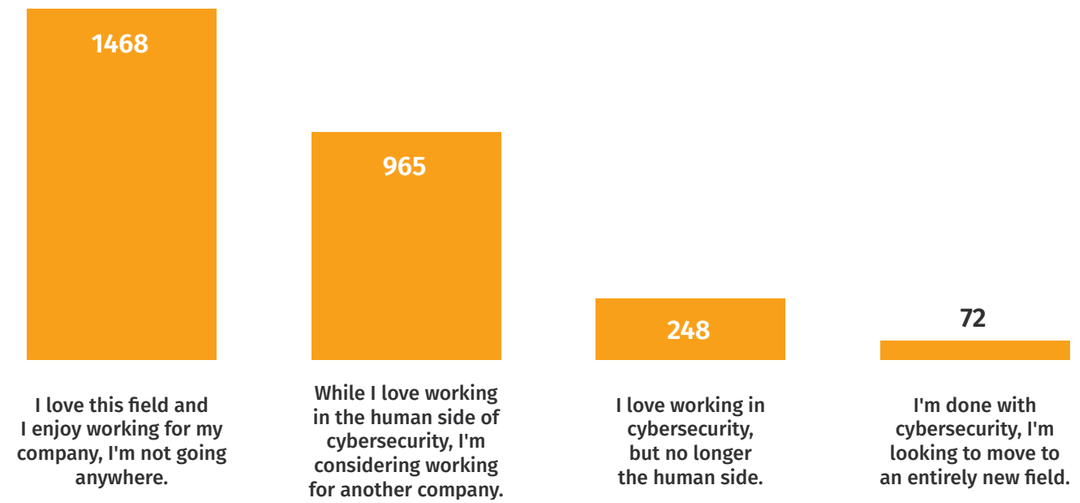
Finally, consider the impact of your role. Are you just contributing to your overall security awareness and culture program, or are you overall responsible for it? There is over a $15,000 difference between the two.

Salary Average by Job Role (Management vs Contributor)

How Are You Feeling?

Now this may sound like an odd question to ask, but we felt it was important. We want to track how happy people are in this field, and if in the coming years those numbers are going up or down. Once again, we were pleasantly surprised at just how much people enjoy the human side of cybersecurity, as almost 90% of respondents said they want to stay in this field. However, a good percentage of those people are looking for work at a different company. So, while most people love the human side as a career, in many cases, not so much the company they work for. Less than 12% want to get out of this field or out of cybersecurity altogether.

How are you feeling, are you happy in your role, do you enjoy working for your company? Is cybersecurity in your future or do you want to try something else?



How to Grow Your Compensation and Career

Action Items for Non-Technical Individuals

Expand Your Role

Security awareness and culture roles can be perceived as limited to just annual computer-based training or some similar compliance-driven activity. However, as a leader in securing your workforce and driving cultural change, your role can and should involve so much more.

- Ensure that leadership understands the strategic importance and focus of your role.
- Work with the security team to improve and simplify its communications with your workforce, help manage security tool rollouts (such as MFA), and create policies that are easier for people to understand and follow.
- Partner with the Incident Response Team to assist with internal and external incident communications.
- Work with senior leadership on tabletop exercises to strengthen their incident response abilities.

You have a huge number of opportunities to expand your value to the security team and leadership, so make the most of it!

Develop Your Security Skills

Develop your understanding of security fundamentals so that you better understand the terms, technologies, and challenges involved. You are not expected to become a technical expert (that's why your organization has a security team), but it is important that you understand the models, frameworks, and terminology. This will enable you to better understand your organization's risks and to communicate with both the security team and leadership about them.

A great way to start this process is to approach each of the different sub-teams within your security team. Learn how they operate and what their goals and key challenges are.

- Ask your SOC staff what they do and have them walk you through the data they analyze and what they look for.
- Talk to your Cyber Threat Intelligence Team about the most common tactics, tips, and procedures (TTPs) that cyber threat actors use to target your workforce. Don't know what a TTP is? Ask them and have them teach you about the MITRE ATT&CK® (and be prepared for a very excited but long response).
- Ask your Incident Response Team to walk you through the incident response playbook.

And don't forget to look at the career training roadmap listed in **Appendix B** of this report. It can help you develop your understanding and expertise in the security field. You don't have to become a technical cybersecurity expert, but the better you understand the security frameworks, models, and terms used, the more effective you will be.

Action Items for Technical Individuals

While highly technical individuals often understand cybersecurity concepts, technology, and controls, we often see them struggle to effectively engage and secure their workforce. Quite often, outreach, communications, and training initiatives by these experts are confusing and difficult to follow, or even overwhelming or intimidating for those with less expertise in the field. This is due to a cognitive bias called the "**Curse of Knowledge**," a cognitive bias where the more expertise someone has on a specific subject, the more difficult it is for them to effectively teach or communicate it. This can be especially true in the highly technical world of cybersecurity. Security awareness professionals with strong technical security backgrounds should be aware of their "curse of knowledge" and take measures to compensate for it.

Know Your Bias

If you are highly technical or have a strong security background, make sure you work with others to help craft your messaging. Your expertise is a plus, but as mentioned above, security concepts and technologies that are easy for you are most likely difficult, confusing, and intimidating for most others. Examples include how to use password managers or hovering over the link in an email – two very common solutions that many security professionals do not realize can be confusing to other people. One of the biggest challenges security professionals often face is simplifying security for their workforce. If you don't have someone to partner with, one option is to leverage AI to help simplify your workforce communications, security policies training, or tool roll-out announcements. Just ensure you are using AI solutions that protect the privacy of anything sensitive you may share.

Develop Communication and Engagement Skills

Be sure you have someone on your security awareness team who has the skills for effective communication and engagement. This can include training someone on your team, partnering with your Communications or Marketing departments to assist with all security-related communications and outreach, or even embedding one staff member from each department on your security team. In addition, consider acquiring the appropriate skills yourself to more effectively engage your workforce (see the Career Development section in **Appendix B**).

Open Ended Questions

New for this year, we asked the community a series of open-ended questions. This is what we learned.

A What is the single most effective action, approach, or campaign you've run to shift employee security behavior or culture this past year, and why?

The biggest theme we identified was the need for a continuous cadence of training throughout the year. You can have a big event, but if you are doing nothing else throughout the year, you are not making an impact. This correlates well with the data that the longer you sustain your program, the more likely you will have an impact. So, while Cybersecurity Awareness Month may be a fantastic opportunity to reach out to, engage, and secure your workforce, you need to be sure you are continuously informing your workforce the other eleven months of the year.

Simulations, especially phishing simulations, were extremely popular, with over 20% of the 1,180 submissions sharing the effective impact they had. There were multiple suggestions on how to make them successful, including monthly simulations, gamifying the simulations in a positive manner (focusing on enabling, recognition, and rewards for success), regular follow-ups in monthly newsletters, tips, and micro-videos.

B What was the most unexpected or surprising outcome you've learned while managing your security awareness program?

The key takeaway from this question was the need for focusing on the basics. Respondents emphasized how they underestimated how vulnerable employees were and how important it was to focus on the fundamentals. At times, we can feel it's important to cover all the latest attack methods or different risks, but we need to focus on the fewest set of key risks possible. The National Cybersecurity Alliance has their "Core Four" of fundamental behaviors, which are:

1. Strong Passwords and Password Managers
2. Multi-Factor Authentication
3. Detecting and Stopping Scams/ Social Engineering Attacks
4. Updating Your Systems and Devices

A less present, but insightful theme, is that soft skills matter more than expected. It was mentioned by some that the success of their program seemed less about the technical content and more about the program leader's ability to influence, inspire, and communicate effectively. We saw a surprising number of respondents admit they hadn't anticipated how much of the job would revolve around building relationships, marketing the program internally, and resolving conflicts.

C How can the security awareness community better help you?

By far, the biggest challenge emphasized here was lack of time and staff, which correlates to what we found earlier in top challenges. Practitioners are asking for practical playbooks, roadmaps, templates, and other actionable materials that can be used right away, anything that can save people time. This is once again why we are emphasizing the use of Generative AI, as it can be the dedicated intern you have always needed.

Second is resources specific to role-based or specialized training for departments like HR, Finance, or more technical, skills-based training for developers or IT admins.

D What frustrates you the most about our industry or community?

The most common frustration was lack of support and resources, not just from leadership, but from their own security teams who perceive awareness as a purely compliance or entertainment effort. Several quotes included:

"Leadership treats security as a checkbox, not a priority."

"Leadership's failure to invest in employee growth demotivates teams… without adequate support, employees become disengaged."

"Awareness isn't taken seriously in the security community."

"We're treated like HR-lite, not security professionals."

"We're seen as the soft, fluffy side of cyber."

This one we did not expect, but it makes sense: vendor overreach. Respondents expressed concern over buzzword-heavy solutions that confused the community, overpromised, and did not deliver.

E What didn't we ask this year that you'd like us to ask next year?

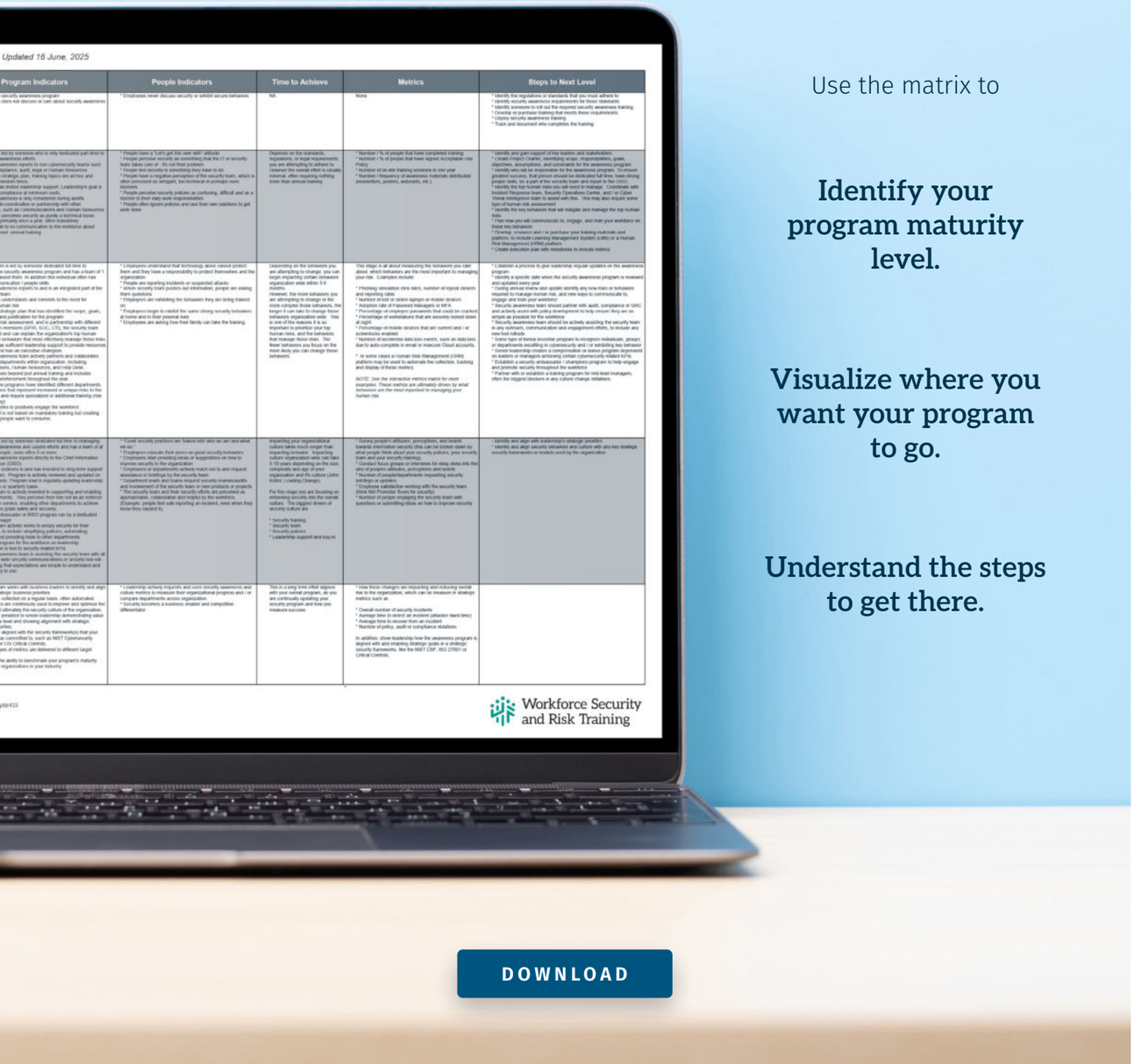
The biggest take away is people want to know what others are doing to prepare for AI, including how to securely use Generative AI, and how to prepare their workforce for AI deepfake-related scams and attacks.

A close second: the need for metrics, e.g., more information on how to measure behavior, culture, and program success. Many respondents wanted future surveys to address how organizations measure effectiveness—particularly behavioral outcomes rather than just compliance or participation.

"The success of their program seemed less about the technical content and more about the program leader's ability to influence, inspire, and communicate effectively."

Appendix A
Maturity Model Indicators Matrix

NOTE: A digital copy of the Maturity Model Indicators Matrix is available for download here.



Use the matrix to

Identify your program maturity level.

Visualize where you want your program to go.

Understand the steps to get there.

Appendix B
Career Development

Organizations and security leaders act on the fact that cybersecurity is no longer just a technical challenge, but also a human challenge. Security teams around the world are looking for trained professionals who specialize in the human side of cybersecurity.

If you are looking to get involved in this field or are already involved but want to develop your skills, career, and compensation, SANS Institute offers a clearly defined learning path to help you succeed.

Where to Start?

If you are new to information security or security awareness, the first class you will want to take is:

LDR433: Managing Human Risk

This three-day course lays the foundation of risk management, changing organizational behavior, and ultimately managing and measuring human risk. Course content is based on lessons learned from hundreds of security awareness programs from around the world. In addition, you will learn not only from your instructor, but from extensive interaction with your peers and gain access to the course digital download package. Finally, through a series of eight team labs and exercises, you will develop your own custom plan that you can implement as soon as you return to your organization. You also have the option to test for the **SANurity Aarenes Profesional (SAP)**, the industry's most recognized credential demonstrating expertise in managing human risk.

What Next?

If you don't have a strong security background, you may want to consider one of the following courses. Understanding security frameworks, models, and controls will not only help you better understand the risks and the behaviors that manage those risks but also enable you to more effectively partner with your security team and leadership. There are two different courses to consider at this stage in your career. Each has their advantages, depending on what you hope to achieve.

LDR512: Security Leadership Essentials For Managers

This course empowers you to become an effective security manager and get up to speed quickly on information security concepts and terminology. You don't just learn about security; you also learn how to manage security. This class does not do a deep technical dive into how different security technologies work but instead covers a wide range of security topics across the entire security stack. Areas covered include common security frameworks, security policies and governance, cloud, SOC, network architecture, detection and response, vulnerability management, and DevSecOps. In addition, this course is one of the three courses required for the **Transformational Cybesecurity Leader Triad**. If you are looking for an overview of cybersecurity from a management perspective, this is the course for you.

SEC301: Introduction to Cyber Security

This introductory course takes a technical, hands-on approach for those new to cybersecurity. It covers everything from core terminology to the basics of computer function and networks, security policies, password usage, cryptographic principles, network attacks and malware, wireless security, firewalls, and many other security technologies, web and browser security, backups, virtual machines, and cloud computing. All topics are covered at an introductory level. The hands-on, step-by-step teaching approach enables you to grasp all the information presented, even if some of the topics are new to you. You'll learn real-world cybersecurity fundamentals to serve as the foundation of your career skills and knowledge for years to come. In addition, this course offers numerous, hands-on technical labs ensuring you apply what you learn.

Not sure which one of these two courses to take?

Choose the **LD12** course if you are looking for a high-level or management perspective to the world of information security.

Choose the **SEC301** course if you want a more hands-on, technical introduction to the tools and technology of cybersecurity.

Choose the **SEC401** or **SEC501** courses if you already have some technical background but want to further develop your skills.

Intermediate Level

Once you have 2-4 years of experience and feel confident in the concepts of both cybersecurity and organizational behavior, here are some additional courses we recommended.

LDR521: Security Culture for Leaders

Cybersecurity is no longer just about technology; it is about people and ultimately culture. This course teaches leaders how to develop, maintain, and measure a strong security culture. Through hands-on, real-world instruction and a series of interactive labs and exercises, you will quickly learn how to embed cybersecurity into your organizational culture. In addition, on the last day, students compete as teams to see who can build the strongest security culture through an online simulation. Finally, this course is one of the three courses required for the **Transformational Cybesecurity Leader Triad**.

LDR553: Cyber Incident Management

This course walks leaders through preparing for and effectively managing an incident. One of the key skills for any organization to successfully manage an incident is their ability to communicate, both internally to the organization but also externally to regulators, government, customers, and the public. This is a perfect role for people with strong communication skills and specializing in the field of human security.

SEC504: Hacker Tools, Techniques, and Incident Handling

This course gives you insights and expertise into how cyber threat actors operate, including the tools they use, the techniques that give them access, and how you can detect and respond to these attacks. If you want to be introduced to the world of today's cyber attackers from a technical, hands-on perspective, this is the class for you.

Advanced Level

Once you have 5-7 years of experience and want to truly develop your security leadership skills, consider the **LD14** course. This course walks you through the strategic planning process and challenges today's CISOs face. Many people consider this the "CISO Course," as it helps develop new and experienced CISOs to become better security leaders and effective business communicators. By better understanding CISO challenges, priorities, and concerns, you can more effectively collaborate with senior leadership and communicate in their terms and language.

LDR514: Security Strategic Planning, Policy, and Leadership

This course gives you tools to become a security business leader who can build and execute strategic plans that resonate with other business executives, create an effective information security policy, and develop management and leadership skills to better lead, inspire, and motivate your teams. In addition, this course is one of the three courses required for the **Transformational Cybesecurity Leader Triad**.

Additional Free Resources

Beyond our courses, SANS Institute offers a variety of free resources to support you and your career in cybersecurity.

Webcasts

SANS hosts one-hour webcasts every week. Led by SANS Instructors and top security experts from around the world, these webcasts are a great way to stay current with the latest risks, threats, and controls.

Summits

SANS hosts one- or two-day Summits each month. Each summit focuses on a specific security field with experts from around the world, to include a summit every August focusing on the human side of cybersecurity. This is not only a great way to learn but also a chance to network with your peers. You can attend most Summits in-person or virtually.

Security Policy Templates

A comprehensive library of security policy templates to help you build or refine your own policies.

Posters and Cheat Sheets

Quick-reference guides for just about every field in cybersecurity.

OUCH! Newsletter

A monthly security awareness newsletter, written by a guest editor subject matter expert. Translated into 20 languages, share OUCH! with your family or friends, listen online to the OUCH! Podcast or distribute as part of your security awareness program.

Main Authors

The 2025 Security Awareness Report was developed by the community, for the community. The following key contributors led the development of the original survey and the creation of the final report.

Lance Spitzner
Technical Director
SANS Workforce Security & Risk Training

Chad Jones
Principal Data Analyst

Rachael Saffer
Director of Marketing
SANS Workforce Security & Risk Training

Advisory Board

For 2025, we formed an advisory board of twelve community members to help guide the survey development, data analysis, and report content. These volunteers were key in making this the most successful and useful Security Awareness report to date.

Autumn Johnson
Senior Manager, Security Awareness and Communications
Box

Beauregard Simmons
Consultant
Choice Strategies

Edel O'Brien
Information Security Awareness Manager
Central Bank of Ireland

Jatinder Bal
Cyber Security Awareness Manager
NSW Department of Customer Service

Jenna Esparza
Cyber Assurance Manager
Sandia National Laboratories

Jessica Burdette
Information Security Analyst
Guardian Credit Union

Lesley Swann
Human Risk Analyst
Baker Donelson

Markus Guenther
Senior Security Consultant
Temet

Melecia McLean
Security Training and Culture
TikTok

Michelle Stephens
Cybersecurity Education and Digital Content Specialist
Oak Ridge National Labs

Rachel Fetters
Ph.D. Behavior Analytics Portfolio Lead
Accenture

Thomas McMahon
Sr. Security Analyst
Lowe's

SANS

About SANS Workforce Security and Risk Training

SANS Workforce Security & Risk Training, a division of the SANS Institute, helps organizations manage human risk through focused, role-based education. Covering security awareness, risk fundamentals, and compliance topics, the program, built by experts that train the industry, supports cultural change and measurable behavior improvement. Training is threat-informed, aligned to real-world responsibilities, and structured to scale across teams - from end users to business leaders.

SANS Workforce, previously known as SANS Security Awareness, has trained over 6.5 million people, across 1300+ organizations around the world, whilst supporting Security Awareness Officers in their mission to simply and effectively build a best-in-class Security Awareness Program.

www.sans.org/for-organizations/workforce

Workforce Security and Risk Training