



SANS

**SECURITY
AWARENESS**

Embedding a Strong Security Culture

SANS 2024 Security Awareness Report®

Table of Contents

Executive Summary	3
Key Findings	3
Data From Around the World	4
Section 1: Benchmarking Your Program	6
Security Awareness Maturity Model ®	6
Benchmarking the Maturity of Your Program Against Others	8
Top Human Risks	9
Most Common Program Challenges? – Lack of Time and Staff	10
Name of Your Program	11
To Whom Do Security Awareness Programs Report?	12
Supporters and Blockers	12
How Strong Is Your Partnership with the Cybersecurity Team?	13
Section 2: Maturing Your Program	14
Action Items to Increase Team Size	16
Section 3: Compensation and Career	17
Compensation	17
What Is Your Job Title?	19
How Are You Feeling?	19
How to Grow Your Compensation and Career: Action Items for Non-Technical Individuals	20
How to Grow Your Compensation and Career: Action Items for Technical Individuals	21
Appendix A: Security Awareness Maturity Model® Indicators Matrix	22
Appendix B: Career Development	23
Where to Start?	23
Acknowledgements	25
About SANS Security Awareness	26

Executive Summary

People have become the primary attack vector for cyber threat actors around the world. As a result, humans rather than technology represent the greatest risk to organizations. Security awareness programs and the professionals who manage them are key to mitigating this human risk. This report is designed to enable organizations to better manage that risk and ultimately drive a strong security culture. The report is divided into three sections.

1 **Section 1** provides an overview of and data points on security awareness programs which can be used to benchmark your program against others in a variety of different areas.

2 **Section 2** provides data-driven steps to grow and mature your security awareness program.

3 **Section 3** provides security awareness professionals guidance on developing skills and growing their career.

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

In this report, the **term security awareness program** is used to describe a structured effort to engage, train, and secure your workforce and 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. And that's fine, because we are more concerned about enabling you to secure your workforce and your organization than the name of your program. So, wherever you see the term security awareness in this report, simply replace that term with the term or description that fits your organization.

Key Findings

Maturing Your Program

Similar to past years, 2024's survey found the most important variable that correlates with mature awareness programs is the size of your security awareness team. The larger your security awareness team, the more mature your program. This year's survey found that organizations that were effectively changing their workforce's behavior had a team of at least 1.8 dedicated full-time employees (FTEs). To go beyond behavior and embed a strong security culture with a strategic metrics framework requires at least 4.2 FTEs.

Growing Your Career

This report presents an in-depth analysis of compensation and pay rates, with the average salary of security awareness professionals being \$108,483 globally. We found considerable differences in pay based on region, background, industry, and program maturity.

Are You Happy?

We asked a new question this year; are people happy in their role? An overwhelming majority said yes (though many would like to continue their same role but in a different company).

Data From Around the World



This edition of the Security Awareness Report features the participation of over 1,000 security awareness practitioners from over 70 countries spanning the globe. 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

This section provides a framework and resources to identify the maturity of your organization's security awareness program, data you can use to benchmark your program, as well as risks and challenges that a security awareness program will face and must overcome to successfully cultivate a security-minded workforce.

Security Awareness Maturity Model®

To determine the maturity of awareness programs, we leverage the Security Awareness Maturity Model®. Established in 2011 through a coordinated effort by more than 200 awareness officers, the Security Awareness Maturity Model enables organizations to identify and benchmark the current maturity level of their Security Awareness Program and identify a path to improvement. The most mature programs not only change their workforce's behavior and culture, but also measure and demonstrate the program's value to leadership via a strategic metrics framework.



Figure 1

As outlined in the Security Awareness Maturity Model®, the different levels of programs are as follows:

Non-Existent

Program does not exist. Employees have no idea that they are a target, 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

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

Program identifies the top human risks to the organization and the behaviors that manage those risks. Program goes beyond just 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 and require additional or specialized role-based training. Content is communicated in an engaging and positive manner that encourages behavior change. As a result, people understand their role in cybersecurity, follow organizational policies, and exhibit key behaviors to secure the organization.

Long-Term Sustainment and Culture Change

Program has the processes, resources, and leadership support in place for long-term sustainment, including (at a minimum) an annual review and update of the program. As a result, the program is an established part of the organization's culture and is current and engaging. Program has gone beyond changing behavior and is changing the workforce's shared attitudes, perceptions, and beliefs about cybersecurity.

Strategic Metrics Framework

Program has a robust metrics framework aligned with and supporting the organization's mission and business goals. Program is no longer just measuring and reporting on changes in behavior and culture, but ultimately how these changes are reducing risk and enabling leadership to achieve their strategic priorities. As a result, the program is continuously improving and able to demonstrate return on investment (ROI).

This report includes a copy of the Security Awareness 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

What are the average maturity levels for security awareness programs, 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 very similar to 2023, showing little change since last year.

Select Your Program's Maturity Level Using the Security Awareness Maturity Model

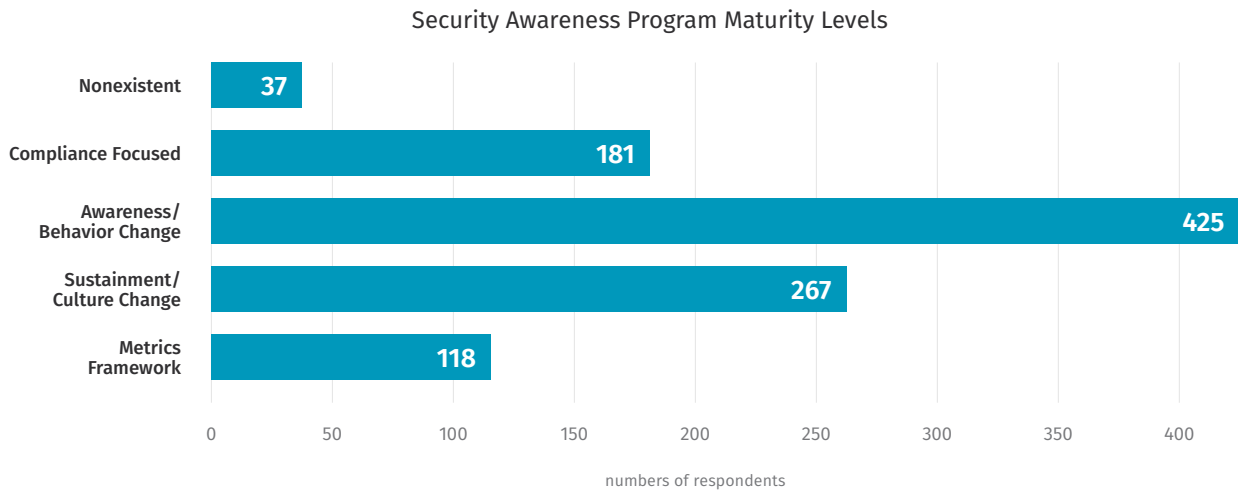


Figure 2

Top Human Risks: What are the top three concerns or human risks you are focusing on for 2024?

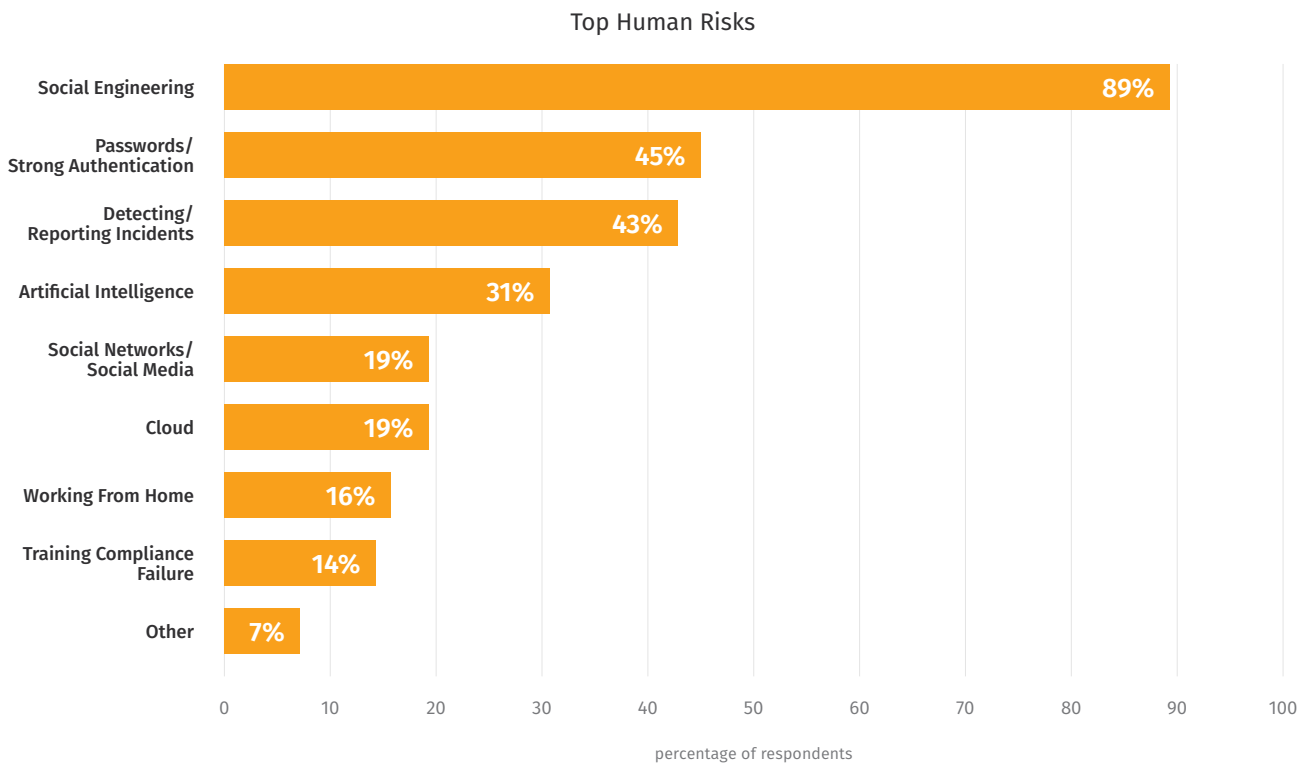


Figure 3

Top Human Risks

If security awareness programs are ultimately about managing human risks, which human risks are organizations most concerned about? Figure 3, below, shows that respondents cite one human related risk above all others as their top concern, Social Engineering (Phishing/Vishing/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 see a rise in both numbers and sophistication in smishing and vishing. This is in part as organizations are getting better at detecting and stopping phishing attacks, but also because fewer organizations have control over and visibility into employees' mobile devices. Social engineering attacks were 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 in any language or voice they want.

2 Passwords/Authentication

How people authenticate and manage their passwords was a top risk, but we were expecting this risk to be ranked closer to social engineering. One reason we believe passwords are perceived as a lower risk is the active deployment of numerous authentication controls such as identity access management (IAM), single sign-on (SSO), and multi-factor authentication (MFA). Authentication is a primary attack vector, and as a result, organizations are investing heavily in controls to enable strong authentication.

3 Detection/Reporting

Detection and reporting tied with passwords/authentication in the risk ranking. Detection/reporting as a top concern is a positive development, as it implies organizations are going beyond just the human firewall (prevention) to developing the human sensor (detection/response) which helps organizations reduce attacker dwell time. The key to developing a human sensor network is not only training your workforce on what to look for, but also making it as simple as possible to report a suspected incident. In addition, your security culture is key. How likely are people to report an incident if they know they caused it? If you have a highly trusted security culture, people are far more likely to report. If you have a toxic or punitive security culture, people are far more likely to hide and not report an incident they caused.

4 Artificial Intelligence

This is the first year AI popped up as a risk, and unsurprisingly so. The issue we see with AI is not that it is inherently vulnerable or unsafe, it's that AI is so new that organizations are struggling to figure out how to use it and the risks, policies, and controls that must be in place to manage those risks. For many organizations, addressing the risks of AI will be similar to cloud-based software as a service (SaaS) models. Until organizations address these issues, cybersecurity teams will struggle to figure out what to tell the workforce and how to train them.

Most Common Program Challenges? – Lack of Time and Staff

In addition to understanding the cyber-based threats, it is important to understand the most common challenges in building and managing an effective security awareness program. This year it was simple, the number one challenge is lack of time and people. Awareness practitioners have too much to do and too few resources to do it. This makes perfect sense. Securing your workforce is ultimately a people problem and requires people as part of the solution. It takes time for a security awareness team to build trust and partnerships with other departments; work with the cybersecurity team identifying top workforce and role-based risks; communicate to, engage with, and train the workforce; track and measure impact; coordinate with leadership; and numerous other actions. When it comes to securing your workforce and building a strong security culture, you cannot simply purchase a tool and solve your problems. It takes people to secure people and ultimately drive culture change.

Program Challenges: What do you feel are the two biggest challenges limiting your ability to succeed?

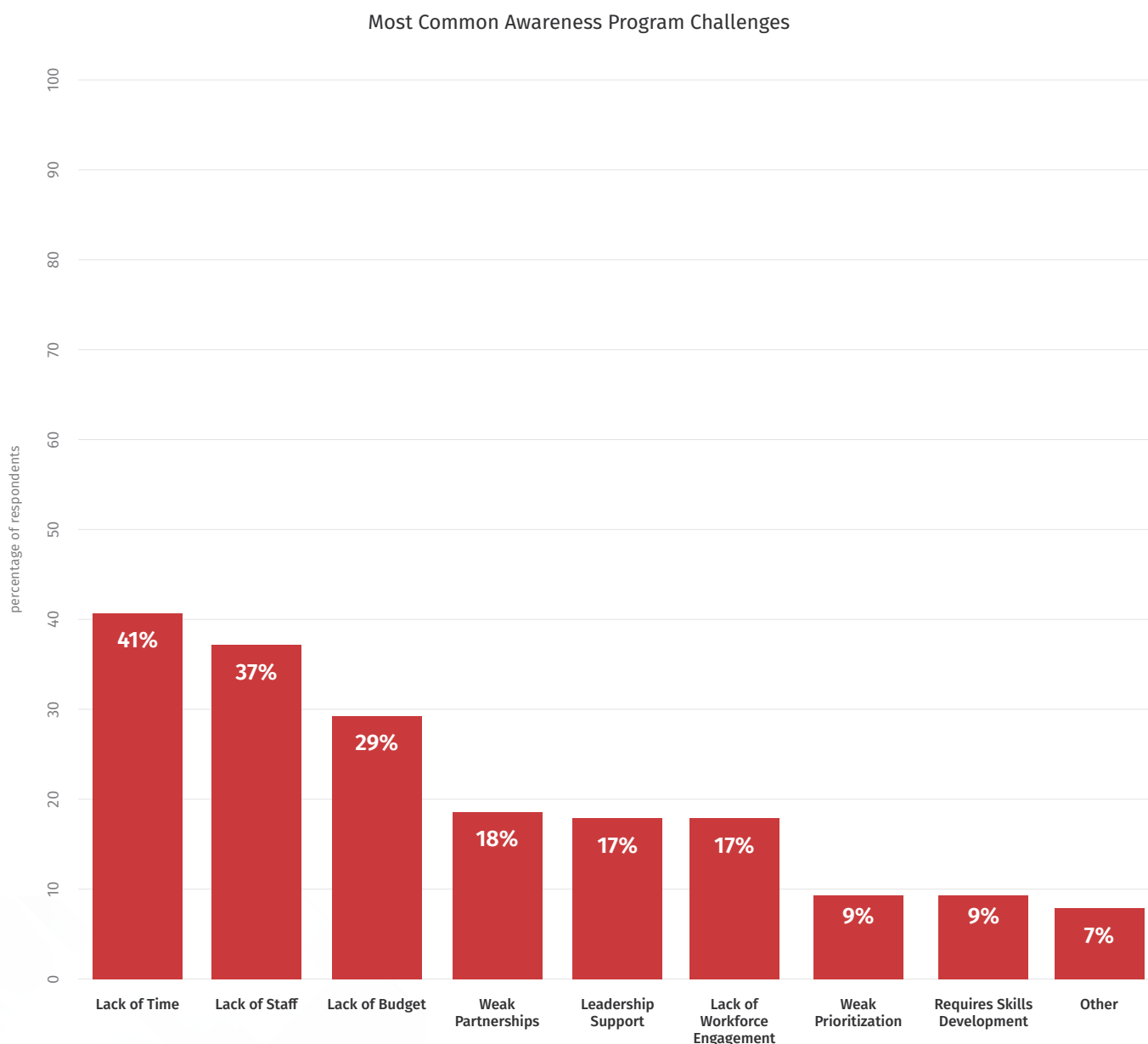


Figure 4

Name of Your Program

We asked people what they call their awareness program. We find that the name of an awareness program can often impact various elements of that program, such as who the program lead reports to as well as the program's budget and priorities, etc. We found that awareness program names varied widely. Names included everything from "Cyber Safety" to "Organizational Change Management." We struggled to determine the most common names. So, we instead identified the most common words used in the naming of the programs. Figure 3, below, is a word cloud of the top ten words most used when naming an awareness program. We were happy to see that the words "legal," "privacy," and "compliance" did not show up in the top ten. While these are important goals, they often distract from the mission of securing your workforce. Long story short, we recommend you not be too worried about the name of your program as long as it works for you.



To Whom Do Security Awareness Programs Report?

We want to know which department or teams security awareness professionals report to. Which department the security awareness team reports to can have a huge impact on its ability to secure the workforce. Our concern is teams that report to legal, audit, or training may be focused only on compliance, i.e., checking the box. These teams are often siloed from and do not interact with the cybersecurity team. The ability to actively partner with the cybersecurity team is critical to managing human risk. The cybersecurity team is not only the primary source for identifying and prioritizing your top human risks, but is also commonly involved in policy development, security tool rollouts, and communicating to the workforce on security matters. The more the security awareness team integrates and partners with the cybersecurity team on all these activities, the more effectively they can secure your workforce. In fact, security awareness should be just one part of the overall risk management strategy of every chief information security officer (CISO). Similar to years past, we see the vast majority of security awareness teams reporting to the cybersecurity or information technology (IT) teams.

Reporting: What department best describes where you report to?

Top Ten Departments the Security Awareness Team Reports

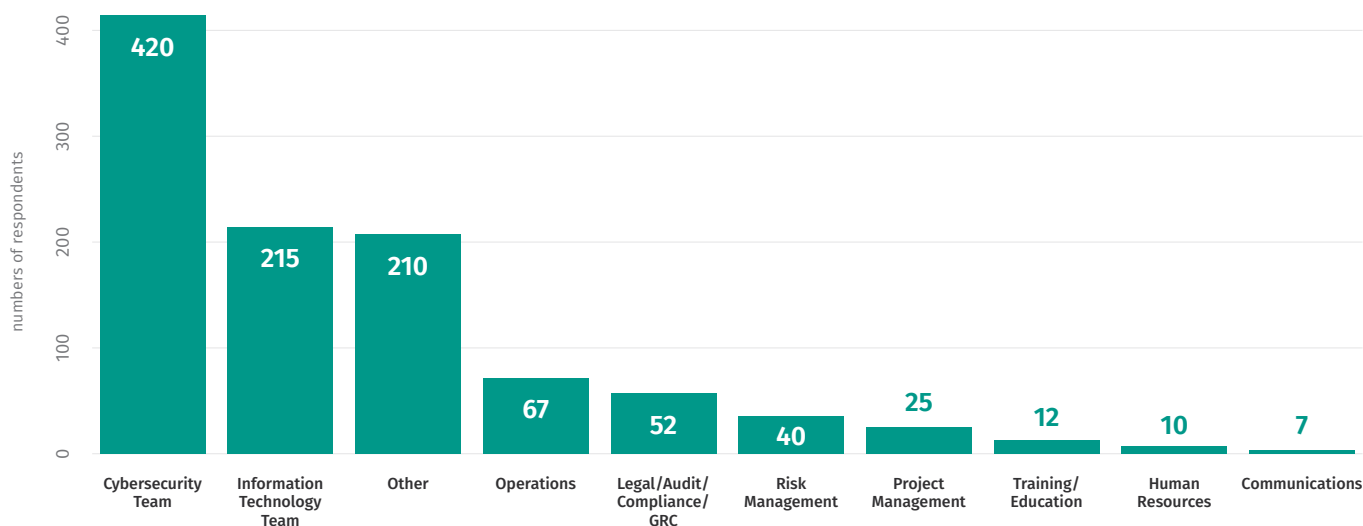


Figure 5

Supporters and Blockers

One of the survey's objectives was to better understand the top supporters and blockers of security awareness programs. As in past years, the top supporters were the IT and information security departments. This makes sense as security awareness programs are often run by or directly support these teams' concerns or initiatives. However, for 2024, there is a new blocker. In years past, the two most common departmental blockers were Finance and Operations, and while they topped the list this year, a new addition to the list of options, mid-level managers, beat them all. Mid-level managers manage teams, focus on ensuring team goals are met, and often perceive the cybersecurity team as a blocker. This can be a challenging group to reach as there is no direct connection between them and the cybersecurity team. You may consider a special 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.

Security Awareness Program Blockers

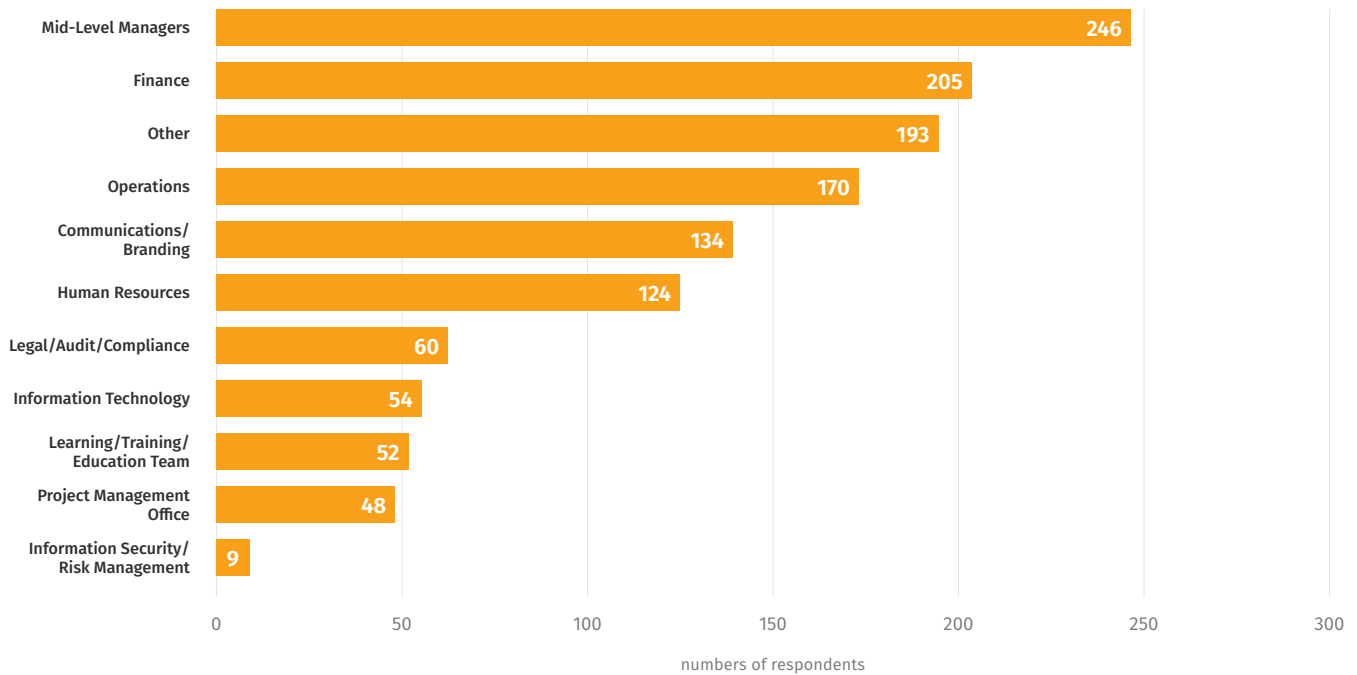


Figure 6

How Strong Is Your Partnership with the Cybersecurity Team?

Following the question about supports and blockers, we asked security awareness professionals about the strength of their partnerships with the cybersecurity team. We were both surprised and happy to see just how strong those partnerships are. Every security awareness team should be working with their security operations center (SOC), cyber threat intelligence team, incident response team, and others. This helps ensure the security awareness team is not only using data to drive what risks they focus on and how, but that they can also partner with and help the cybersecurity team in its other security related activities, including communications, policy development, and tool roll-out. These strong partnerships are key to going beyond simply changing your workforce's behaviors and moving toward building a strong security culture.

Security Team: How strong is your relationship with the information security team?
Do you actively partner with them on understanding threats, identifying human risks, helping with outbound communications, or interacting with the workforce?

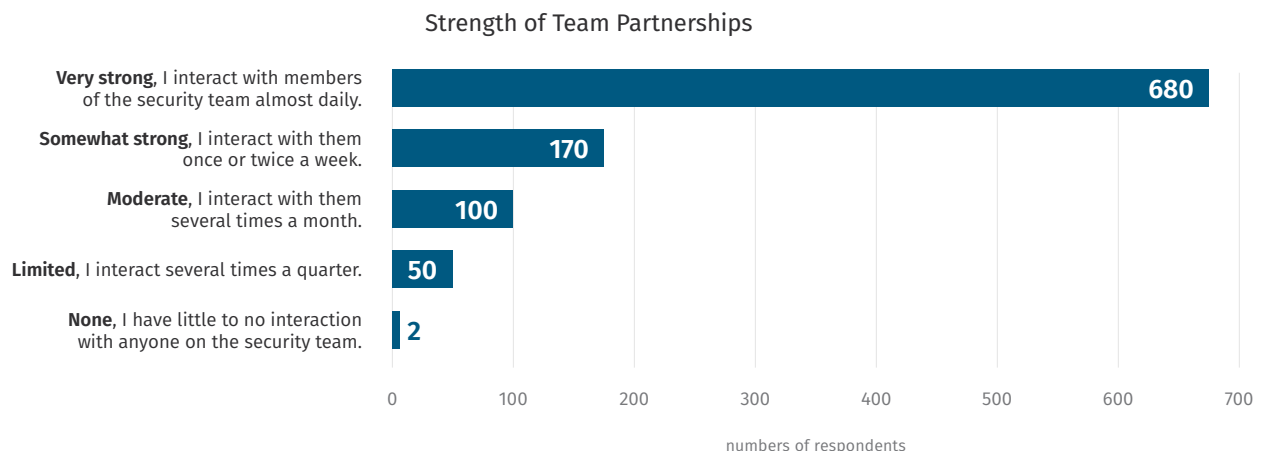


Figure 7

Section 2

Maturing Your Program

Now that you have a better understanding of your security awareness program's maturity and the data you can use to benchmark your program, we need to identify the key drivers of program maturity and what you can do based on that information. Once again, this year's survey found a strong correlation between the size of a security awareness 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 FTE, we mean individuals who spend 75% or more of their time on security awareness.

This finding makes sense: managing human risk is a "people problem," so it requires people to drive the solution. Organizations with the largest security awareness teams are able to 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 secure their workforce. To have an impact, most programs need at least a combined effort of 1.8 FTEs to effectively change behavior, this means at least 1.8 people who focus 75% or more of their time on the program. The most mature security awareness programs on average have at least 4 combined FTEs dedicated to or helping manage the program. You will notice these numbers have gone down from last year, which is attributed to the new wording of the question. We are no longer asking how many people contribute to your program. Instead, we narrowed the scope of the question by asking how many people dedicate 75% or more of their time to the program. We felt this was a more accurate way of measuring the impact of an awareness program's FTE count. Either way the question is framed, for the past five years the results have remained consistent. The more people dedicated to or working on a security program, the more mature the program.

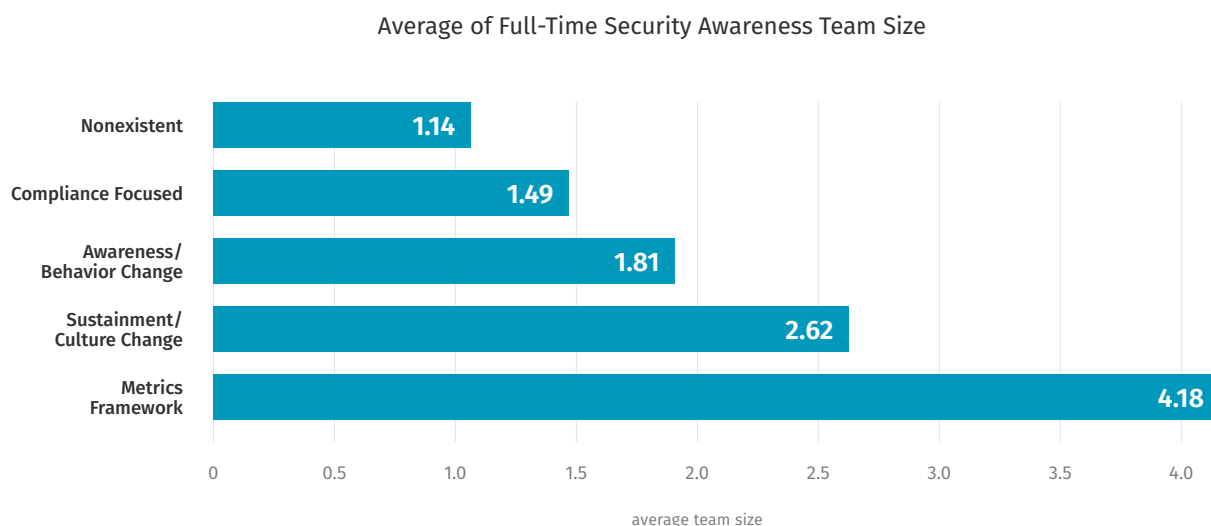


Figure 8

We are often asked, "How many FTEs do I need?" Unfortunately, there is no simple answer. We examined various approaches to quantify an answer, however, we found that because every organization has different goals, mission, and risk tolerance, any correlations were tenuous at best. We found no connection between number of FTEs and number of employees. Further, we found that it did not matter whether a company had 5,000 or 250,000 employees. In many ways it takes the same effort to run monthly phishing simulations, launch and track computer-based training, create and push email, develop infographics, work with the cybersecurity team to identify top risks, and partner with the Communications or Human Resources departments.

One challenge large organizations often face is scaling their security awareness program. Reaching large numbers of people in different regions, roles, cultures, or languages is especially difficult. So, the larger your organization, the larger your security awareness team must be. Conversely, even relatively small companies (approximately 1,000 employees) still need a baseline of at least 1.5 FTEs dedicated to the security awareness team. If you are looking for a more linear approach to sizing your security awareness team, consider a 10:1 ratio, i.e., for every ten people on your cybersecurity team, delegate one person to focus on the human side of cybersecurity.

Compare, if you will, the two different ways a security awareness officer role could be described. **Example 1** is how most awareness officers describe their job, in terms of what they do, while **example 2** is more risk focused. The actions of each example effectively engage the workforce. The problem is one of perception. Leadership may perceive the role described in the first example as a job in digital entertainment. Then notice the second example. Its description is risk focused and therefore more likely to connect with and gain the support of leadership.

Example 1

Hi, my name is Renan, and I'm the Security Awareness Officer. I'm the person managing all of our security training activities. For example, I co-led the newly released security awareness micro-videos and posters as well as last month's guest speaker symposium. 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 the key drivers in over 75% of all security incidents in the past year? I work with the cybersecurity team to engage, train, and change our workforce's behaviors so they act in a far more secure manner. Our goal is to dramatically reduce our workforce's risk, increasing our ability to securely make the most of technology, including adopting AI as part of our new innovation initiative.



Action Items to Increase Team Size

1 Talk to Leadership (and Your Cybersecurity Team) in Terms of Risk

Leadership and cybersecurity 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, it is important to focus on and speak in terms of risk. Human risk is far more likely to align with most organizations' strategic security priorities, gain leadership buy-in, and resonate with a cybersecurity team. Help the members of your cybersecurity team understand how you can help and work with them to identify the top human risks and the key behaviors that manage those risks. Demonstrate how effective communications, training, and engagement is changing those key behaviors and ultimately building a strong security culture. Partner your SOC, incident response, and cyber threat intelligence teams to better understand not only what they do, but also how you can help them solve their human-risk-related challenges.

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 culture) vulnerable. A simple but effective way to demonstrate this is to count how many people are on your cybersecurity team then count how many of them are dedicated to the technology side versus the human side. We often see 50-person cybersecurity teams with only one person 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 Break Down Your Needs

Document all the different steps and initiatives you need to undertake to make the program effective. One approach is to align initiatives with 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? Once aligned, identify and document the number of FTEs needed for each of these efforts, and at the same time demonstrate the value of those efforts, then 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.

4 Leverage AI

If you don't have the budget to hire additional resources, leverage generative AI (GenAI). In many ways, GenAI can act as an intern or subject matter expert to help with all of your needs, from creating emails and content to data or risk analysis. You and your team are still responsible for the final results, but GenAI is becoming extremely powerful in giving you back your most precious resource – time. [Learn more how to leverage GenAI in managing human risk in this series of blog posts.](#)

5 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, and 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.

Section 3

Compensation and Career

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

Compensation

Similar to past years, we wanted to know the average salaries for security awareness practitioners. The average annual salary for a security awareness role in 2024 was \$108,483. This is a \$10,000 increase from 2023. Keep in mind this draws on responses from all industries and regions. In terms of geography, North America has the highest average annual salary at \$129,905.

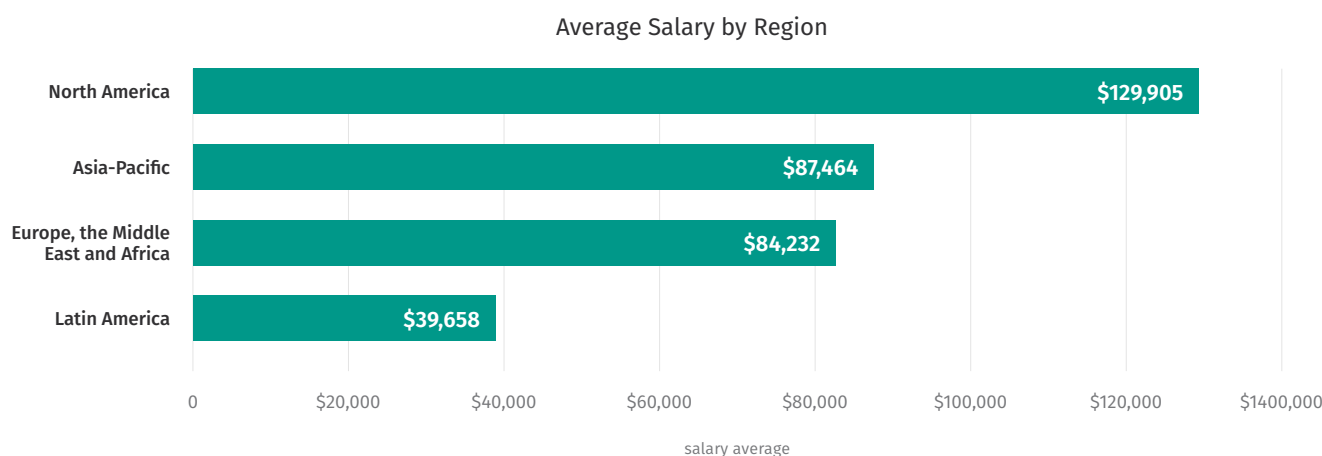


Figure 9

We looked at a variety of other variables to determine which had the greatest impact on pay. The two biggest variables seen in 2024 were **industry** and **background**. The highest-paying industries were healthcare, pharma, real estate, and consumer goods, averaging \$125,000/yr. The utilities and finance sectors were close seconds. The industries paying the least were metals, mining, accommodation, and automotive, averaging \$70,000/yr.

We saw even more dramatic numbers based on background. The highest paid people were those with backgrounds that included technical skills like software developer, IT administrator, and information security, at roughly \$115,000/yr. Surprisingly, those with legal and compliance backgrounds were the top earners in terms of compensation at \$130,000/yr.

The lowest compensated backgrounds were marketing, graphic design, and human resources at \$65,000. Once again, these numbers are based on a global data set and not adjusted for region.

Finally, and unsurprisingly, the maturity of your program can be a big indicator of your pay. Individuals who reported the maturity level of their program at the highest stage (Stage 5, Strategic Metrics Framework) were on average paid twice as much as people reporting that they did not have an awareness program or were just starting one. This makes sense as organizations that have the highest maturity levels are most likely the organizations willing to invest in the people to run, monitor, and maintain a security awareness program.

Average Salary by Professional Background

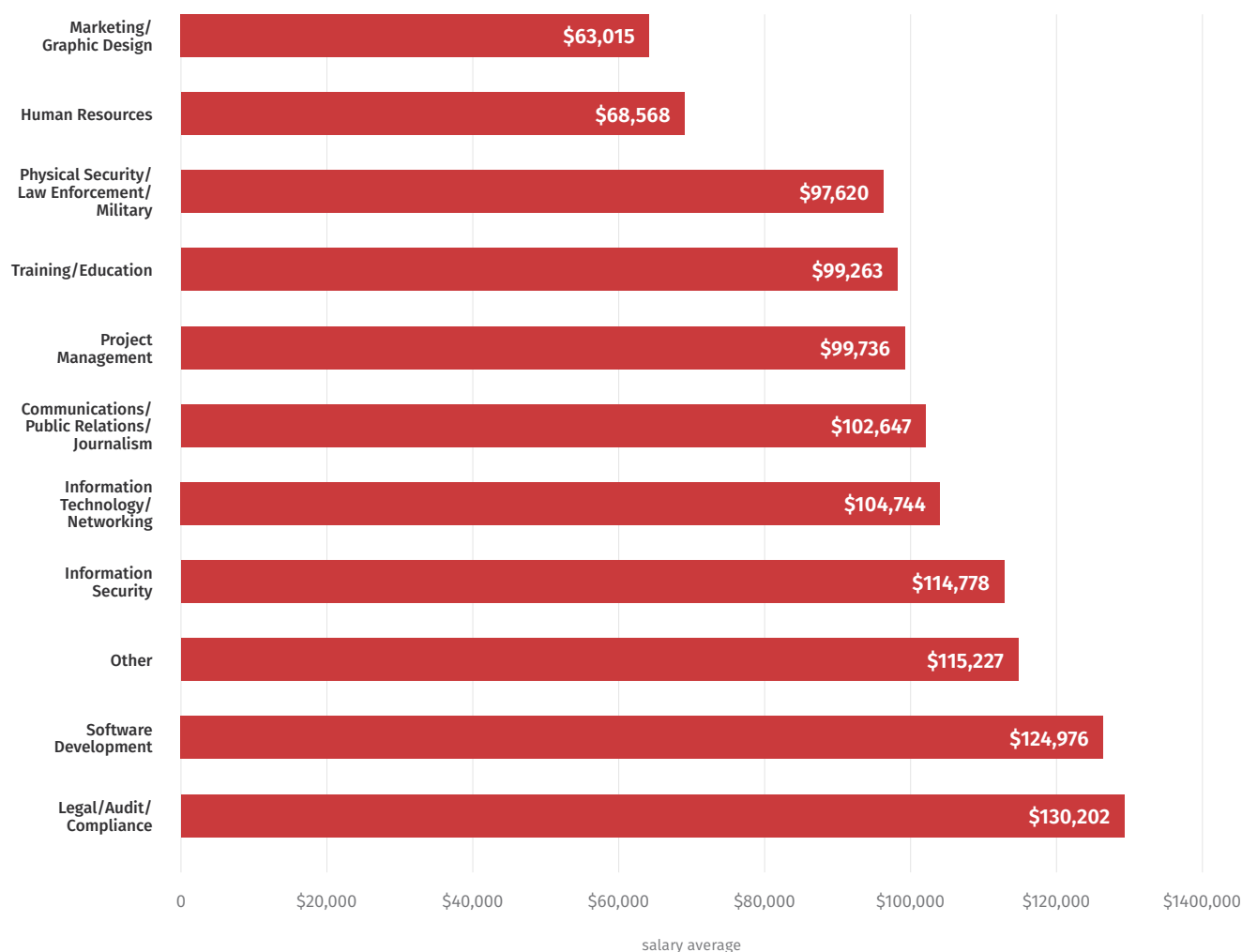


Figure 10

Average Salary by Program Maturity

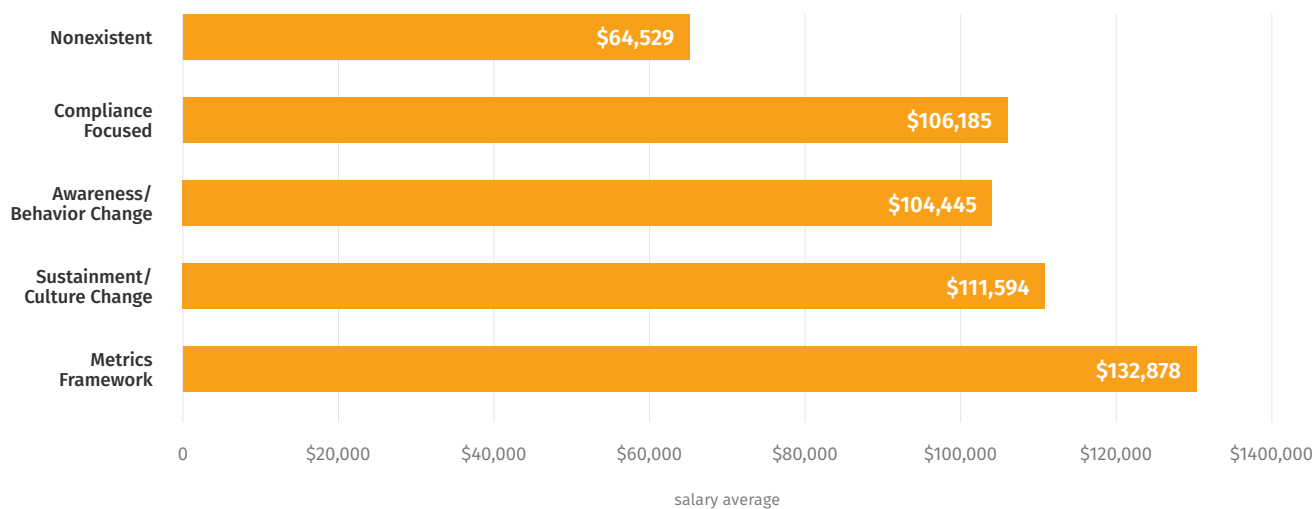


Figure 11

What Is Your Job Title?

This question is important in helping ascertain the roles involved in security awareness programs and how many job titles reflect a human focused role. Out of the 976 total job titles provided, 15% (147) were human related. Unsurprisingly, the terms **awareness** and **training** appeared most in the job titles. It will be interesting to track over time if and what other titles become more popular.

Most Common Security Awareness Job Titles

Keyword	Count	Examples
Awareness	75	Security Awareness and Training, Global Cybersecurity Awareness Leader, Head of Information Security Awareness
Training	27	Security Awareness and Training, Security Training Specialist, Training and Development Lead in Security
Culture	19	Security Awareness and Culture Lead, Security Manager, Security Culture Coordinator
Education	9	Principal Corporate Security Education and Awareness Manager, Education and Awareness Coordinator, Security Education Specialist
Engagement	5	Security Engagement and Awareness Lead, Security Engagement Specialist, Engagement Manager for IT Security
Human Risk	5	Human Risk Analyst, Cyber and Human Risk Manager, Human Risk and Security Advisor
Communication	4	Senior Manager Security Awareness and Communication, Communication and Information Security Officer, IT Security Communication Strategist
Influence	2	Associate Security Analyst (with an influence on security policies), Influencer of IT Security
Behavior	1	Cyberbehavior Engineer

Table 1

How Are You Feeling?

This may sound like an odd question, but it is important. We want to track peoples' happiness in the security awareness field and if those numbers go up or down over time. To be honest, we were surprised at just how much people enjoy the human side of cybersecurity. Nearly 90% of security awareness practitioners want to stay in the field, however, a substantial 30% of them are looking for the same or similar role at a new company. Less than 10% want to leave the field or cybersecurity altogether. In the future, we may expand this line of questioning to ask what people love about their job or why they want to change their job.

Security Awareness Professionals' Job Satisfaction

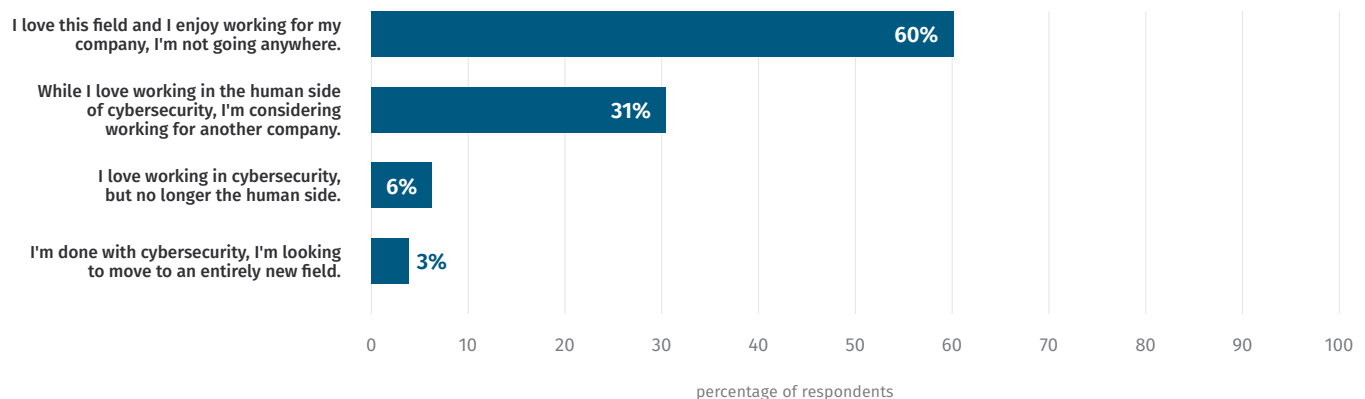


Figure 12

How to Grow Your Compensation and Career: Action Items for Non-Technical Individuals

1 Expand Your Role

Security awareness 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 much more. First, as discussed in the previous section, ensure that leadership understands the importance and focus of your role. In addition, work with the cybersecurity team to improve and simplify communications with your workforce, help manage security tool rollouts (such as multi-factor authentication), and create policies that are easier for people to understand and follow. Partner with the Incident Response Team to assist with any internal or external incident communications. Work with senior leadership on table-top exercises to strengthen incident response capabilities. You have many opportunities to expand your value to the cybersecurity team and leadership, so make the most of it!

2 Develop Your Security Skills

Develop your understanding of security fundamentals so 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 cybersecurity team), but it is important that you have an understanding of the models, frameworks, and terminology. This will enable you to better understand your organization's risks and communicate about them with both the cybersecurity team and leadership. A great way to start this process is to approach each of the different sub-teams within your cybersecurity team. Learn how they operate, their goals, and key challenges. Ask your SOC staff what they do and have them walk you through the data they analyze and what they look for. Ask your Cyber Threat Intelligence Team what the most common tactics, techniques, and procedures (TTPs) are 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](#) model (and be prepared for a very excited but long response). Ask your Incident Response Team to walk you through the incident response playbook. Finally, take a 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. The better you understand the security frameworks, models, and terms used, the more effective you will be.

How to Grow Your Compensation and Career: 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**,” which states that the more expertise someone has on a specific subject, the more likely they are to expect others to know as much as they do on the subject. This cognitive bias can make it difficult for an expert to effectively teach or communicate a subject in which they excel. 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.

1 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 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 others. One of the biggest challenges security professionals often face is making security simple for their workforce. If you don’t have someone to partner with, one option is to leverage AI to help you simplify workforce communications, security policies training, or tool roll-out announcements. Always be sure you protect the privacy of sensitive data when using AI solutions.

2 Develop Communication and Engagement Skills

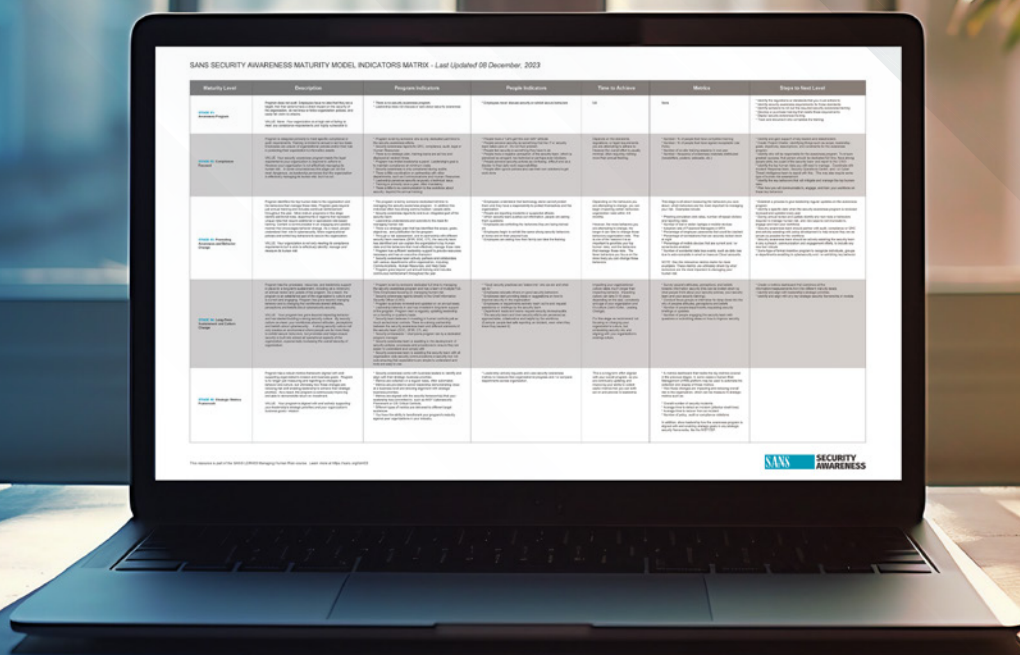
Be sure someone on your security awareness team has effective communication and engagement skills. This includes training your team, partnering with communications or marketing to assist with security-related communications and outreach, or even embedding a staff member from those departments on your cybersecurity team. In addition, consider acquiring your own skills to effectively engage your workforce, (see the Career Development section in **Appendix B**).

Appendix A

Security Awareness Maturity Model®

Indicators Matrix

NOTE: You can download a digital copy of the [Maturity Model Indicator Matrix here](#). Use the matrix to identify the current state of your program's maturity, its desired future state, and the steps that must be taken to get there.



The image shows a laptop on a wooden desk, displaying the SANS Security Awareness Maturity Model Indicators Matrix. The background features a large window with a grid pattern, through which a cityscape is visible. A potted plant is on the right side of the desk. The laptop screen shows a table with the following columns: Maturity Level, Description, Program Indicators, People Indicators, Tools to Address, Metrics, and Steps to Next Level. The table is divided into five rows, each representing a maturity level: Initial, Basic, Intermediate, Advanced, and Expert. Each row contains detailed descriptions, indicators, and steps for achieving that level of maturity.

Maturity Level	Description	Program Indicators	People Indicators	Tools to Address	Metrics	Steps to Next Level
Initial	Basic security awareness training is provided to all employees.	Security awareness training is mandatory for all employees.	Security awareness training is mandatory for all employees.	Security awareness training is mandatory for all employees.	Security awareness training is mandatory for all employees.	Security awareness training is mandatory for all employees.
Basic	Security awareness training is provided to all employees, and the training is tailored to the employee's role.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role.
Intermediate	Security awareness training is provided to all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations.
Advanced	Security awareness training is provided to all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.
Expert	Security awareness training is provided to all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.	Security awareness training is mandatory for all employees, and the training is tailored to the employee's role. The training is ongoing and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations. The training is also tailored to the employee's role and includes phishing simulations.

[DOWNLOAD](#)

Appendix B

Career Development

Organizations and security leaders know for a fact that cybersecurity is no longer a technical challenge alone, but a human challenge as well. Cybersecurity teams around the world are looking for trained professionals specializing in the human side of cybersecurity. Whether you are interested in a career in security awareness or currently in the field and want to develop your skills, career, and compensation, SANS Institute offers several key introductory, intermediate, and advanced level courses to accelerate your career growth.

Where to Start?

If you are new to the world of information security and/or security awareness, the very first class you should take is LDR433.

LDR433: Managing Human Risk

This three-day class lays the foundation of risk management, changing organization 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. You will learn from your instructor as well as through extensive interactions with your peers. Finally, through a series of eight team labs and exercises, you will develop your own custom plan you can implement as soon as you return to your organization. You also have the option to test for the [SANS Security Awareness Professional \(SSAP\)](#) certification, the industry's most recognized credential demonstrating expertise in managing human risk.

What Next?

Understanding security frameworks, models, and controls will help you better understand the risks as well as the behaviors that manage those risks and enable you to more effectively partner with your cybersecurity team and leadership. There are two introductory-level five-day courses to consider at this stage in your career. Each has their advantages, depending on what you hope to achieve. If you do not have a strong security background you may want to consider one of the following classes.

Introductory Level

The following courses are recommended whether you're new to a cybersecurity or cyber manager role.

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 covers a wide range of security topics across the entire security stack without diving too deep into the technical details of security technologies. Areas covered include common security frameworks, security policies and governance, cloud, SOC, network architecture, detection and response, vulnerability management, and DevSecOps. In addition, this is one of three courses required for the Transformational Cybersecurity Leader Triad. If you are looking for an overview of cybersecurity from a management perspective, this course is for you.

SEC301: Introduction to Cyber Security

This course takes a technical, hands-on approach for those new to cybersecurity. SEC301 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. This course offers numerous, hands-on technical labs ensuring you apply what you learn.

Not sure which one of these two courses to take? If you are looking for a high-level or management perspective into the world of information security, [LDR512](#) is the recommended course. If you want a hands-on, technical introduction to the tools and technology of cybersecurity, [SEC301](#) is the best course to take. If you have some technical background but want to develop it further, consider [SEC401: Security Essentials - Network, Endpoint](#).

Still not sure which course is right for you? Contact a [SANS Student Success Representative](#) today.

Intermediate Level

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

LDR521: Security Culture for Leaders

Cybersecurity is no longer just about technology, it is also about people and ultimately culture. This five-day course teaches leaders how to develop, maintain and measure a strong cybersecurity 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. This is one of three courses required for the [Transformational Cybersecurity Leader Triad](#).

LDR553: Cyber Incident Management

This five-day 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 course for people with strong communication skills who specialize in the field of human security.

SEC504: Hacker Tools, Techniques, and Incident Handling

This six-day course provides insights and expertise into how cyber threat actors operate, to include the tools they use, the techniques that give them access, and how to 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 course for you.

Advanced Level

Once you have 5-7 years of experience and want to truly develop your cybersecurity leadership skills, consider [LDR514](#). 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 into better security leaders and more 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 the tools a security business leader needs to 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. This is one of three courses required for the [Transformational Cybersecurity Leader Triad](#).

Additional Free Resources

In addition to training courses, SANS Institute offers a variety of free resources designed to support your professional development and enhance your cybersecurity skills. Explore these valuable tools and opportunities to stay updated and connected in the ever-evolving field of cybersecurity:

Webcasts

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

Summits

SANS hosts monthly one- or two-day conferences. Similar to webcasts, each Summit hosts experts from around the world to speak on specific security issues. This is a great way to learn and network with your peers. Most summits can be attended in-person or virtually.

Security Policy Templates

SANS has a library of security policy templates which you can use to build your own policies.

Posters and Cheat Sheets

SANS's quick reference guides cover almost every field in cybersecurity.

OUCH! Newsletter

SANS's monthly OUCH! security awareness newsletter focuses on a new topic each month and is led by a guest editor subject matter expert. Translated into twenty languages, share OUCH! with your family, friends, and/or as part of your security awareness program.

Acknowledgements

The 2024 Security Awareness Report was developed by and for the community, in partnership with SANS Institute. The following key contributors produced this report.

Lance Spitzner

Lance has over 25 years of security experience in cyber threat research, security architecture, and security culture and training. He helped pioneer the fields of deception and cyber intelligence with his creation of honeynets and founding of the Honeynet Project. In addition, Lance has published three security books, consulted in over 25 countries and helped over 350 organizations build security behavior and culture programs to manage their human risk. Lance is the author of and an instructor for **LDR433: Managing Human Risk** and **LDR521: Security Culture for Leaders**. Lance is a frequent speaker and works on numerous community projects. Before information security, Mr. Spitzner served as an armor officer in the Army's Rapid Deployment Force and earned his MBA from the University of Illinois.

Chad Jones

Chad is a seasoned data analytics professional with experience in customer success, sales, and business operations within technology and technology-enabled sectors. His diverse background has equipped him with a deep understanding of client success, value creation, and the ability to establish ROI through successful outcomes. With a strong focus on SaaS and cybersecurity industries, Chad's expertise in leveraging data for insightful decision-making sets him apart.





About SANS Security Awareness

SANS Security Awareness, a division of SANS Institute, provides organizations with a comprehensive security awareness solution that enables them to easily and effectively manage their human cybersecurity risk. SANS Security Awareness has worked with more than 1,300 organizations and trained more than 6.5 million people worldwide. The program offers globally relevant and expert-authored tools and training to help individuals shield their organization from attacks, as well as a fleet of savvy guides and resources to guide their work every step of the way.

To learn more, visit
www.sans.org/security-awareness-training