SANS 2023 SECURITY AWARENESS REPORT®

MANAGING HUMAN RISK

SANS SECURITY AWARENESS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

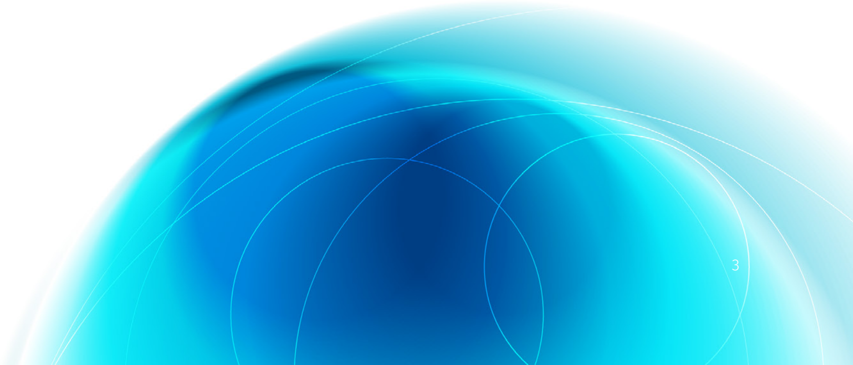
People have become the primary attack vector for cyber threat actors around the world, humans rather than technology represent the greatest risk to organizations. Security Awareness Programs, and the professionals who manage them, are key to mitigating that human risk. This report is divided into three sections. The first section provides an overview of our industry and enables you to benchmark your program against others in a variety of different areas. The second section analyzes how to grow and mature your security awareness program. It provides not only data from the survey and what the data means, but also actionable steps you can take to better manage your organization's human risk. The third section provides actionable steps on how security awareness professionals can develop their skills and grow their career. This report does not have to be read straight through, feel free to jump to the sections that interest you the most.

Finally, a word about terms. In this report, the term security awareness is used to describe a structured effort to engage, train, and secure your workforce with the goal of managing human risk. 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, and 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 manage human risk. Wherever you see the term security awareness in the report, simply replace that term with whatever term or description you and your organization use.

KEY FINDINGS

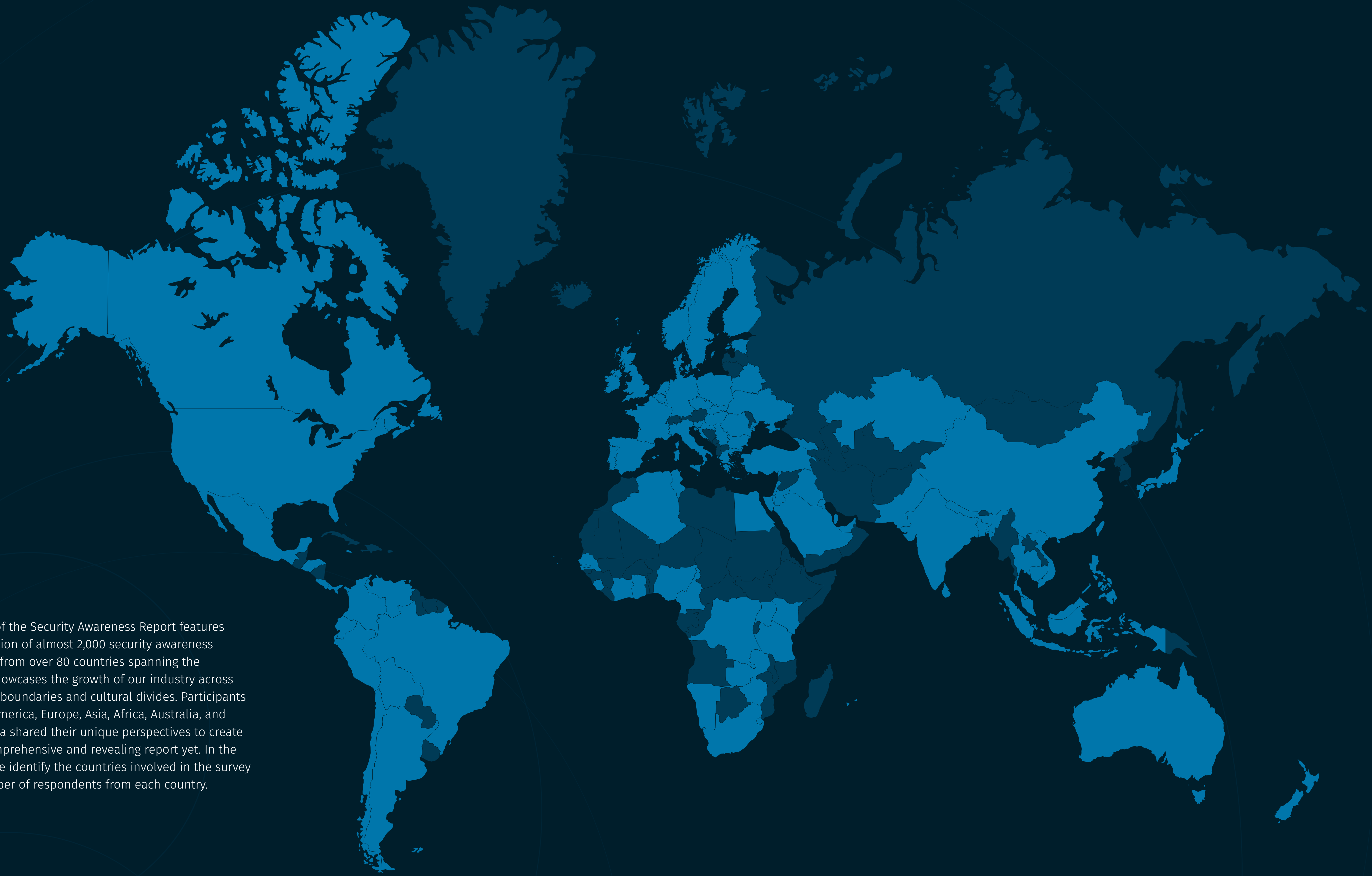
MATURING YOUR PROGRAM
Similar to the past three years, this year's survey found that the top two variables that correlate with mature awareness programs are leadership support and the size of your Security Awareness Team. The stronger your leadership support, and the more full-time employees (FTEs) you have supporting your awareness program, the more mature your program is likely to be. This year's survey found that organizations that were effectively changing behavior had a team of at least three FTEs. Organizations that went beyond behavior change and were effectively building a strong security culture, and that had a strategic metrics framework to measure that change, on average had a team of at least six FTEs.

GROWING YOUR CAREER
This year's report presents a far more in-depth analysis of compensation and pay rates, including by location, industry, and specialization. In contrast to past years, we found for the first time that people who specialized exclusively in the field of security awareness and human risk management (as defined by their job title) were paid more than their security awareness peers whose job titles suggest other areas of expertise or focus.



DATA FROM AROUND THE WORLD

This edition of the Security Awareness Report features the participation of almost 2,000 security awareness practitioners from over 80 countries spanning the globe. This showcases the growth of our industry across geographical boundaries and cultural divides. Participants from North America, Europe, Asia, Africa, Australia, and South America shared their unique perspectives to create our most comprehensive and revealing report yet. In the map below we identify the countries involved in the survey and the number of respondents from each country.



SECTION 1
BENCHMARKING YOUR PROGRAM

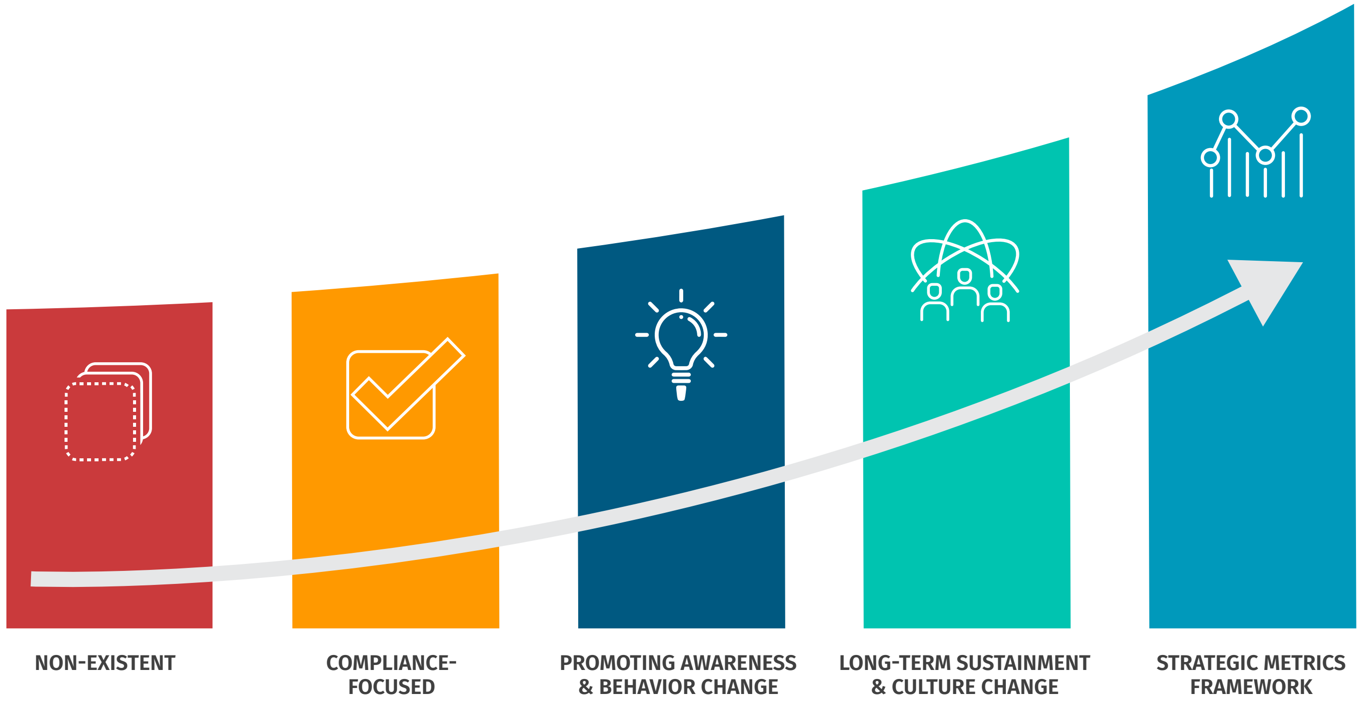
This section provides background on the security awareness industry, what the typical security awareness program looks like, and how different programs compare.

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.

SECURITY AWARENESS MATURITY MODEL®

Your Roadmap to Managing Human Risk


NON-EXISTENT
COMPLIANCE-FOCUSED
PROMOTING AWARENESS & BEHAVIOR CHANGE
LONG-TERM SUSTAINMENT & CULTURE CHANGE
STRATEGIC METRICS FRAMEWORK

SANS SECURITY AWARENESS

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

NON-EXISTENT
Employees have no idea that they are a target or that their actions have a direct impact on the security of the organization. They 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 being held on 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 just annual training and includes continuous 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
The program has the processes, resources, and leadership support in place for long-term sustainability, 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. It has gone beyond changing behavior and is changing the workforce's shared attitudes, perceptions, and beliefs about cybersecurity.

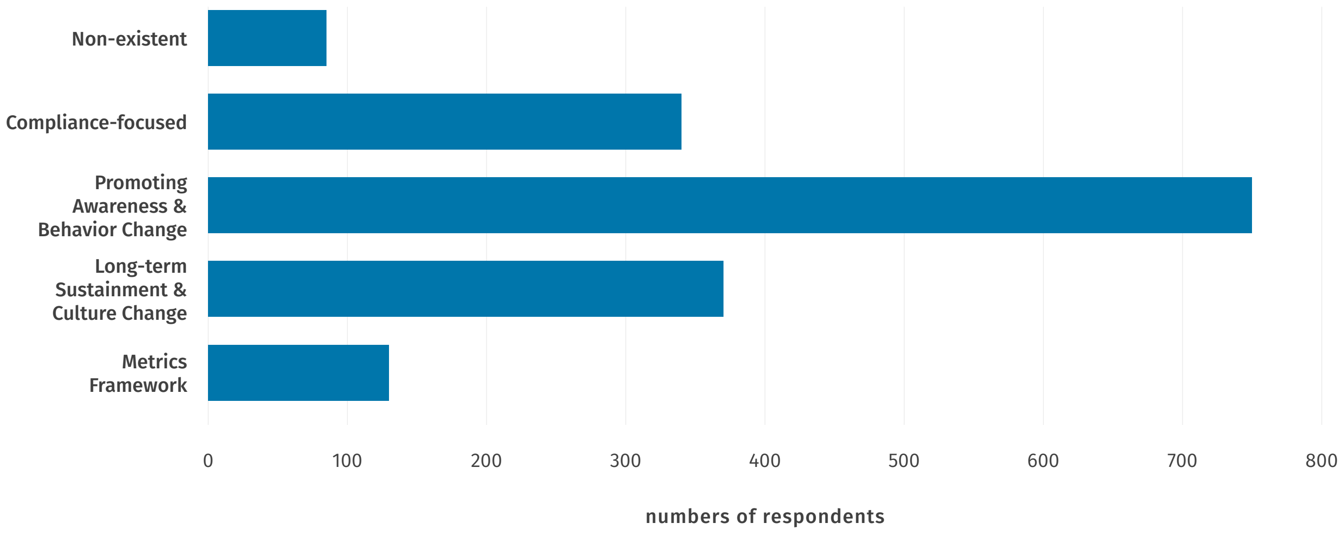
STRATEGIC METRICS FRAMEWORK
The program has a robust metrics framework aligned with and supporting the organization's mission and business goals. The program is going beyond measuring and reporting on changes in behavior and culture to examining how these changes are reducing risk and enabling leadership to achieve its strategic priorities. As a result, the program is continuously improving and able to demonstrate a return on investment.

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

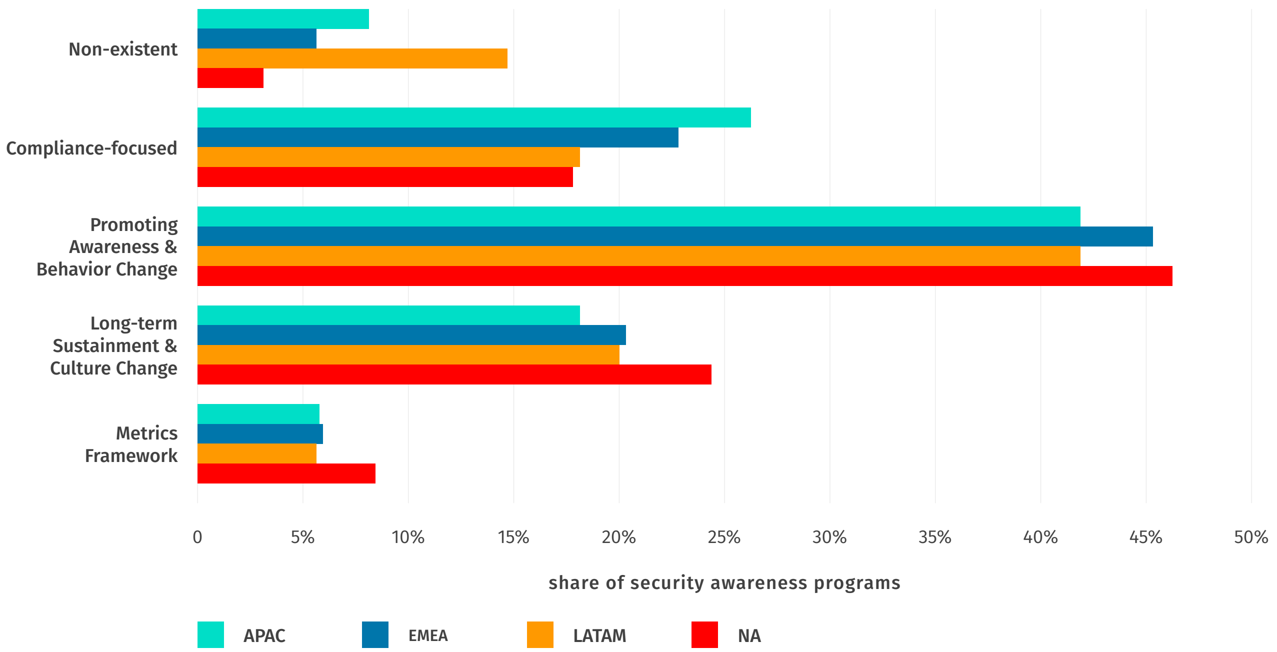
What are the average maturity levels for Security Awareness Programs, and how does your program compare against others? Overall, the results are an almost perfect bell curve.

MATURITY LEVELS OF SECURITY AWARENESS PROGRAMS



The results for 2023 mark an improvement over last year, when compliance-focused programs were more common than long-term sustainment and culture change. Looking at maturity across regions, most regions share a similar bell-curve breakdown. In other words, most regions around the world share relatively similar maturity levels in their Security Awareness Programs.

PROGRAM MATURITY BY REGION



TOP HUMAN RISKS

If Security Awareness Programs are ultimately about managing human risks, which of those risks are of most concern to organizations? The figure below shows that respondents cite one risk above all others, what we call the "three *ishings:" Phishing/Vishing/Smishing. The top four human risks cited by organizations are discussed below.

1 PHISHING/VISHING/SMISHING

This category refers to the three most common social engineering attacks: email-based phishing, text-message (SMS)-based smishing, and voice-based vishing. This risk was by far the top human risk identified by respondents, which is no surprise and reflects similar findings from other security reports. With the growth of Artificial Intelligence, it is becoming even easier for cyber threat actors to create customized phishing attacks with fewer spelling or grammar mistakes and in any language they want. Remember, this does not just apply to email or messaging: AI can now just as easily synthesize any human voice a cyber attacker wants. In many ways, AI is rocket fuel for cyber threat actors, so we can expect an increase in both the sophistication and breadth of these types of attacks.

2 PASSWORDS/AUTHENTICATION

This one was no surprise as a top risk, but to be honest we were expecting this to be ranked a much higher risk, equivalent to Phishing. One reason we believe passwords are comparatively perceived as a much lower risk is the active deployment of Password Managers to make strong passwords simpler, and / or the adoption of stronger authentication controls such as Multi-Factor Authentication (MFA).

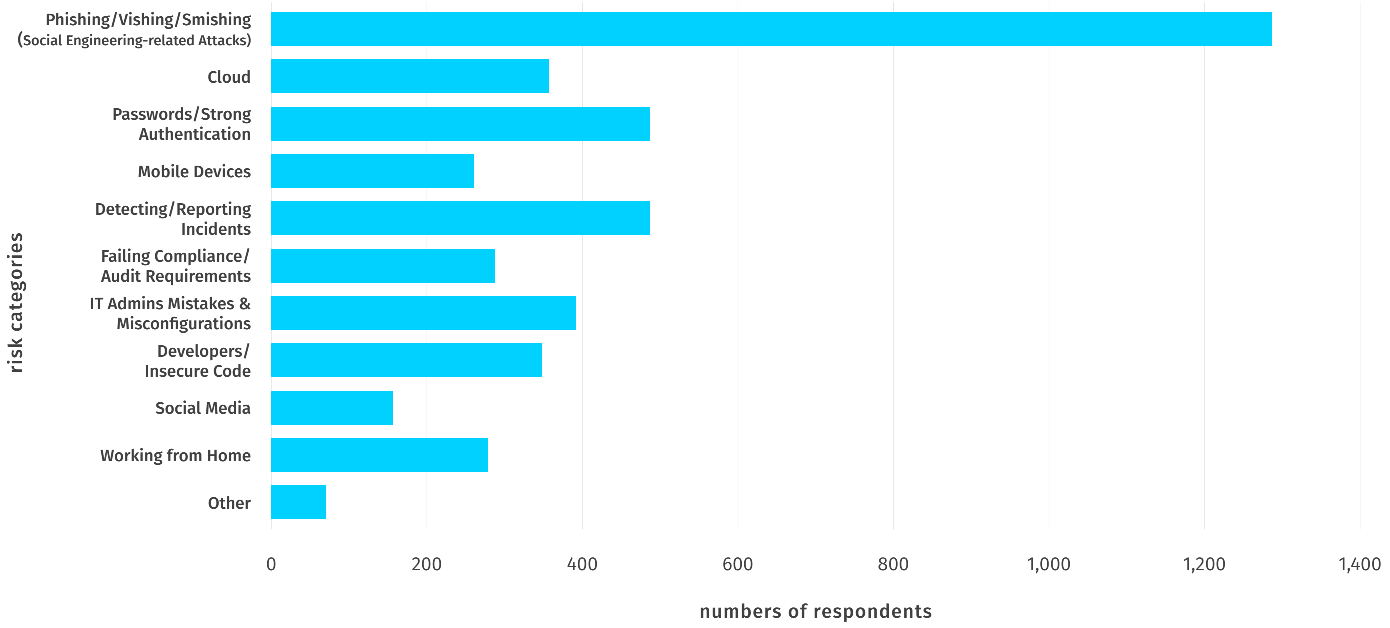
3 DETECTION/REPORTING

Tied in the risk ranking with Passwords/Authentication was Detection and Reporting, which surprised us. 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 understanding your security culture is key. How likely are people to report an incident even 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 not report and try to hide an incident they caused.

4 IT ADMIN MISCONFIGURATION

This risk category has been popping up more and more as a concern. IT admins manage sensitive systems and data, more often in the cloud. The problem is that the cloud can be a very confusing environment – the moment you finally figure it out, the technology advances, features change, and new functionality is added. In other words, it is very easy to make a mistake. Have you ever been confused by the cloud? IT admins get confused as well, but when they make a mistake – such as accidently exposing a dataset of highly sensitive data publicly – the impact of the incident is far greater. We are seeing huge demand for specialized training for IT admins (and developers) on how to securely manage and use the cloud.

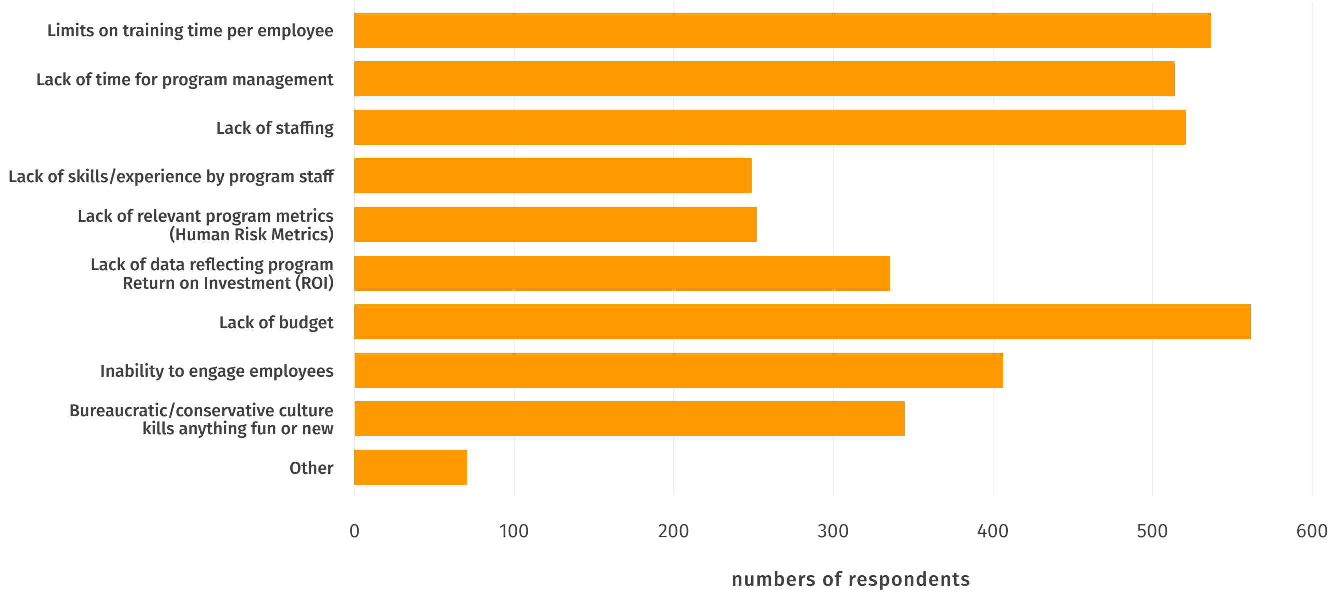
TOP HUMAN RISKS TO ORGANIZATIONS



MOST COMMON PROGRAM CHALLENGES

In addition to understanding the cyber-based threats that our industry is facing, it is important to understand the most common challenges that people are facing in building and managing an effective Security Awareness Program. What surprised us most from this year's survey is not what problems stood out the most, but rather which ones were among those standing out the least – in particular, metrics. We thought that metrics would be a top concern, but as shown in the figure below metrics and demonstrating return on investment were near the bottom. This makes sense when you look at the other responses. When people are struggling with the fundamentals – such as lack of budget, lack of time or lack of staff and can't get anything done – it's hard to be concerned about, much less focus on, metrics.

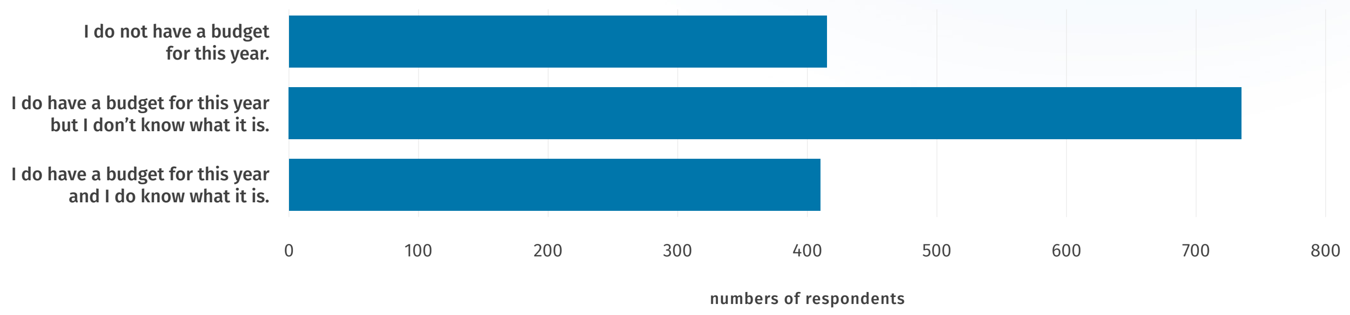
PROGRAM CHALLENGES



PROGRAM BUDGET

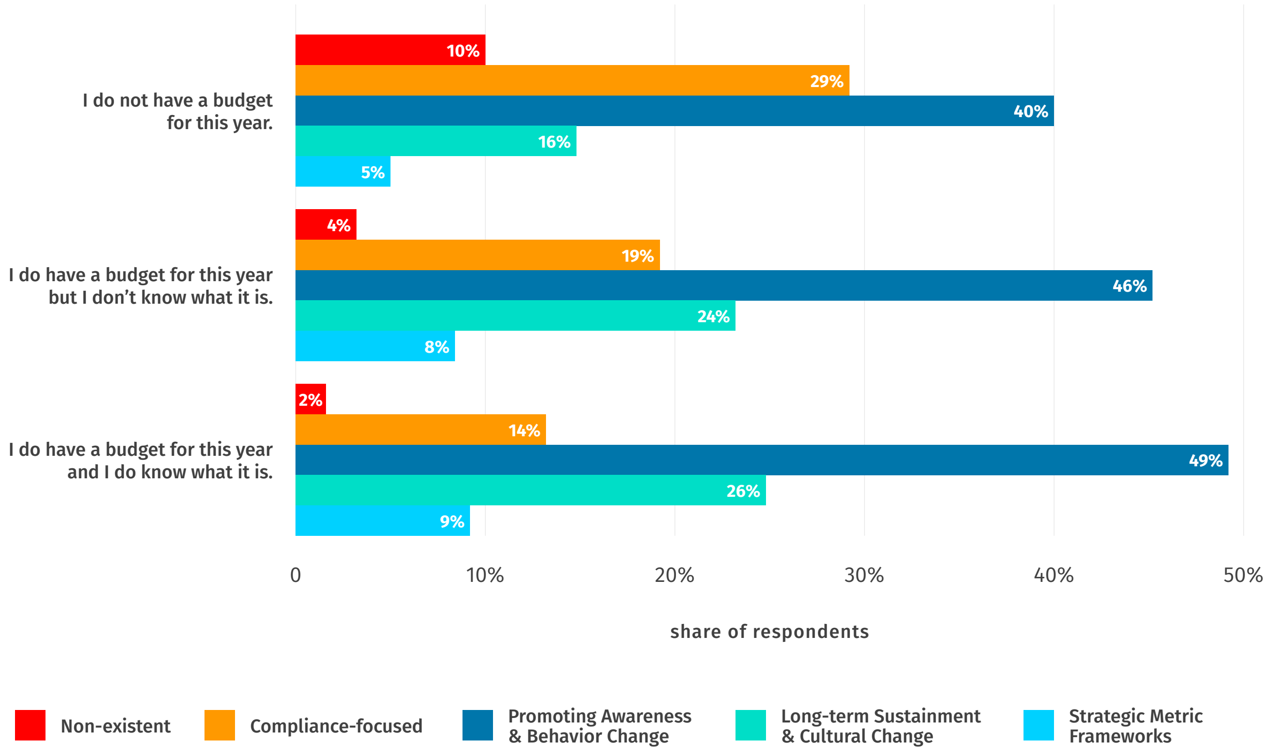
A new question about program budgets was added to this year's survey. We did not ask specifically about budget amounts, but rather only if respondents had a security awareness budget and, if so, whether they knew how much their budget was. The findings were surprising. First, 75% of respondents said they did have a budget, which was more than we expected. However, only 25% knew what their budget was.

BUDGET KNOWLEDGE



The survey found differences in maturity levels between programs that have a budget versus those that do not have one. Not surprisingly, organizations that have a budget have more mature Security Awareness Programs. But there was little difference in maturity levels between those that have a budget and don't know what their budget is versus those that have a budget and do know what their budget is. We're not exactly sure how to interpret this, but it appears that the biggest influencing factor is not how much your budget is, but whether leadership believes in you enough to provide your program with a budget to begin with.

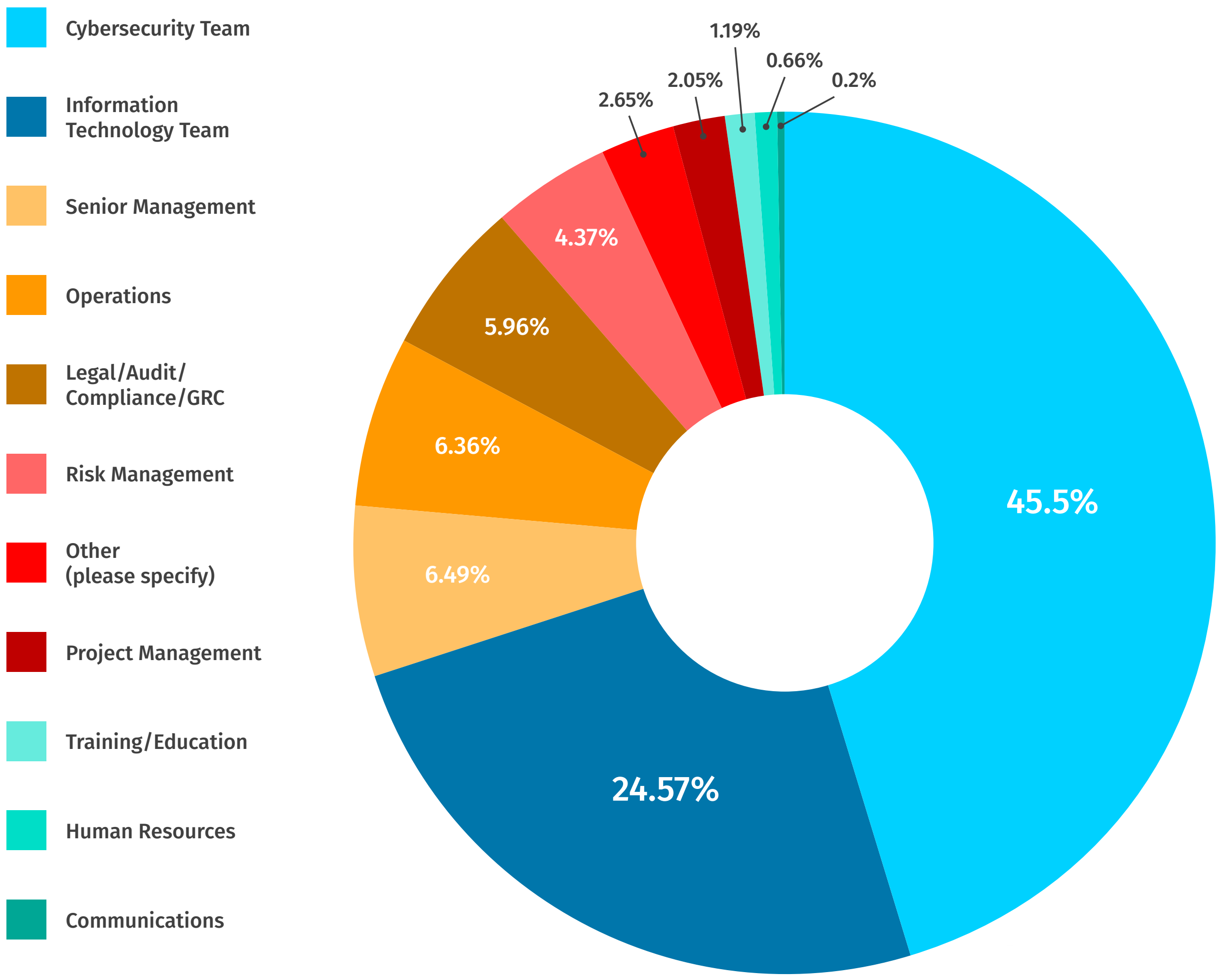
PROGRAM MATURITY BY BUDGET AWARENESS



TO WHOM DO SECURITY AWARENESS PROGRAMS REPORT?

We were interested in learning what departments or teams security awareness professionals most often report to. To the Security Team, where they can more effectively coordinate their efforts and manage human risk? Or to Human Resources or Legal, with a focus on compliance? The vast majority of respondents said they report to the Cybersecurity, Information Technology, Operations or the Risk Management Team (combined for a total of 72%), which implies more of a focus on human risk. Only a small percentage report to Human Resources, Legal, Audit and Training (7%), which implies more of a compliance focus.

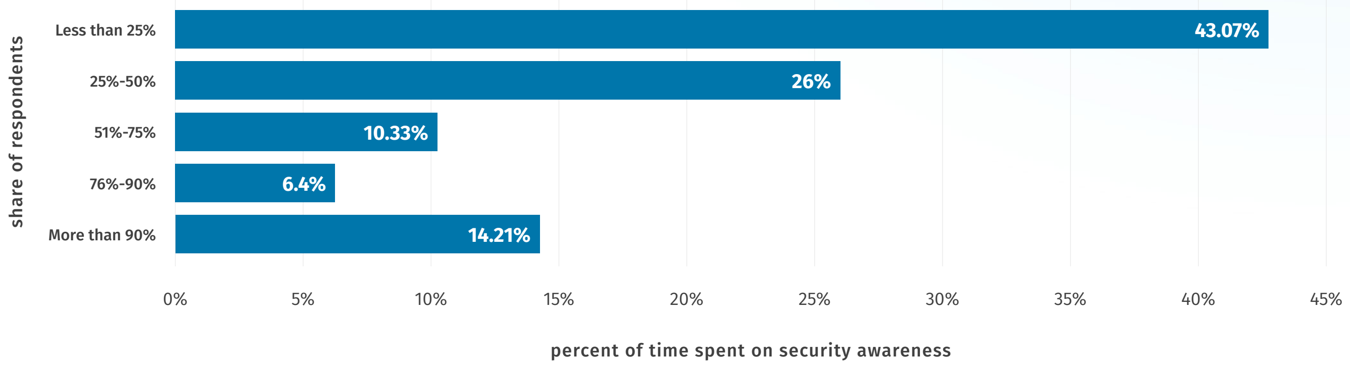
TO WHOM DO YOU REPORT?



BENCHMARKING AWARENESS PROFESSIONALS

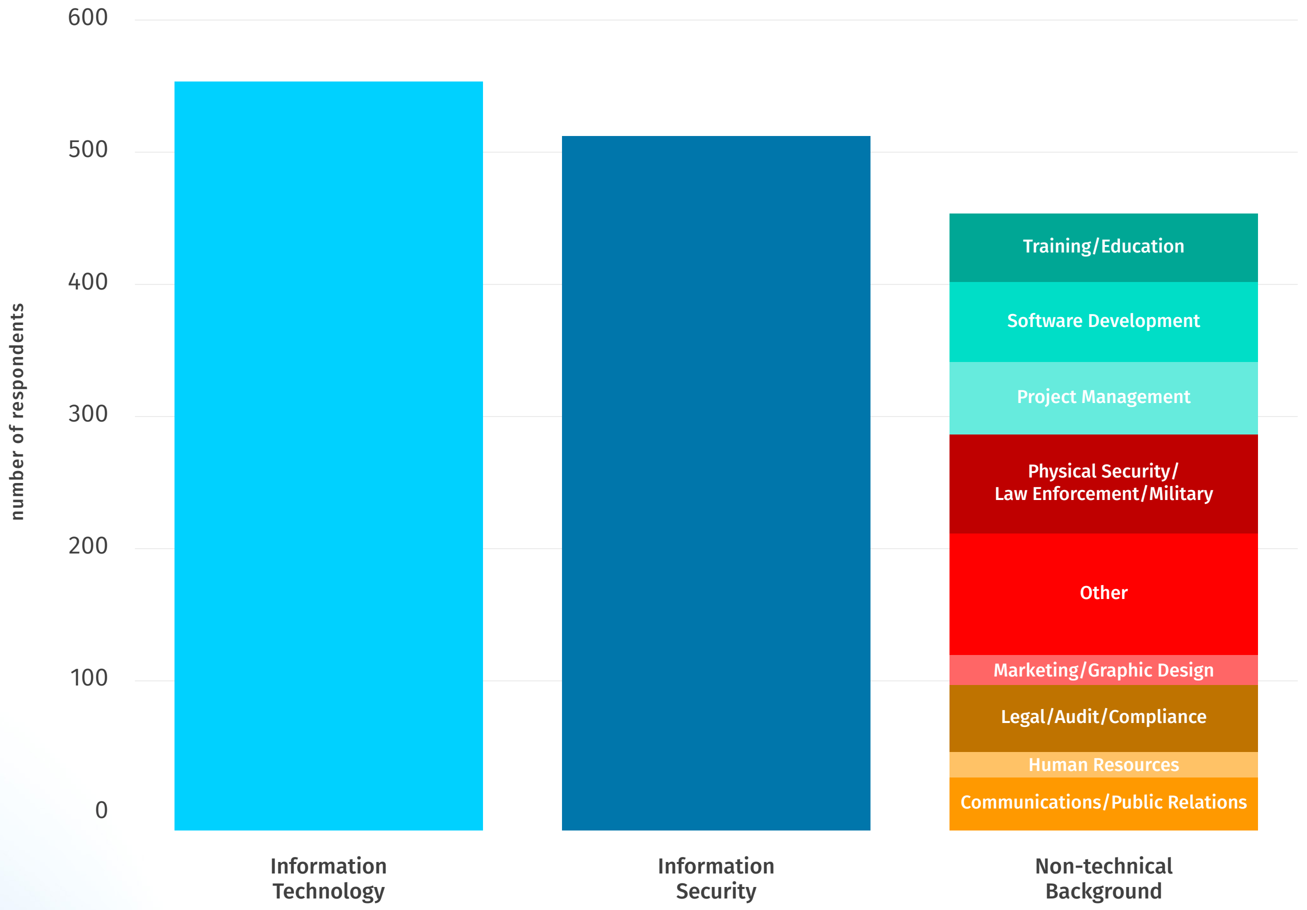
Similar to years past, security awareness is often perceived by organizations as a part-time task, with almost 70% of security awareness practitioners reporting this year that they spend 50% or less of their time on it. These numbers are almost identical to last year.

TIME ALLOCATION TO SECURITY AWARENESS



Also similar to years past, most security awareness professionals surveyed in 2023 have a security or technical background.

BACKGROUNDS OF SECURITY AWARENESS PROFESSIONALS



SECTION 2
MATURING YOUR PROGRAM

Now that you have a better understanding of the security awareness industry and how you and your organization may compare, we need to identify the key drivers of program maturity and what can you do based on that information. An analysis of all the data identify the two biggest drivers of program maturity as:

1 **LEADERSHIP SUPPORT**
The most mature Security Awareness Programs are those that have the greatest leadership support. This is not a surprise, as this has been a consistent finding for the past three years, and aligns with findings from other organizational change programs and related research. What we need to understand is how to best build and sustain leadership support.

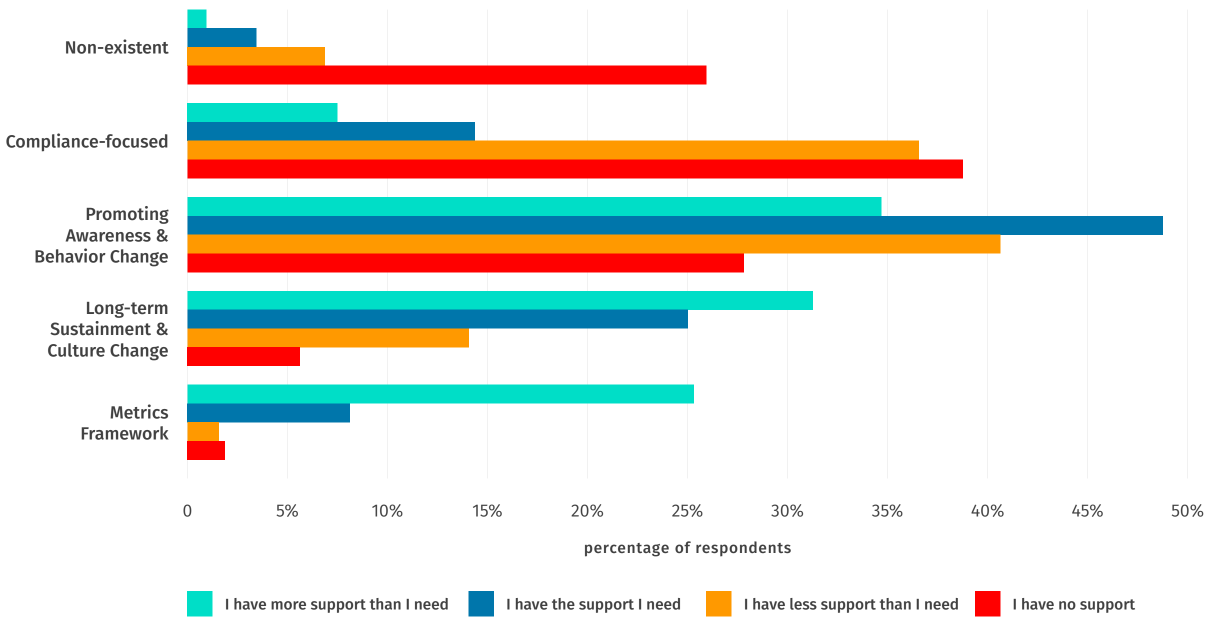
2 **TEAM SIZE**
The most mature programs have the largest Security Awareness Teams. Managing human risk is not a technology challenge, it is a human challenge, and as such it requires people to solve problems.

As you review the findings, notice how these two drivers are inter-related. The stronger your leadership support, the more likely you will be provided the resources you need, such as a larger team and a budget. The larger your Security Awareness Team, the more you can get done, such as partnering with other departments, analyzing and prioritizing your top human risks, simplifying and communicating policies, engaging and training your workforce, collecting and reporting metrics, etc. Given this inter-relationship, this section examines in more detail how you can improve these two key drivers.

LEADERSHIP SUPPORT

This year's survey results strongly correlate leadership support with program maturity. Not only does this align with findings from surveys in past years, it also aligns with most organizational change studies and efforts.

PROGRAM MATURITY BY LEADERSHIP SUPPORT



ACTION ITEMS FOR GREATER LEADERSHIP SUPPORT

TALK TO LEADERSHIP (AND YOUR SECURITY TEAM) IN TERMS OF RISK
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 human risk management. Human risk is 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, 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 reducing human risk. Partner with your Security Operations Center, 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, leadership may perceive the role describe as being in the entertainment business. Notice how in the second example the job description is much more risk focused, far more likely to connect with leadership and far more likely to gain their support.

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 helped lead the new micro-videos we just released and the recent security awareness posters and 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. My job is to manage our human risk. Did you know that our staff was the key driver in over 75% of all of our security incidents in the past year? I work with the security team to engage, train, and change our workforce's behaviors so they behave in a far more secure manner. Our goal is to dramatically reduce our workforce's risk while increasing their ability to securely make the most of our technology, including Cloud as part of our new Digital Transformation initiative.

CREATE A SENSE OF URGENCY
Does leadership perceive the human as a significant risk? Leverage data and statistics from within your own organization (as Renan did in Example 2) to demonstrate to leadership the need to address human risk. Work with your Security Operations Center or Incident Response Teams to get those data points, such as documenting past incidents and how most were human-related, or with Cyber Threat Intelligence Teams to demonstrate how people are now the primary attack vector.

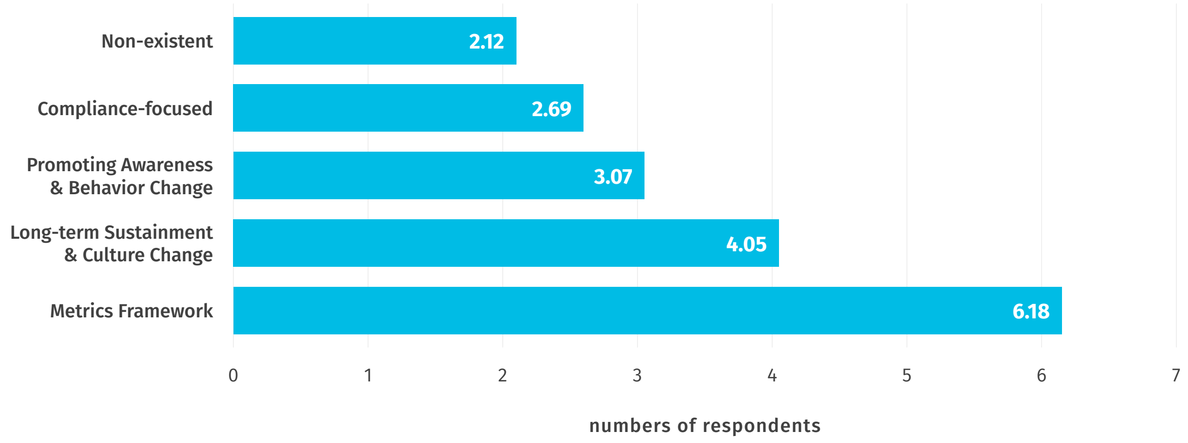
COMMUNICATE THE IMPACT
Dedicate two to four hours a month to collecting metrics about the impact and value of your Security Awareness Program and communicate that value to leadership. This information can include informal metrics, established key performance indicators, and even success stories. Enable leadership to better understand and regularly see the value that your program is providing. Not sure what metrics to collect? Review the Security Awareness Maturity Model Indicators Matrix in Appendix A of this report.

TEAM SIZE

Once again, this year's survey found a direct correlation (and most likely the strongest correlation) between team size and program maturity: the larger your Security Awareness Team, the greater your program's maturity level. We asked respondents to report how many full-time employees (FTEs) supported their awareness program. By FTE, we mean the combined efforts of multiple people. For example, if two people are each working 50 percent of their time on the awareness program, combined they equal a single FTE.

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 three FTE's to effectively change behavior. The most mature Security Awareness Programs on average have at least six combined FTEs dedicated to or helping manage the program.

SECURITY AWARENESS PROGRAM MATURITY BY AVERAGE NUMBER OF FULL-TIME EMPLOYEES



ACTION ITEMS TO INCREASE TEAM SIZE

DEMONSTRATE THE INVESTMENT GAP BETWEEN TECHNICAL AND HUMAN-FOCUSED SECURITY

Help leadership better understand WHY people are so actively targeted. Explain that while your organization has become very effective at securing technology, it has under-invested in the human side, leaving its workforce 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 will see 50-person Security Teams with 49 of those people 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-to-1 ratio of technical security professionals to human-focused security professionals.

BREAK DOWN YOUR NEEDS

Document all the different steps and initiatives you need to undertake in order to make your program effective. These can include working with the Security Team to identify and monitor your top human risks; with Audit and Legal for compliance purposes; with Human Resources and Communications for employee outreach and training; with IT, developers, and other technical staff to implement role-based training; and with various departments to simplify security policies in general. If you can 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 FTEs on your team, see if you can hire short-term contractors to take on and help manage specific initiatives.

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; with Human Resources to help with new hires or to measure and build a strong culture; and with Business Operations to help analyze metrics and data points.

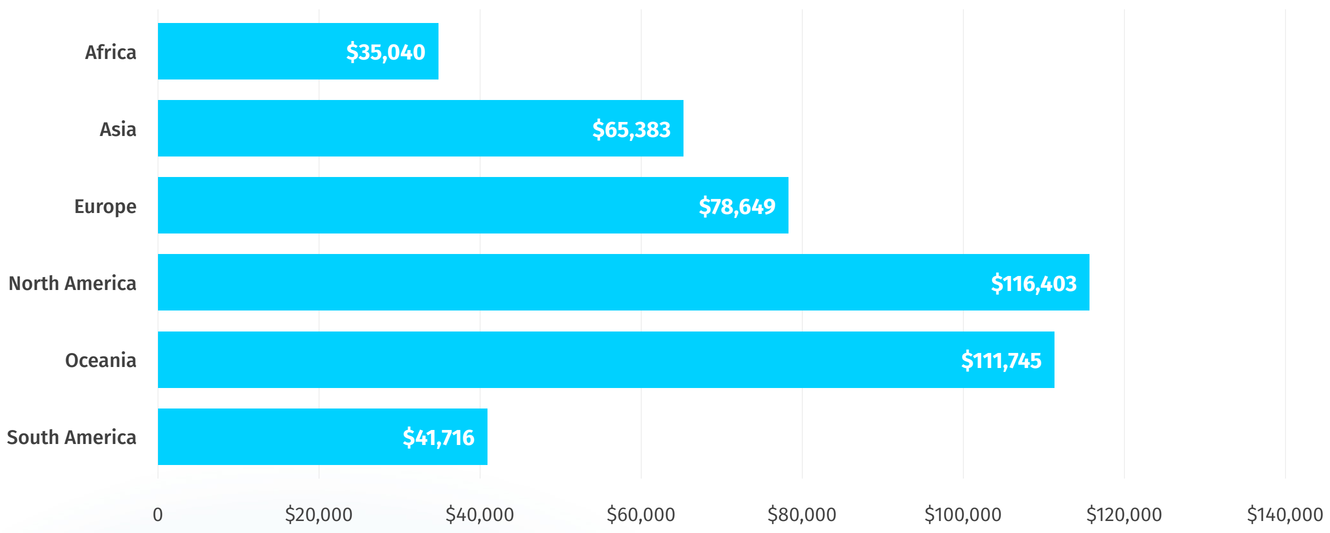
SECTION 3
GROWING YOUR CAREER

The goal of the this section is to enable security professionals to grow their skills and careers in human risk management, including their compensation. The hope is that in the near future we will begin to see not only CISOs who started on the technical side of cybersecurity, but also CISOs who began their careers on the human-risk side.

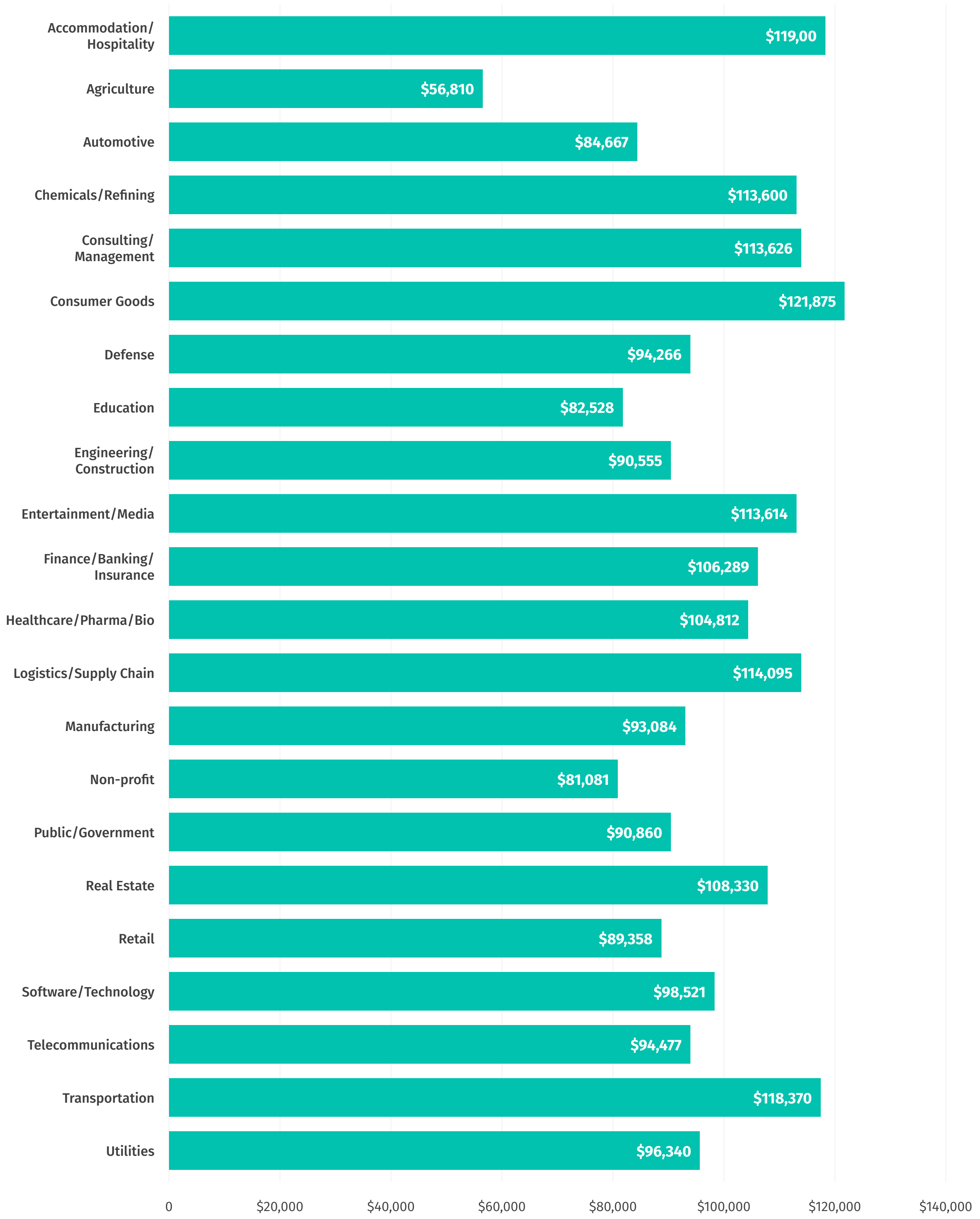
COMPENSATION

Similar to past years, we wanted to know what the average salaries are for people in the field. The average annual salary for someone involved in security awareness in 2023 was $97,998.08. 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 $116,403 and Africa the lowest at $35,040. For industries, security awareness professionals working in consumer goods have the highest salary at $121,875, with agriculture the lowest at $56,810.

AVERAGE SALARY BY CONTINENT

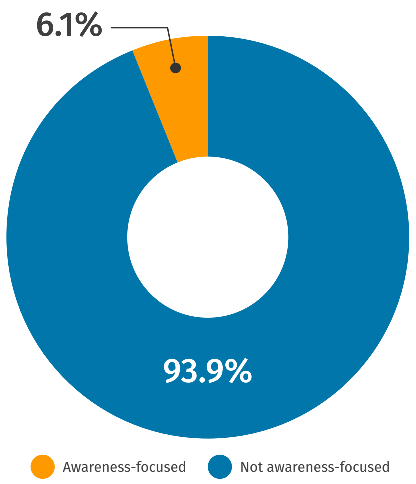


AVERAGE SALARY OF SECURITY PROFESSIONALS BY INDUSTRY



In addition, we wanted to understand if people's compensation is influenced by their level of specialization in the human-risk side of cybersecurity. For this year's survey, we defined people specializing in the human side of cybersecurity as those having one of the following words in their job title: *awareness*, *behavior*, *culture*, *influence*, *engagement*, *training*, *communication*, or *human risk*. For example, titles such *security analyst*, *IT manager*, *compliance*, *operations manager*, or *security engineer* were not considered as specializing in the human-risk side. What is surprising is that of 1,864 people surveyed who gave their job title, only 114 (less than 10 percent) have a job title that we would consider human-specific. This indicates our field is still very much in its infancy.

ROLE-FOCUSED, ALL RESPONDENTS

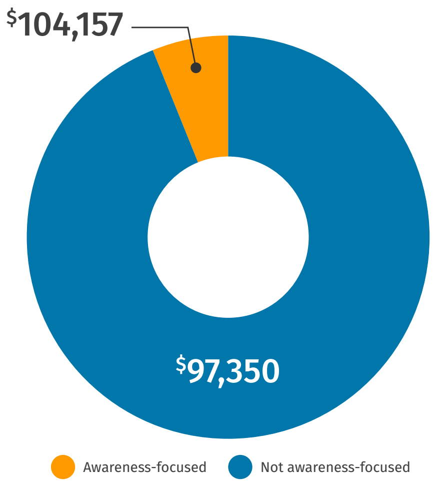


How do the salaries of those who have job titles that are human-risk-focused compare to the salaries of those whose titles are not human-risk-focused? For the first time, this year's survey found that people specializing in human risk (as defined by their job title) are paid more than those with titles not focused on awareness. On average, awareness-focused roles are paid $7,000 more annually. Globally, the salaries of awareness professionals whose title reflects a human-risk focus average $104,157 compared to $97,350 for professionals with all other roles. In North America, the average salary of awareness professionals whose title reflects a human focus average $122,486, versus $115,366 for professionals with un-related job titles.

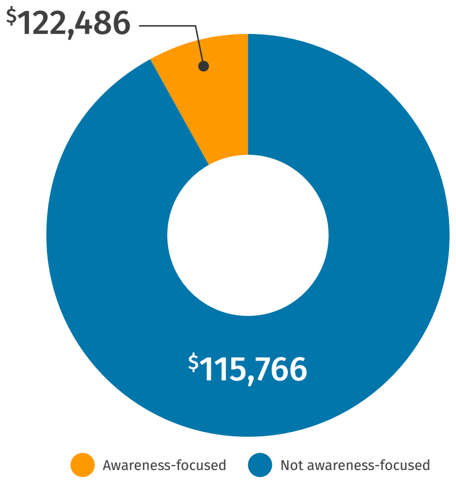
This change from last year could be the result of several factors. First, the 2023 survey marked the first year we defined roles by an individual's title rather than by an individual's background. Second, this year's report is one of our largest data sets and most global. Finally, the field of managing human risk is growing, with security leaders beginning to understand that awareness is more than just annual computer-based training – or at least we'd like to think this is one of the driving reasons why the salaries of human-risk-focused professionals are increasing.

The survey also compared the average salaries of professionals with technical backgrounds versus those without such backgrounds. In years past, people with technical backgrounds were paid much more than those with non-technical backgrounds. This year that difference shrunk, with technical professionals on average paid only $2,000 more annually than non-technical professionals.

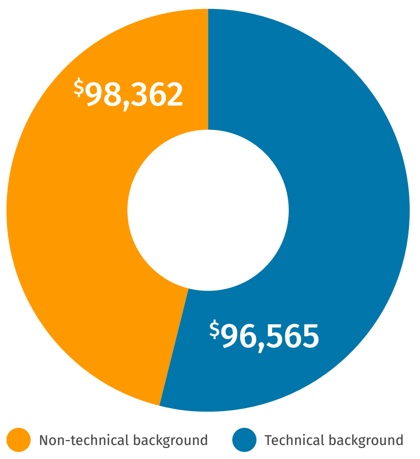
AVERAGE SALARY BY FOCUS TYPE



AVERAGE SALARY BY FOCUS TYPE, NORTH AMERICA ONLY



AVERAGE SALARY BY BACKGROUND TYPE



ACTION ITEMS FOR NON-TECHNICAL INDIVIDUALS

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 managing human risk, your role can and should involve so much more. First, as discussed in the previous section, ensure that leadership understands the importance and focus of your role: human risk management. In addition, work with the Security Team to improve and simplify its 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 incident communications, internally or externally. Work with senior leadership on table-top 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!

UPDATE YOUR TITLE
If your position is truly to manage human risk, and if your leadership believes in the importance of that goal, have your title changed to reflect your area of specialization.

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 have an understanding of 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 Security Operations Center 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 are the most common TTPs that cyber threat actors use to target your workforce. Don't know what a TTP is? Ask them, and have them teach you all 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 SANS courses listed in Appendix B of this report that 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, taxonomies, 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," which basically holds that the more expertise someone has on a specific subject, the more difficult it is for them to 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 take care to be aware of their "curse of knowledge" and address the biases and misconceptions that it can engender.

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 to make security simple for their workforce.

ACCESS OR 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 Department to assist with all security-related communications and outreach, or even embedding one of that department's staff members 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).

SUMMARY OF KEY ACTION ITEMS

MATURING YOUR PROGRAM

TALK TO LEADERSHIP (AND YOUR SECURITY TEAM) IN TERMS OF RISK
Leadership and Security Teams often perceive security awareness as not part of security, but rather as a compliance effort that has little relevance to managing risk. To help change such perceptions, focus on and speak in terms of human risk management. Human risk is far more likely to align with most organizations' strategic security priorities, gain leadership buy-in, and resonate with a Security Team. Help your Security Team members understand how you help them, 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 reducing human risk. Partner with Security Operations Center, Incident Response and Cyber Threat Intelligence Teams not only to learn their work but also to show them how you can help solve their human-risk-related challenges.

CREATE A SENSE OF URGENCY
Does leadership perceive the human risk as a significant risk? Leverage data and statistics from within your own organization to demonstrate to leadership the need to address human risk. Work with your Security Operations Center or Incident Response Team to document past incidents and how most were human-risk-related. Work with Cyber Threat Intelligence Teams to demonstrate how people are now the primary attack vector.

COMMUNICATE THE IMPACT
Dedicate a half-hour to an hour a week to collecting metrics about the impact and value of your Security Awareness Program and communicate that value to leadership. This information can include informal metrics, established key performance indicators, or even success stories. Enable leadership to better understand and regularly see the value that your program provides. Not sure what metrics to collect? Review the Security Awareness Maturity Model Indicators Matrix in Appendix A of this report.

DEMONSTRATE THE DISCREPANCY BETWEEN TECHNICAL AND HUMAN-FOCUSED SECURITY
Help leadership better understand WHY people are so actively targeted. Explain that while your organization has become very effective at securing technology, it has under-invested in the human side, leaving its workforce 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 those people focused on technology and maybe just 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-to-1 ratio of technical security professionals to human-focused security professionals.

BREAK DOWN YOUR NEEDS
Document all the different steps and initiatives you need to undertake in order to make your program effective. These can include working with the Security Team to identify and monitor your top human risks; with Audit and Legal for compliance purposes; with Human Resource and Communications for employee outreach and training; with IT, developers, and other technical staff to implement role-based training; and with various departments to simplify security policies in general. If you can identify and document the number of full-time employees 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 full-time employees on your team, see if you can hire short-term contractors to take on and help manage specific initiatives.

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; with Human Resources to help with new hires or to measure and build a strong culture; and with Business Operations to help analyze metrics and data points.

GROWING YOUR CAREER

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 managing human risk, your role can and should involve so much more. First, ensure that leadership understands the importance and focus of your role: human risk management. In addition, work with the Security Team to improve and simplify its 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 in any incident communications, internally or externally. Work with senior leadership on table-top 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 have an understanding of the models, frameworks, and terminology. This will enable you to better understand your organization's risks and 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 Security Operations Center 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 are the most common TTPs that cyber threat actors use to target your workforce. Don't know what a TTP is? Ask them, and have them teach you all about the MITRE ATT&CK model. Ask your Incident Response Team to walk you through the incident response playbook. Finally, take a look at the SANS courses listed in Appendix B of this report that can help you develop your understanding and expertise in the security field. You don't have to be a cybersecurity expert, but the better you understand the security frameworks, taxonomies, and terms used, the more effective you will be.

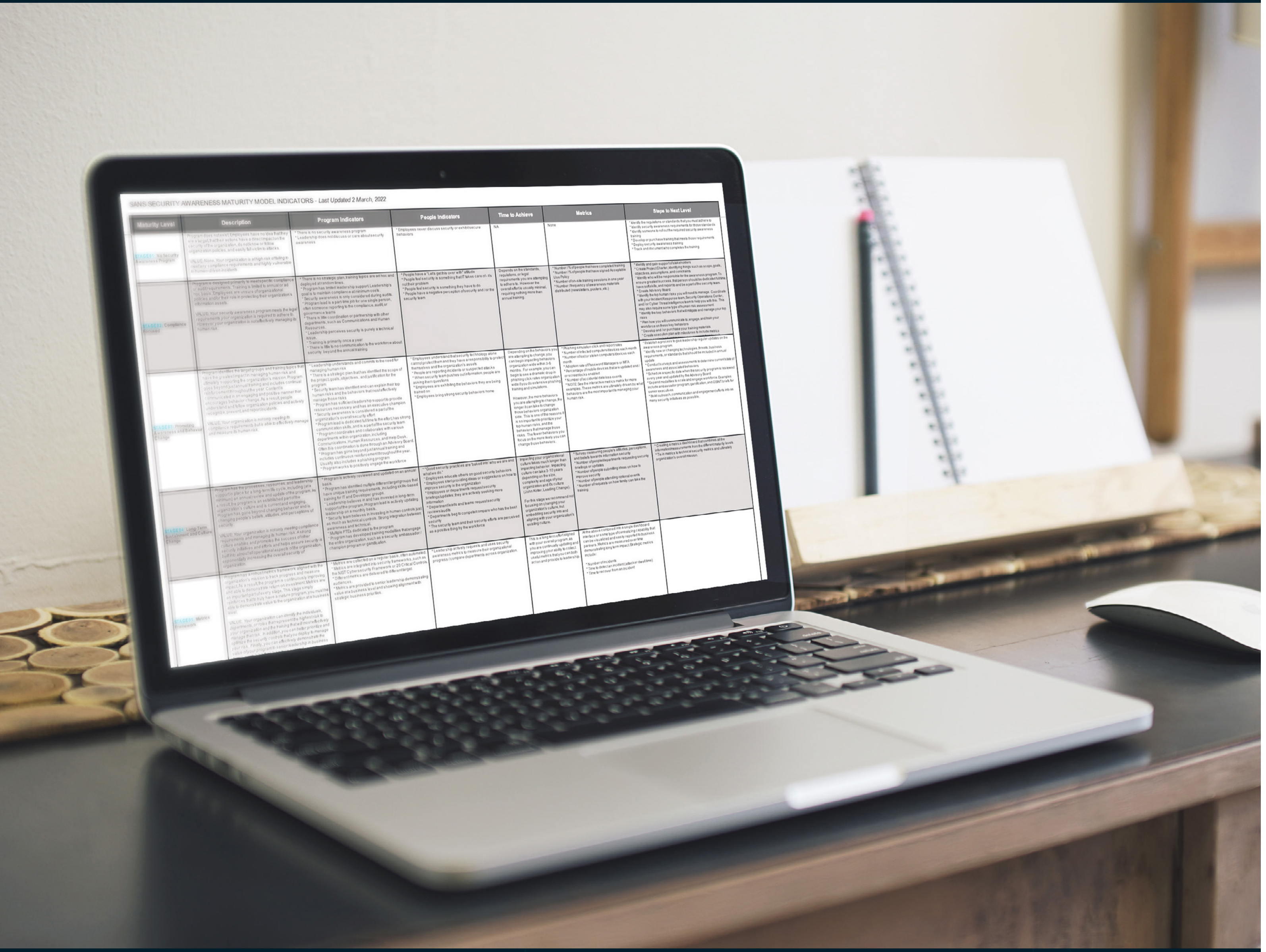
UPDATE YOUR TITLE
If your position is truly to manage human risk, and your leadership believes in the importance of that goal, have your title changed to reflect your area of specialization.

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 security concepts and technologies that are easy for you are most likely difficult, confusing, or even intimidating for many 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 to make security simple for their workforce.

ACCESS OR 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 Security Team, partnering with your Communications or Marketing Department to assist with all security-related communications and outreach, or even embedding one of the department's staff members 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.)

APPENDIX A
SECURITY AWARENESS MATURITY MODEL INDICATORS MATRIX

NOTE: You can download a digital copy of the Maturity Model Indicators Matrix



DOWNLOAD

APPENDIX B
CAREER DEVELOPMENT

Organizations and security leaders increasingly recognize that cybersecurity is no longer just a technical challenge, but a human challenge as well. Security Teams around the world are looking for trained professionals specializing in the field of human security (awareness, behavior and culture). For those of you who are looking to get involved in this field, or are already involved but looking to develop your skills, the SANS Institute offers key courses to help develop your career path.

WHERE TO START?

If you are new to the world of information security and/or security awareness, the very first class you will want to start with is MGT433: Managing Human Risk.

MGT433: MANAGING HUMAN RISK

This three-day class lays the foundation for security awareness, changing organization behavior, and ultimately managing and measuring human risk. The course content is based on lessons learned from hundreds of Security Awareness Programs from around the world. You will learn not only from your instructor, but also from extensive interaction with your peers, and you'll 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. Students also have the option to test for the SANS Security Awareness Professional (SSAP) credential, the industry's most recognized credential demonstrating expertise in managing human risk.

LEARN MORE

WHAT NEXT?

You may need to develop your security expertise if you do not have a technical or a security background. Understanding key security frameworks, concepts, and controls will help you better understand risks and the behaviors to manage those risks. It will also empower you to more effectively communicate with your Security Team and leadership. SANS offers two five-day courses to consider at this stage in your career. Each has its advantages, depending on what you hope to achieve.

MGT512: SECURITY LEADERSHIP ESSENTIALS FOR MANAGERS

This course empowers you to become an effective security manager and get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. To help you accomplish this goal, MGT512 covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls are covered in conjunction with key management topics that address the overall security lifecycle. This includes governance and technical controls focused on protecting, detecting, and responding to security issues.

LEARN MORE

SEC301: INTRODUCTION TO CYBERSECURITY

This five-day course takes a technical, hands-on approach for those new to cybersecurity. It covers everything from core terminology to the basics of computer functions 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 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 that will serve as the foundation for your career skills and knowledge for years to come.

Not sure which one of these two courses to take? If you are looking for more of a high-level or management perspective on information security, MGT512 might be your best choice. If you want a more hands-on, technical introduction to the tools and technology of cybersecurity, then SEC301 is recommended.

LEARN MORE

INTERMEDIATE LEVEL

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

MGT521: SECURITY CULTURE FOR LEADERS

Cybersecurity is no longer just about technology, it is about people and, ultimately, culture. This five-day course will teach leaders how to leverage the principles of organizational change, enabling them 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.

LEARN MORE

SEC504: HACKER TOOLS, TECHNIQUES, AND INCIDENT HANDLING

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

LEARN MORE

ADVANCED LEVEL

Once you have 5-7 years of experience and want to truly develop your security leadership skills, consider taking SANS MGT514: Security Strategic Planning, Policy, and Leadership. The course will walk you through the strategic planning process and the challenges faced by today's Chief Information Security Officers. Many people consider this the "CISO course" that helps new and experienced CISOs become better security leaders and more effective business communicators. By better understanding the challenges, priorities, and concerns of CISOs, you can more effectively collaborate with senior leadership and communicate in their terms and language.

MGT514: SECURITY STRATEGIC PLANNING, POLICY, AND LEADERSHIP

This course gives you the 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.

LEARN MORE

THE SANS COURSE ROADMAP

SANS has almost a hundred different courses to choose from, so if you feel that a class is missing or you would like to develop a different skill, be sure to check out the **SANS Course Roadmap**. Cybersecurity is a dynamic and challenging career, and the more skills you develop in the field the more opportunities (and options) you will have.

LEARN MORE

ACKNOWLEDGEMENTS

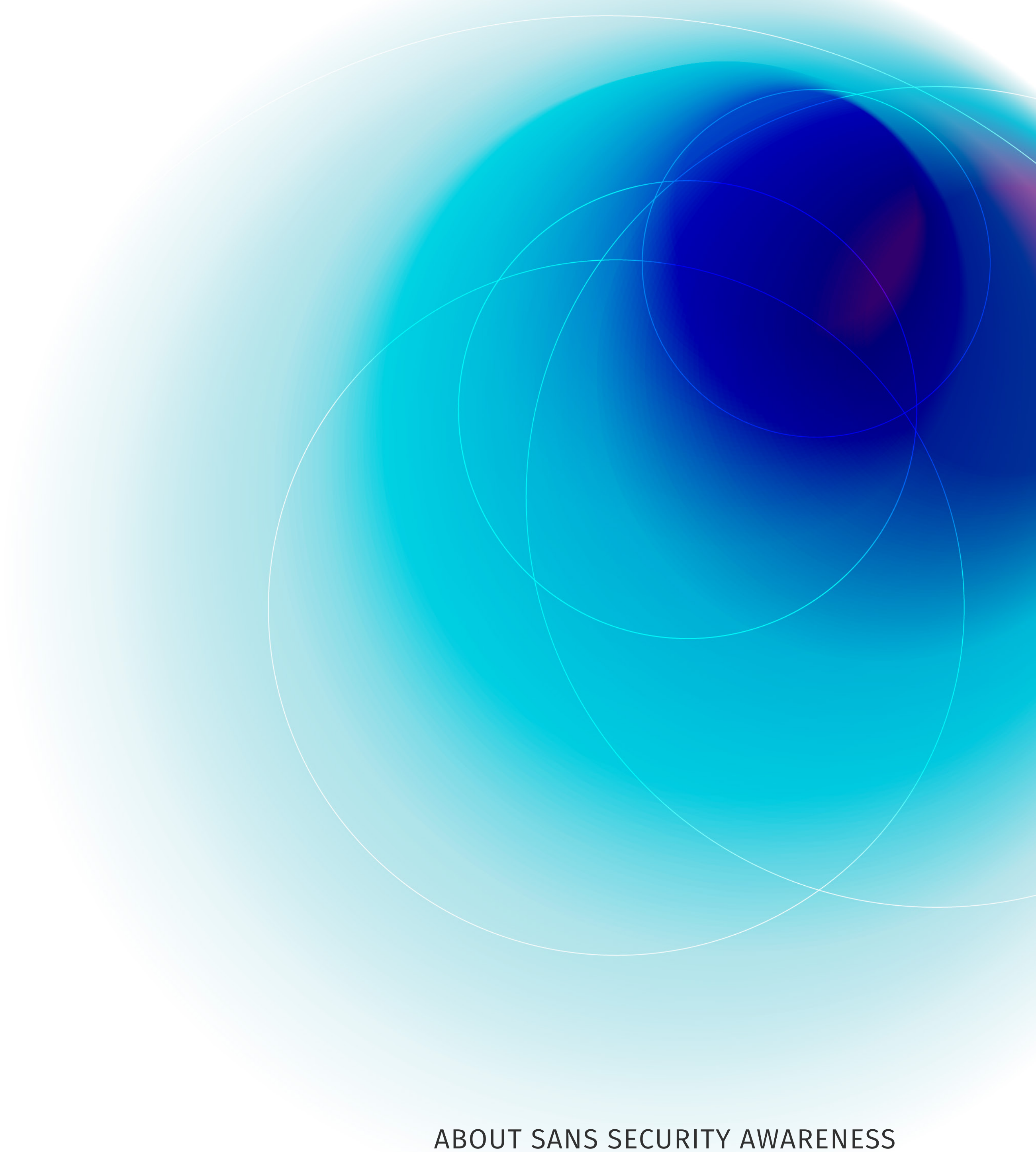
The 2023 Security Awareness Report was developed by the community for the community, in partnership with the SANS Institute. The following key contributors produced this report.

LANCE SPITZNER

Lance Spitzner has more than 25 years of security experience in cyber threat research, security architecture, and awareness and training. He helped pioneer the fields of deception and cyber intelligence with his creation of honeynets and his founding of the Honeynet Project. Lance has published three security books, consulted in more than 25 countries, and helped more than 350 organizations build security awareness and culture programs to manage their human risk. Lance is a frequent presenter and a serial tweeter (@lspitzner), and he works on numerous community projects. Before entering the information security field, Lance served as an armor officer in the U.S. Army's Rapid Deployment Force and earned his MBA from the University of Illinois.

CHAD JONES

Chad Jones 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 Cyber Security industries, Mr Jones' expertise in leveraging data for insightful decision-making sets him apart.



ABOUT SANS SECURITY AWARENESS

SANS Security Awareness, a division of the 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 around the world. 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

SANS SECURITY AWARENESS