

2019 SANS Security Awareness Report

The Rising Era of Awareness Training

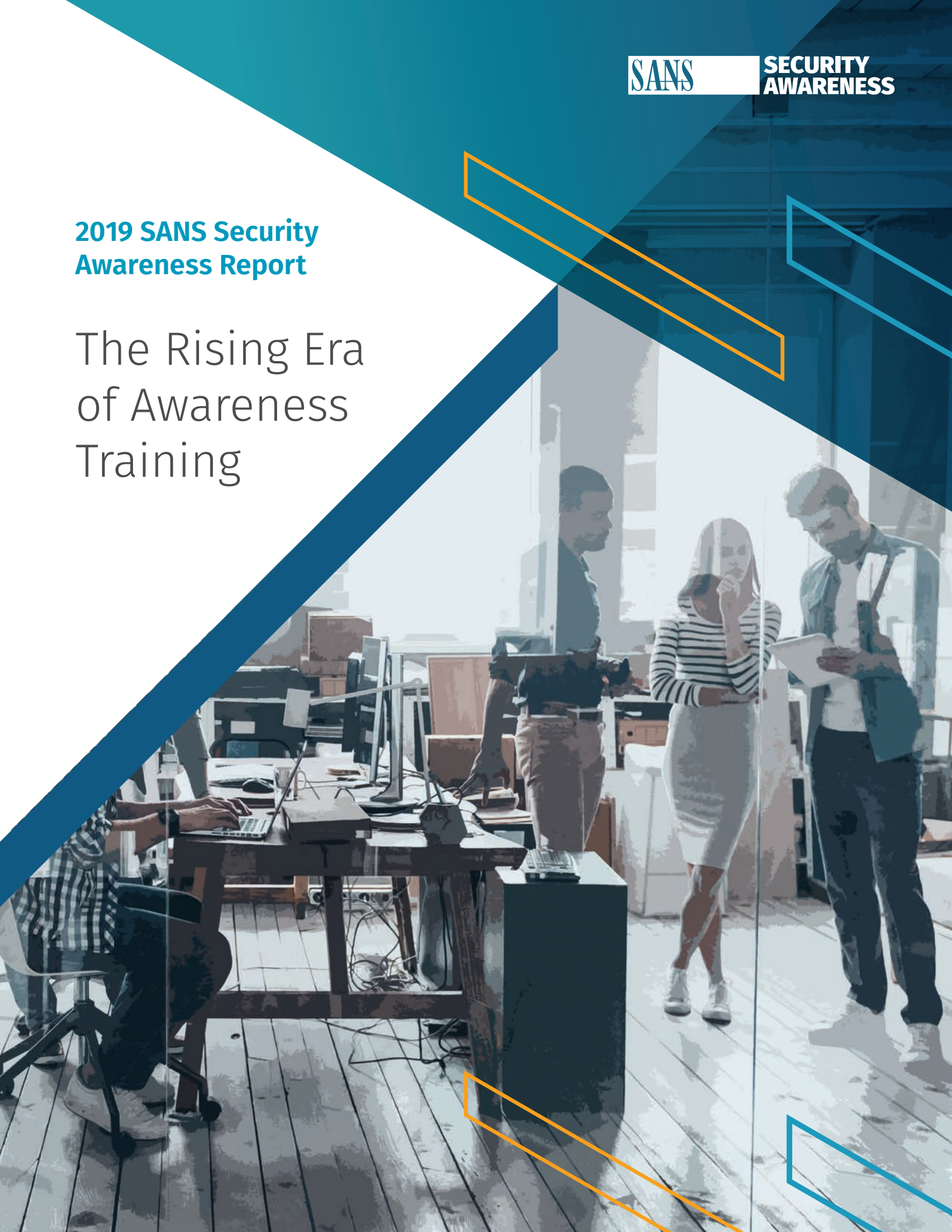


Table of Contents

Executive Summary.....	4
About This Report.....	6
Overview	6
How to Measure Success	6
Benchmarking Your Program's Maturity Level.....	8
Blockers and Supports.....	9
Action Items.....	10
Predicting Success.....	11
Leadership Support = Program Maturity	11
Action Items.....	12
Budget and Program Success	12
Additional Steps	13
The Most Valuable Resources for Security Awareness.....	14
Action Items: Get the Most out of Your Time	17



Table of Contents

Analysis by Industry: Who is the Most Aware?	18
Demographics – Who Runs Security Awareness Programs?	20
Background	20
Action Item for Communicating to Learners and Leadership	21
The Organizational Structure of a Security Awareness Department.....	22
Job Titles for Security Awareness Professionals	23
Action Item.....	23
Summary of Key Action Items	24
Appendix A – Hiring Requirements for a Security Awareness Officer	26
Appendix B – NIST NICE Framework Mapping.....	27
A Big Thanks.....	28
Contributors.....	28
Authors.....	29
About SANS Security Awareness	31

Executive Summary

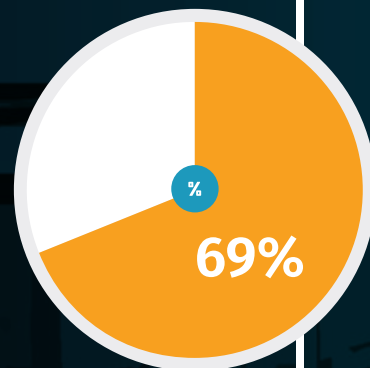
The 2019 SANS Security Awareness Report represents data aggregated from security awareness professionals from around the world. The analysis of this data identifies and benchmarks how organizations manage their human risk to include security awareness program maturity, funding, and staffing. Outlining what enables organizations to create thriving programs, lessons learned uncovering potential pitfalls, and how to address them is the predominant intent of this annual report.

A brief summary of key findings for 2019 include:

- 1 For a mature awareness program, we recommend the person in charge of awareness should have a job title that reflects their dedicated awareness role. To encourage a deeper understanding and appreciation of this, we've added a new recommendation to the report this year, which can be located in the section, [Job Title](#).

- 2 The survey results show that an effective way to garner leadership support is to leverage peer comparisons via **benchmarking**. **Among those organizations whose leadership believe that their peer organizations are investing significantly,**

69% of them are treating security awareness training as a top priority.

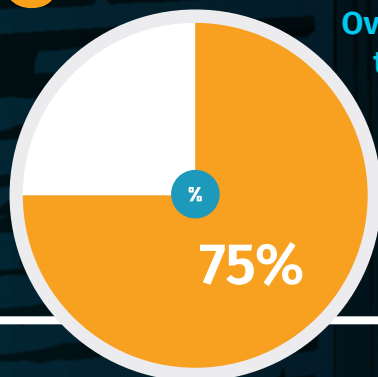


This is nearly a 10X increase over those organizations whose leaders who do not perceive their peers as investing in awareness.

Included in your report download is the [SANS Security Awareness Value of Managing Human Risk for Leadership presentation](#), which outlines tactics for gaining leadership support for your awareness program.

3

Time, not budget, continues to be an awareness professional's greatest challenge.



Over **75%** of security awareness professionals are part-time, meaning they're spending less than half their time on security awareness.

The implication is that awareness is simply mounted on to their other job requirements. This is the largest single factor limiting the growth and maturity of programs.

4

A lack of **soft skills**, such as communications and marketing, continue to limit an organization's ability to engage their workforce. Awareness professionals generally bring a dynamic set of technical skills, but can lack the skills to communicate their program needs. Outlined within **Appendix A** of this report, information can be found on the expectations, requirements, and skills recommended for a typical security awareness & communications manager-focused role. There is also detailed information regarding the job description and mapping to the NIST NICE Framework.

5

The data shows a strong correlation between full-time employee (FTE) staffing, program maturity, and success.

Programs have achieved success at changing behavior when there have been at least 2 FTEs dedicated to awareness.

Organizations reporting successful change in culture and metrics programs indicate 4 FTEs dedicated to awareness.



While there is a general tendency to isolate individual employees as the cause of security-related issues, the data within the report demonstrates that addressing an organization's human cyber risk is best handled by making consistent systemic training investments. This report examines the most effective steps to address them, enabling you to benchmark your awareness program against your peers and other organizations.

About This Report

Overview

The SANS Institute conducts a global annual survey of security awareness professionals and this year, 1,570 qualified respondents completed the survey from hundreds of cities in countries all over the world. In its fifth annual release, this SANS Security Awareness Report gathers results from this survey and correlates the trending reported data. By reporting on these results, we can enable security awareness professionals to make data-driven decisions on how to improve their security awareness program and benchmark their program against others.

We continue to conduct a year-over-year analysis by comparing key trends. However, in some cases, the conclusions throughout this report might lean toward the subjective side. Therefore, we've provided commentary and observations to the raw data that has been presented as graphs or tables. This empowers you to reach your own conclusions on the data pulled from the survey.

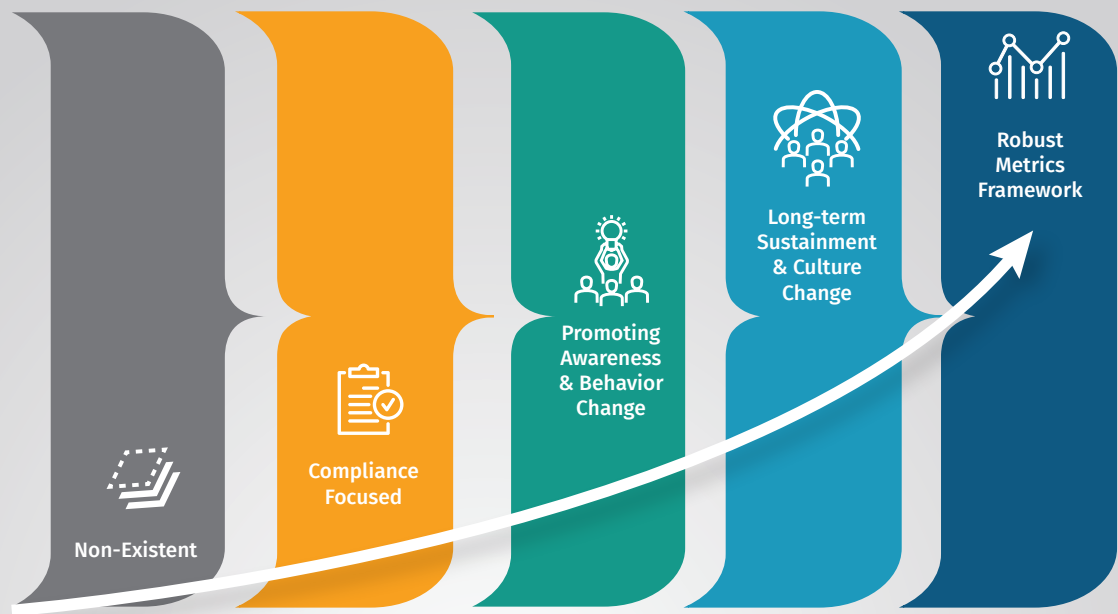
How to Measure Success

This report's intention is to help you identify what successful awareness programs are doing effectively and what failing or immature awareness programs could improve upon. We define success using the **Security Awareness Maturity Model™**.

Established in 2011 by over 200 awareness professionals, the Security Awareness Maturity Model grants organizations with the ability to easily identify where their security awareness program is currently at, where a qualified leader can take it, and outlines the path to get to where they want to be.

The model is based on five distinct stages, each building upon the previous stage.

SANS Maturity Model®



Non-Existent: In this stage, an awareness program of any capacity does not exist. Employees have no idea that they are a target to cyber attacks. They are not aware that their actions have a direct impact to the security of the organization, and they do not know or understand organization policies. Anyone could easily fall victim to attacks.

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

Promoting Awareness & Behavior Change: Within this stage, the program identifies training topics that have the greatest impact in supporting the organization's mission and focuses on those key topics. The program goes beyond annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work and at home. As a result, people understand and follow organization policies and actively recognize, prevent, and report incidents.

Long-Term Sustainment & Culture Change: Program has the processes, resources, and leadership support in place for a long-term lifecycle, including at least an annual review and update of the program. As a result, the program and cybersecurity are an established part of the organization's culture.

Robust Metrics Framework: When a robust metrics framework exists, there is the ability to track progress and measure impact. As a result, the program continuously improves and there is a clear return on investment. This does not imply metrics are limited to the last stage of the model. Metrics are an important part of every stage. This stage simply reinforces that to truly have a mature program, you must not only be changing behavior and culture, but have the metrics to demonstrate that change.

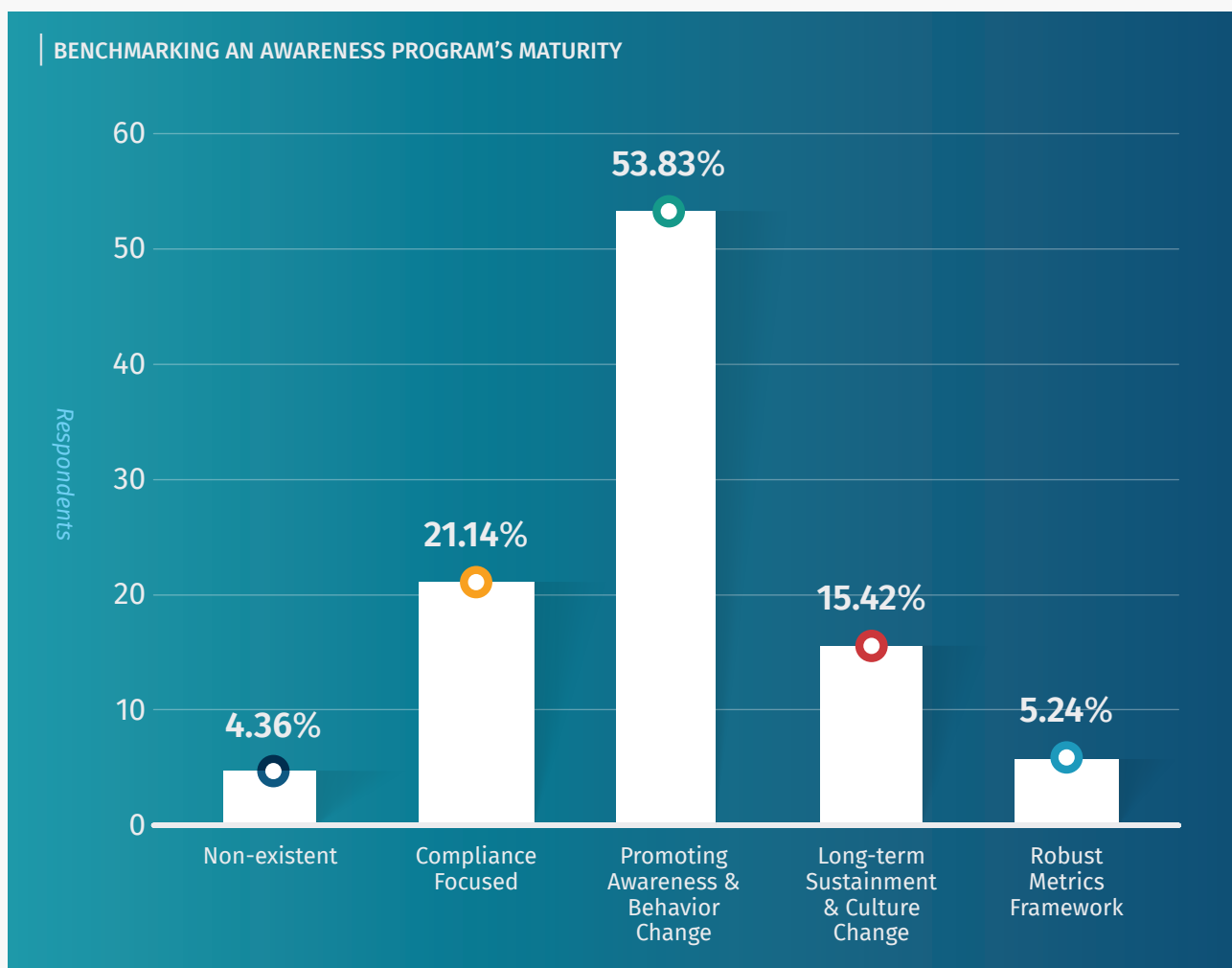
One of the key survey questions sought to determine which specific stage the respondent believed their awareness program to fall under. We then compared those results to the additional data provided.

There are multiple ways organizations can leverage the maturity model. The first is to benchmark your organization against others. A second approach is to use the model as a simple, but highly effective tool to communicate to leadership your goals and the program's value to your organization. Finally, the model is often used as a framework, a roadmap showing each stage of the lifecycle and the steps required to achieve them.



Benchmarking Your Program's Maturity Level

Over the past three years, there's been a continuous decrease in the two most immature stages, non-existent programs (from 7.6% to 4.36%) and compliance focused programs (from 27.1% to 21.1%). At the same time, there's a clear uptick in the two most mature stages, culture change and metrics framework (up 5% each). **This demonstrates a slow, but steady increase in program maturity over the past three years.**



Blockers and Supports

Awareness programs typically receive strong support from key departments and roles, including communications, security, and senior leadership, but many programs continue to struggle with support from their operations and finance departments. This remains unsurprising, as most awareness programs have a significant budget and operational impact on the organization. What's interesting about the data in the graph *"What Departments Block or Support Awareness Programs?"* is that two primary communications-forward departments, marketing and human resources appear to be on the rise as key blockers in executing a quality awareness program.

Below are several suggestions on addressing these common blockers. When addressing blockers, keep in mind they needn't be converted into complete supporters. In many cases, just shifting their position to 'neutral' can be effective. Successful awareness programs can still excel with detractors, but blockers need to be addressed.



Action Items

Finance

All security awareness programs come with a price tag. Awareness professionals should focus on improving the way they're justifying those costs by not only demonstrating the impact of a training program, but also demonstrating the value of the impact it can have on the overall organization and the program's mission. Consider analyzing costs due to past breaches, costs of compliance failure, or cost requirements to meet partner or vendor security requirements. Then, add up the costs of the security awareness program you intend to roll out and use these two metrics to demonstrate that by investing in security awareness, you can dramatically reduce those other costs.

Operations

Security awareness programs have a significant operational impact. These range from lost employee work time costs, the politics of mandatory training programs, and the complexity related to operating the programs themselves. In order to address the typical concerns around operational cost and disruption, there are two actions to consider. One, simplify awareness programs wherever possible to minimize the operational impact to the organization. This includes minimizing the topics you focus on that have the greatest impact. Two, involve the operations team from the beginning of your planning process and consider adding them to your security awareness advisory board. Make sure your operations team has an active voice in how your program is rolled out, and when.

Still Struggling?

If you are struggling to address your program blockers, consider asking a senior champion for guidance, someone who is a leader or executive and is a believer in your program. Ask them how to best engage or handle specific blockers. Often, they can provide added guidance or insight with a different perspective on how to handle your challenges.

Predicting Success

Leadership Support = Program Maturity

Consistent with five years of data collection and research, the most important independent variable in predicting the maturity level of your security awareness program is **leadership support**.



Action Items

Gaining Leadership Support: Peer Pressure is a Factor

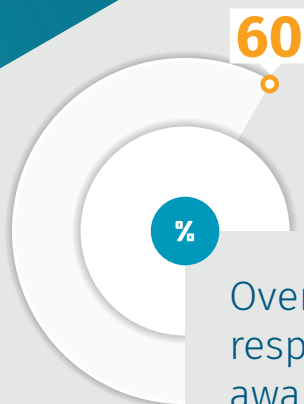
This year's survey results surprisingly showed that peer pressure has a distinctive role in determining whether leadership treats security awareness training a top priority.

Only 7% of organizations whose leadership does not believe their peer organizations are investing in security awareness are treating security awareness as a top priority. Alternatively of organizations whose leadership believes that their peer organizations are investing significantly, a staggering 69% treat security awareness as a top priority.

In the effort to gain leadership support, it is of paramount importance to ensure that the leadership is aware of the investment made by peer organizations on security awareness training. Peer pressure often triggers leadership support on treating security awareness training as a top priority.

Budget and Program Success

Mirroring previous results, survey respondents indicated this year that the size of their budget is not a clear indicator of program success. In fact, over 60% of respondents were not aware of their budget allocation for security awareness. This lack of outlined budget indicates this field is still immature. Work with your leadership to identify clear goals and budget for funding your program.



Over 60% of respondents were not aware of their budget allocation for security awareness.

Additional Action Items

Reports

Security reports, meaningful data, and statistics help demonstrate to leadership the need to address human risk. It also demonstrated how other organizations are actively leveraging awareness programs to effectively manage their human risk. One such report is the [annual Verizon DBIR](#), which highlights the need to address human risk. Another option is to join and work with industry security groups, such as your industry's [ISAC \(Information Sharing and Analysis Center\)](#).

Presenting to Leadership

Use the [SANS Security Awareness Value of Managing Human Risk for Leadership](#) presentation. This slide deck presentation was designed to help you communicate and demonstrate to leadership what human risk is, how awareness programs effectively manage human risk, and how these programs align with the overall strategy of the organization.

Breach

Never let a breach go to waste. They are powerful motivators and teaching tools. If your organization encountered a recent internal incident that was human related, use that moment to help drive the justification for your program. You can also work with your Security Operations Center (SOC) or Incident Response (IR) team and document all human related incidents in the past six months and the related costs. Don't have any breaches? Try using breaches that have occurred within your industry or to peer organizations.

Impact

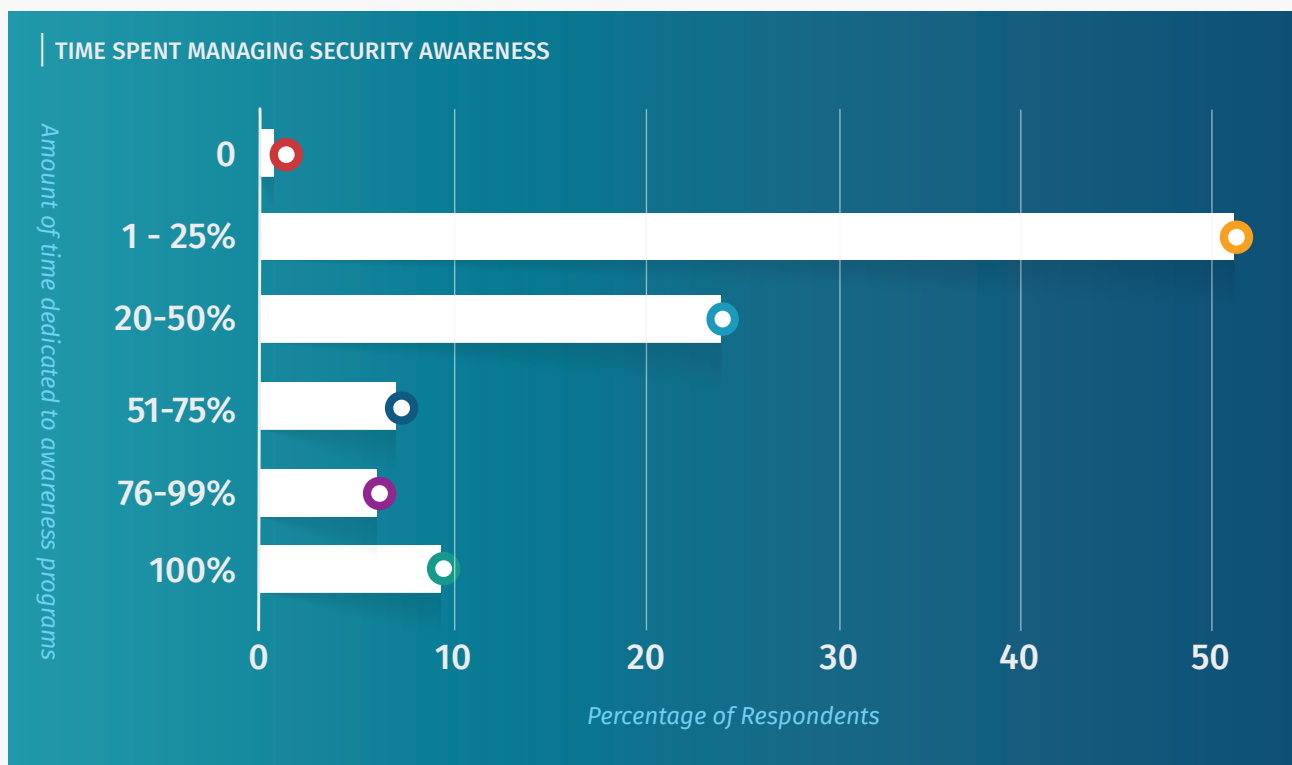
Dedicate at least four hours each month to collecting and communicating the impact of your awareness program to your leadership. Enable them to better understand and regularly see the value of your program. Not sure which metrics to collect? [SANS Security Awareness Metrics Matrix](#).

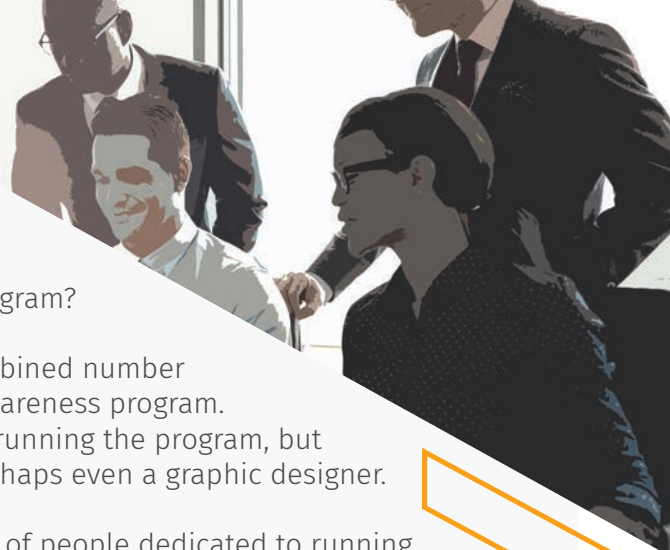
The Most Valuable Resources for Security Awareness

For the third consecutive year, the data clearly shows that lack of time and staffing were the top reported challenges facing awareness professionals. Over 75% of security awareness professionals spend less than half their time on awareness.

We found a small, but statistically significant correlation between the reported maturity level and the percentage of time devoted to the program. Those who spend 75% or more of their time dedicated to awareness reported a maturity level of **Long-Term Sustainment & Culture Change** 32% of the time. Those who reported spending 25% or less of their time dedicated to awareness reported a maturity level of **Long-Term Sustainment & Culture Change** only 13% of the time.

Security awareness is still too often perceived as a part-time job, which dramatically impacts the ability for organizations to mature their awareness program. Just as your Incident Response, Security Operations Center, or EndPoint security teams have full-time individuals dedicating their full effort, managing human risk with a robust awareness program requires full-time focus.



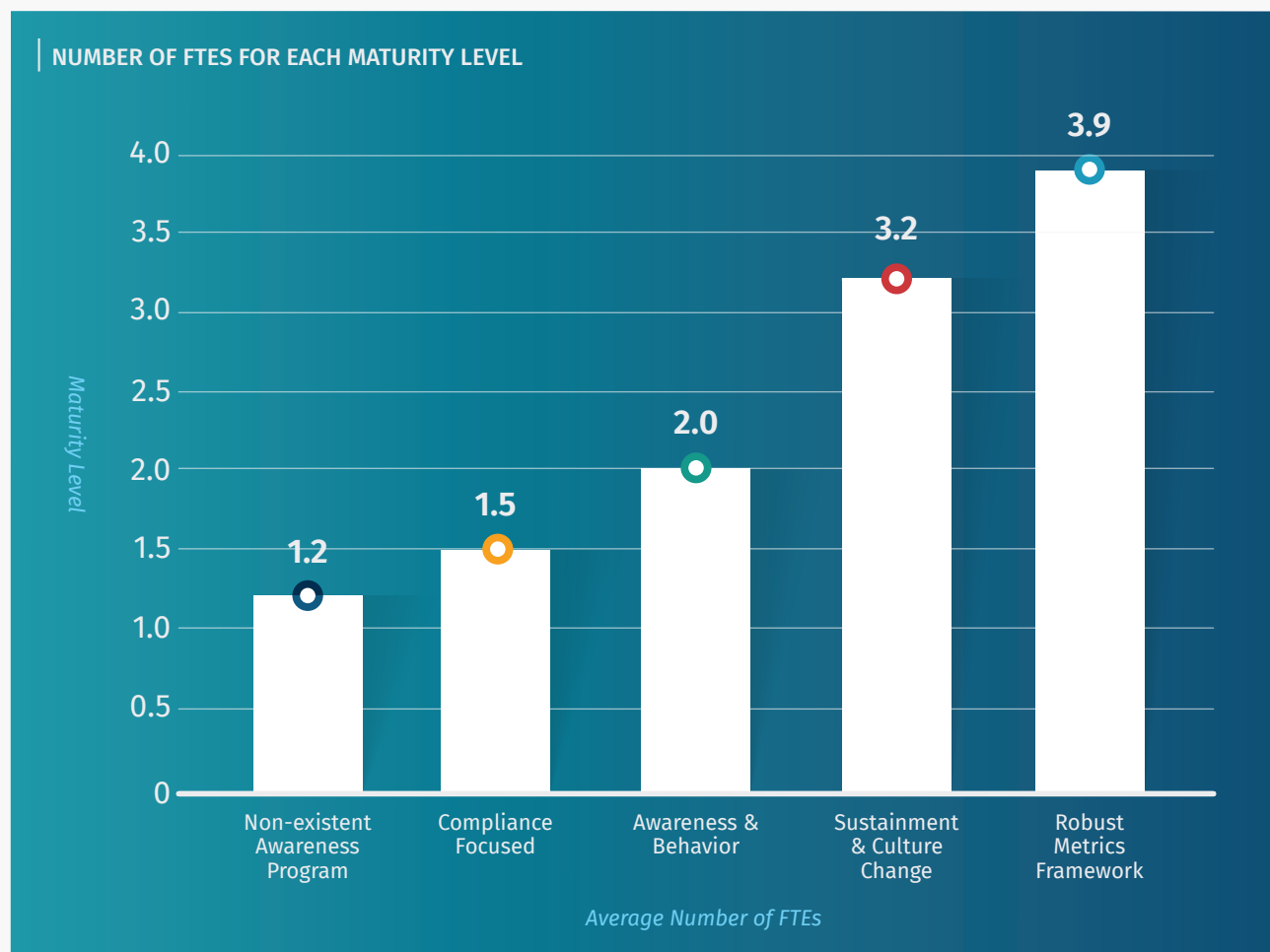


How many people should be involved in your awareness program?

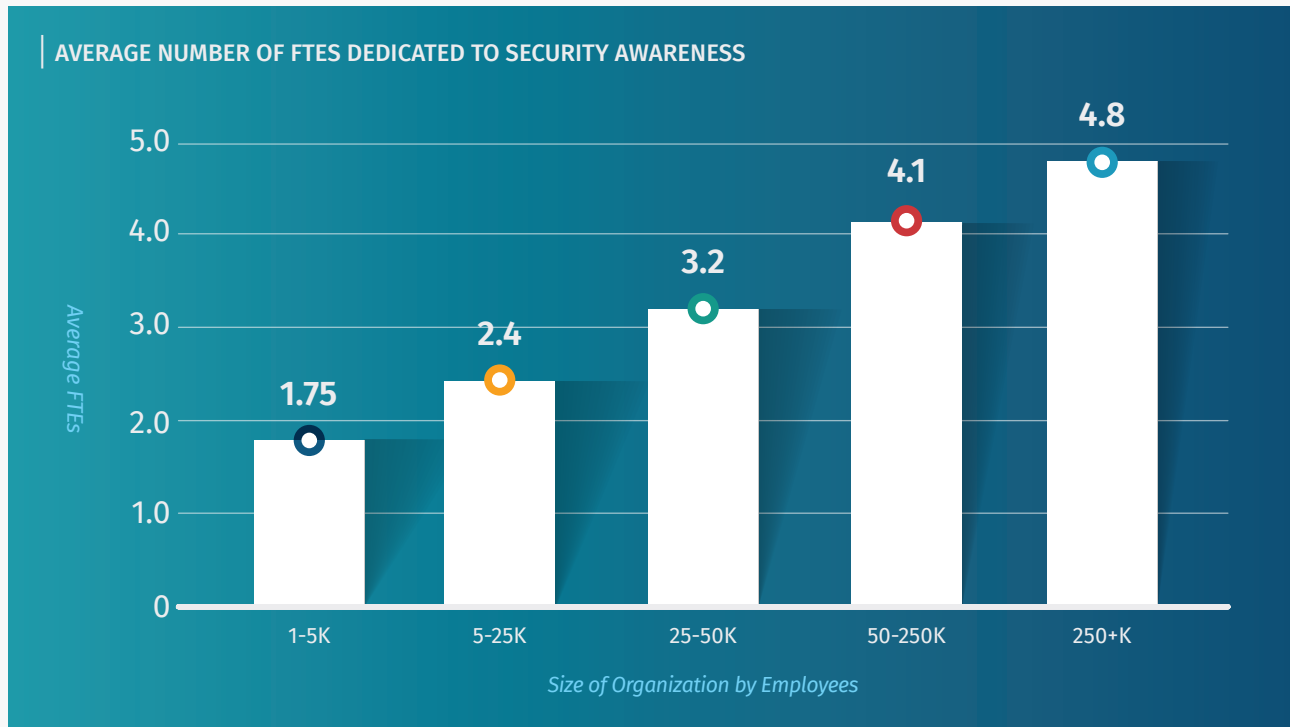
Let's dig into this a little. A good metric is to add up the combined number of FTEs (full-time employees) you have dedicated to your awareness program. This would not only include your security awareness officer running the program, but also the part-time efforts of someone from marketing or perhaps even a graphic designer.

The survey data revealed a strong correlation to the amount of people dedicated to running an awareness program to the maturity of an awareness program. The more people you have, the more mature your program. This makes sense. If your organization has all the budget in the world and all the leadership support to back it up, but just a single employee managing the entire program, who can spend only 25% of their time to awareness (.25 FTE total), how likely is it to drive real impact? It's incredibly difficult without full-time dedication to grow any program beyond compliance. Remember, awareness is not a technical solution, it's a human solution. This means your awareness team needs to be talking to, engaging, and collaborating with others throughout your organization. That takes time.

So, how many people should an organization employ for a robust awareness program? That depends on what level of maturity you want to achieve.



This maturity level visual offers a general guideline, based on an organization of 8,000 people. If your organization is significantly smaller, such as 500 employees, obviously these numbers may be smaller. Look at the average number of FTEs dedicated to awareness based on the size of your organization.



What this data tells us is that a direct awareness-to-employee ratio does not work. As workforce size increases exponentially, FTE size increases incrementally.

The data has been hinting at this for several years, which makes sense.

For many job tasks, such as configuring and deploying computer-based training (CBT) or launching a phishing simulation program, it

doesn't matter if you have 500 people or 50,000 people, the time requirements are similar. What the data indicates

is that larger organizations have more FTEs not just

because of the larger workforce, (that plays a

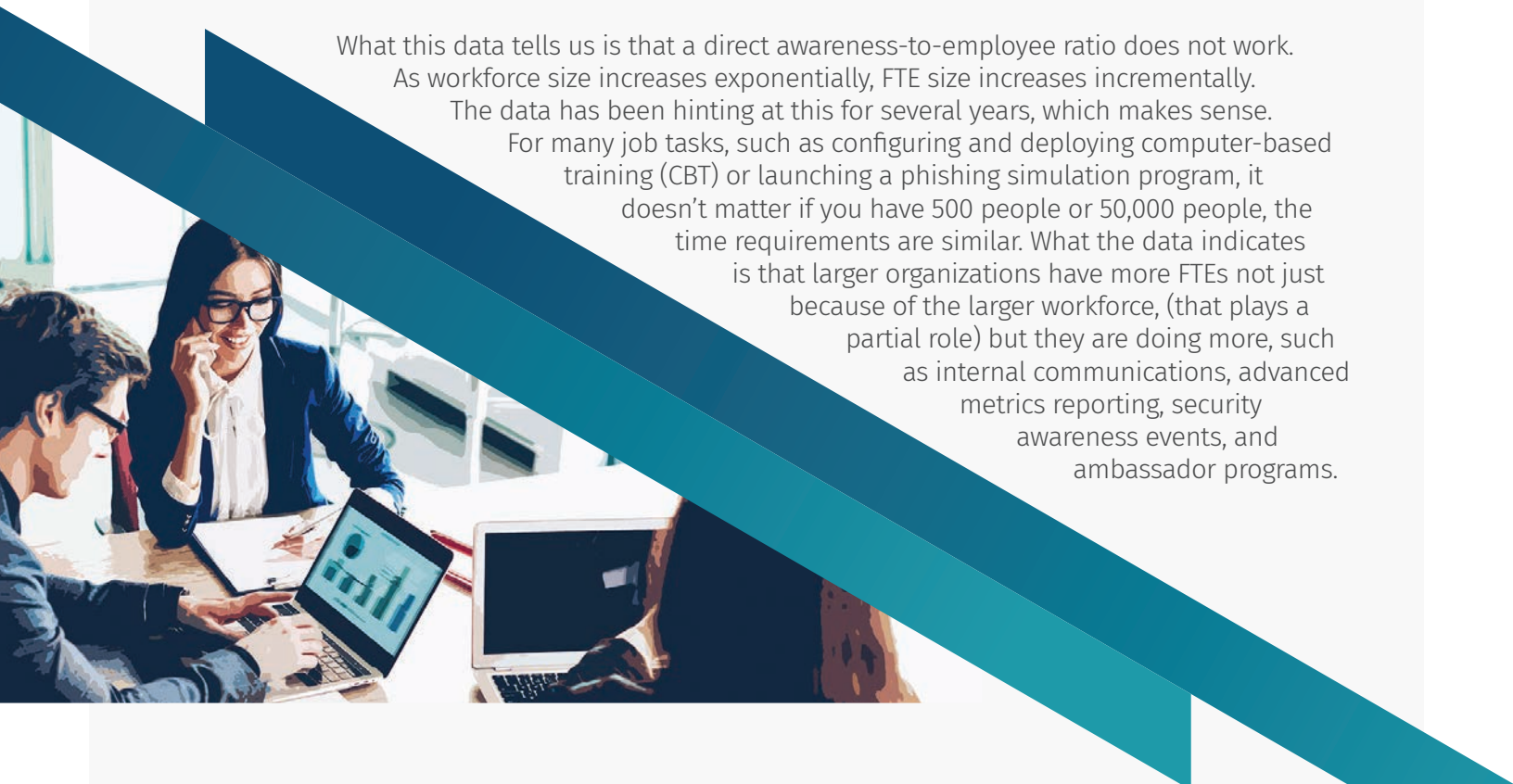
partial role) but they are doing more, such

as internal communications, advanced

metrics reporting, security

awareness events, and

ambassador programs.



Action Items: Get the Most out of Your Time

Buy Time

Use your budget to buy yourself some time. Don't create a monthly newsletter yourself, contract someone to do it for you or license materials from a vendor. Instead of creating a survey, hire a contractor specializing in social science. (If you're just getting started, a great resource to survey building is the book ["Ask" by Ryan Levesque](#).) The more you're able to delegate, the more time you have to create partnerships with your organization, engage with others, and ultimately drive change with your program.

Partnerships

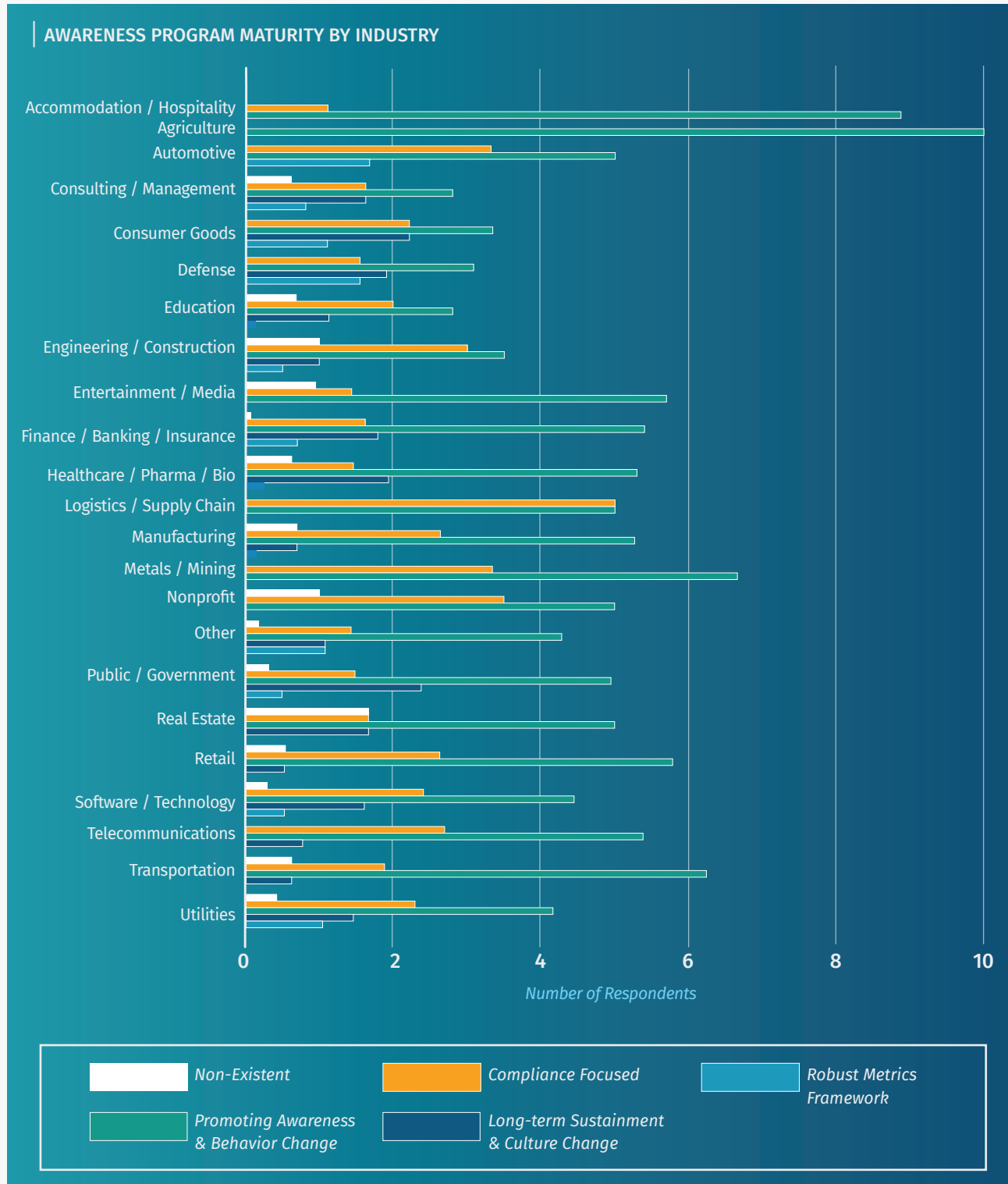
Reach out to other teams or departments such as marketing, graphic design, communications, or security operations. Partnering with other teams will help amplify your reach and allow you to drive adoption of the behaviors you wish to promote.

People

Identify the maturity level you want to achieve, then identify the personnel you will need to achieve that level. For example, will you need someone from the communications department, a graphic designer or an expert in developing surveys? Once you define their roles and estimated time involvement, it will likely be easier to get those individuals to contribute to the building of your program.

Analysis by Industry: Who is the Most Aware?

Below is a graph of the 2019 data as it associates maturity to industry. The data shows that the defense, retail, utility, and consumer industries report the most mature programs, while hospitality, agriculture, and entertainment display the least mature programs.

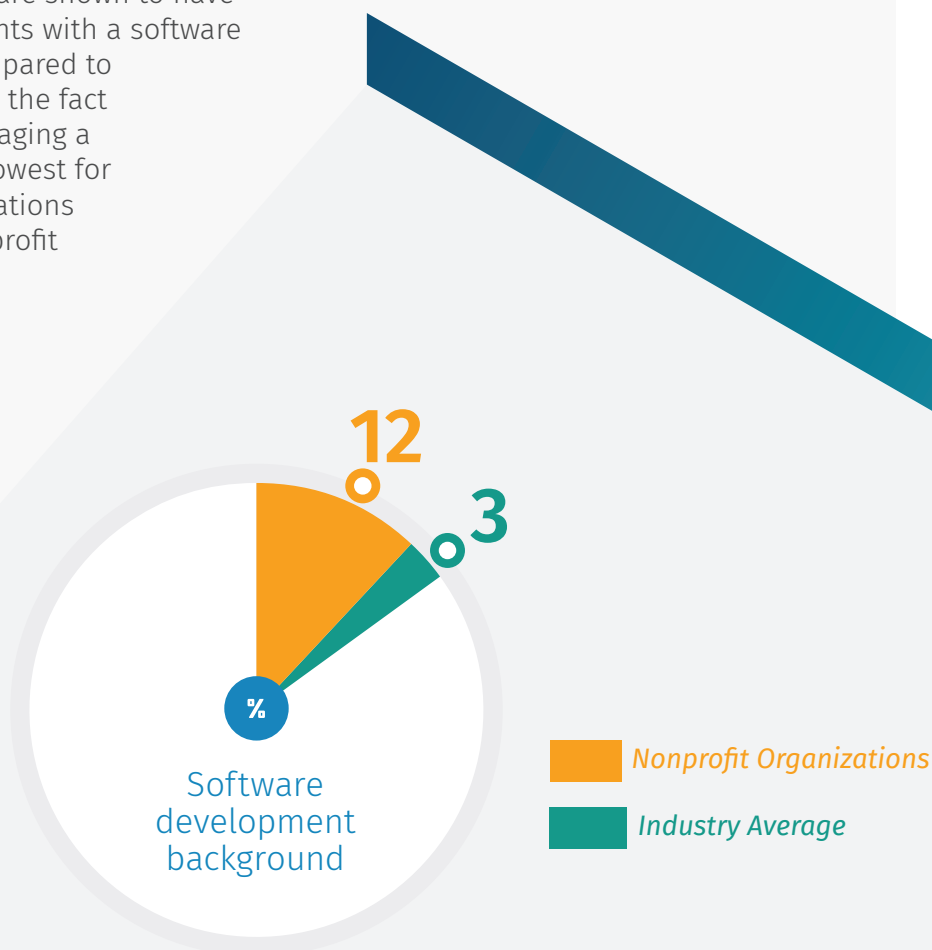


The data shows several interesting outliers from previous years. For example, while the retail industry receives the highest leadership support compared to other industries, it trails on all other performance measures. This anomaly could indicate that while retail leadership is keen on building a previously non-existent security awareness training team, their effort is very immature and the current maturity level and team size (FTEs) has room to grow in the coming years.

On the other end of the maturity spectrum are two industries: consulting and utilities. These industries demonstrate the highest maturity levels. While these industries differ significantly on team-size and number of trainings per employee, both enjoy high level of leadership and high budget per employee. (They're among the top five industries on both fronts.)

Another interesting data point within industries is the composition of security awareness teams. For example, only 7% of those involved in security awareness in engineering/construction have a background in information security, which is significantly lower than the average of 42% across industries. Instead, most of their awareness team (64%) has a background in information technology (IT). This may indicate that, for engineering companies, they either have very small security teams or security awareness needs to be more tightly integrated with IT, making the composition of their awareness teams skew heavily towards those with a background in IT.

Meanwhile, nonprofit organizations are shown to have the highest percentage of respondents with a software development background - 12% compared to an average of 3%. This, coupled with the fact that the average time spent on managing a security awareness program is the lowest for respondents from nonprofit organizations (30%), appears to indicate that nonprofit companies require members of the security team to be multi-taskers, responsible for not only security awareness training but also other tasks that require skills acquired from a software development background.

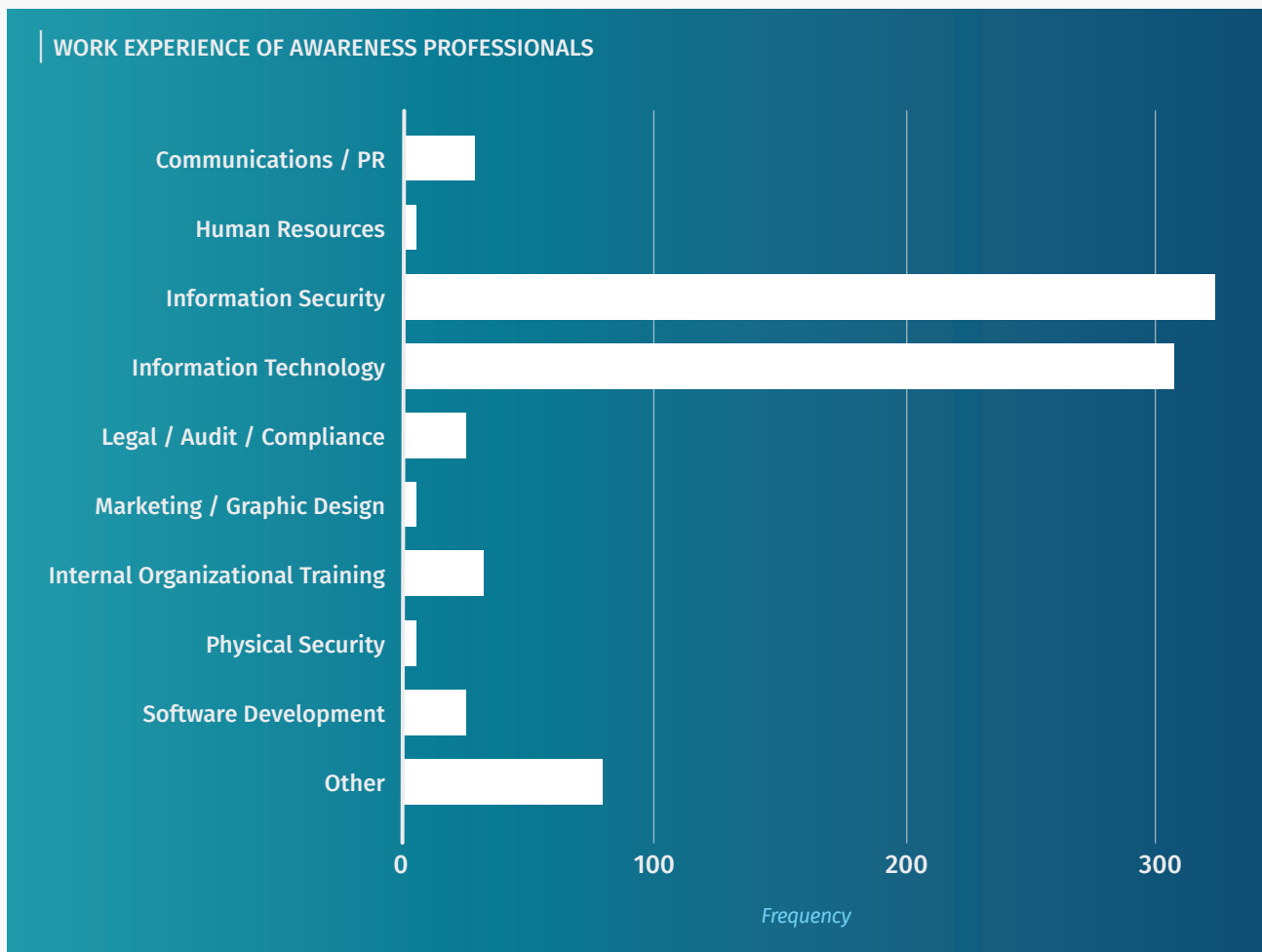


Demographics – Who Runs Security Awareness Programs?

Background

This year's data shows that a majority (80%) of awareness professionals come from some type of technical background. **Less than 20% have a non-technical background such as communications, marketing, legal, or human resources.**

A technical background is an advantage in that you have an understanding of the technologies and human risks involved and the behaviors that most effectively manage those risks. However, the challenge is these same individuals often lack the skills to effectively communicate those risks and engage employees in a way that changes behavior. Soft skills are a critical component to the success of a thriving awareness program.





We observe that those most familiar with the technology often suffer from a condition referred to as the “**Curse of Knowledge**”. This refers to a cognitive bias and means that the more expertise a person has on a subject, the more difficult it can be for them to teach or communicate about it. Security professionals often perceive security, especially security awareness, as being “simple” because it, and the related technology, are a part of their day-to-day life. Experts can make assumptions that security and technology are “common knowledge” for everyone else and they then often build their awareness program based on these misconceptions. As a result, **what experts tend to communicate might not align with what non-experts need to comprehend and apply.**

This not only creates less-effective training materials, but also impacts communication to peers and leadership at many organizations. Technical and security experts should take care to evaluate their bias. They should consider the language they use to speak to learners and leaders. They should also communicate in terms they best understand. This does not mean condescension, rather, a careful study of using the vernacular that will best illustrate the behaviors you aim to teach. In most cases, learners need training that assumes little in the way of security concepts and leaders need to understand how the awareness program supports the organization’s mission and goals.

Action Item for Communicating to Learners and Leadership

Know Your Bias

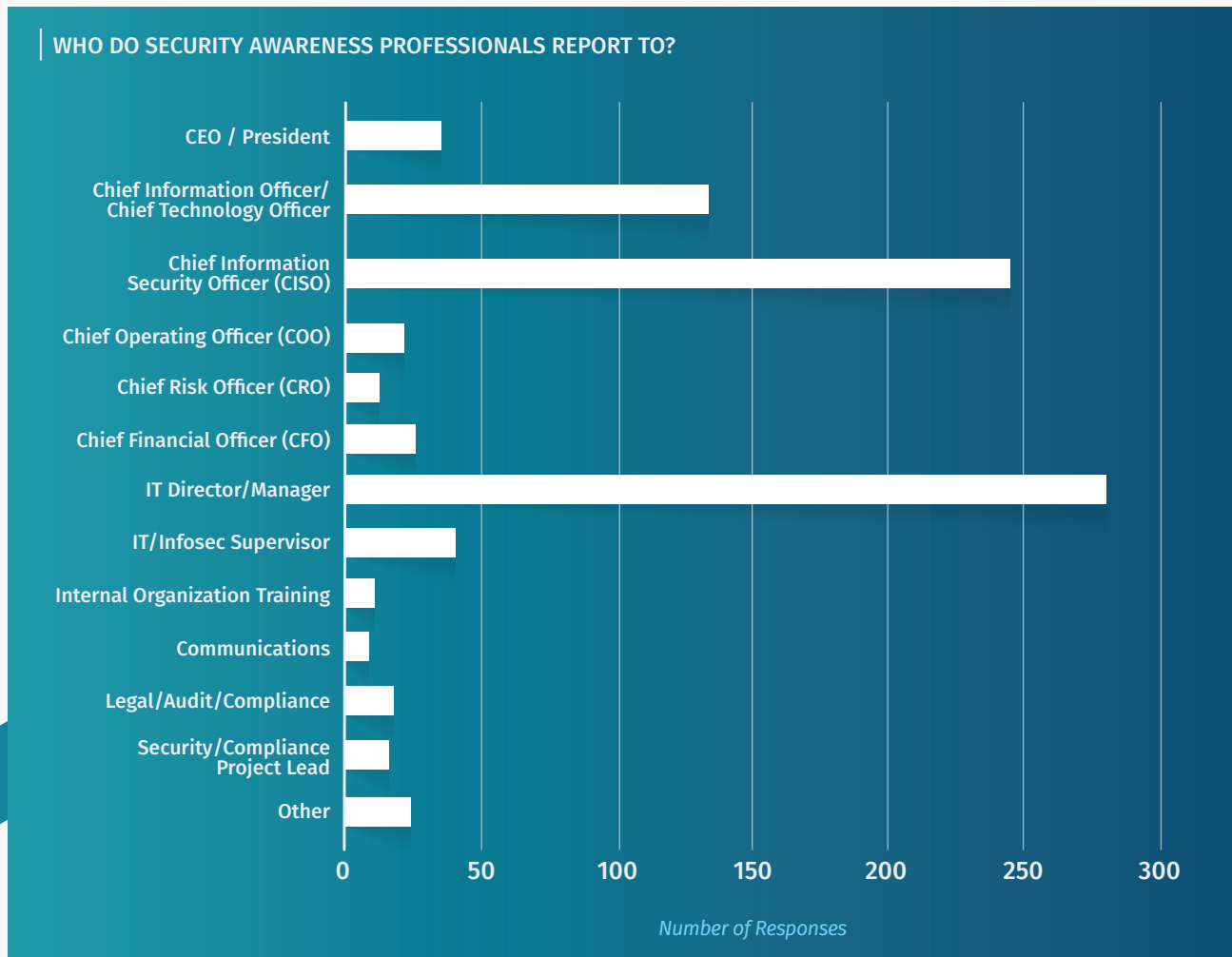
If you are a technical or security expert, make sure you work with others to perfect your messaging. Your expertise is beneficial as long as you pay careful attention to how it contributes to your program.

Soft Skills

Enlist someone on your awareness team who has the soft skills required for effective communication and engagement. This can include training someone on your team to develop soft skills, partnering with your communications or marketing department, or even have one of their members embedded into your security awareness team. Or consider acquiring the appropriate soft skills to help more effectively engage your workforce. Some excellent books on this topic includes: **Nudge, Switch, Thinking, Fast and Slow, Leading Change and Starting With Why**. We have also included a job description template for a Security Awareness and Communications Manager role in **Appendix A**.

The Organizational Structure of a Security Awareness Department

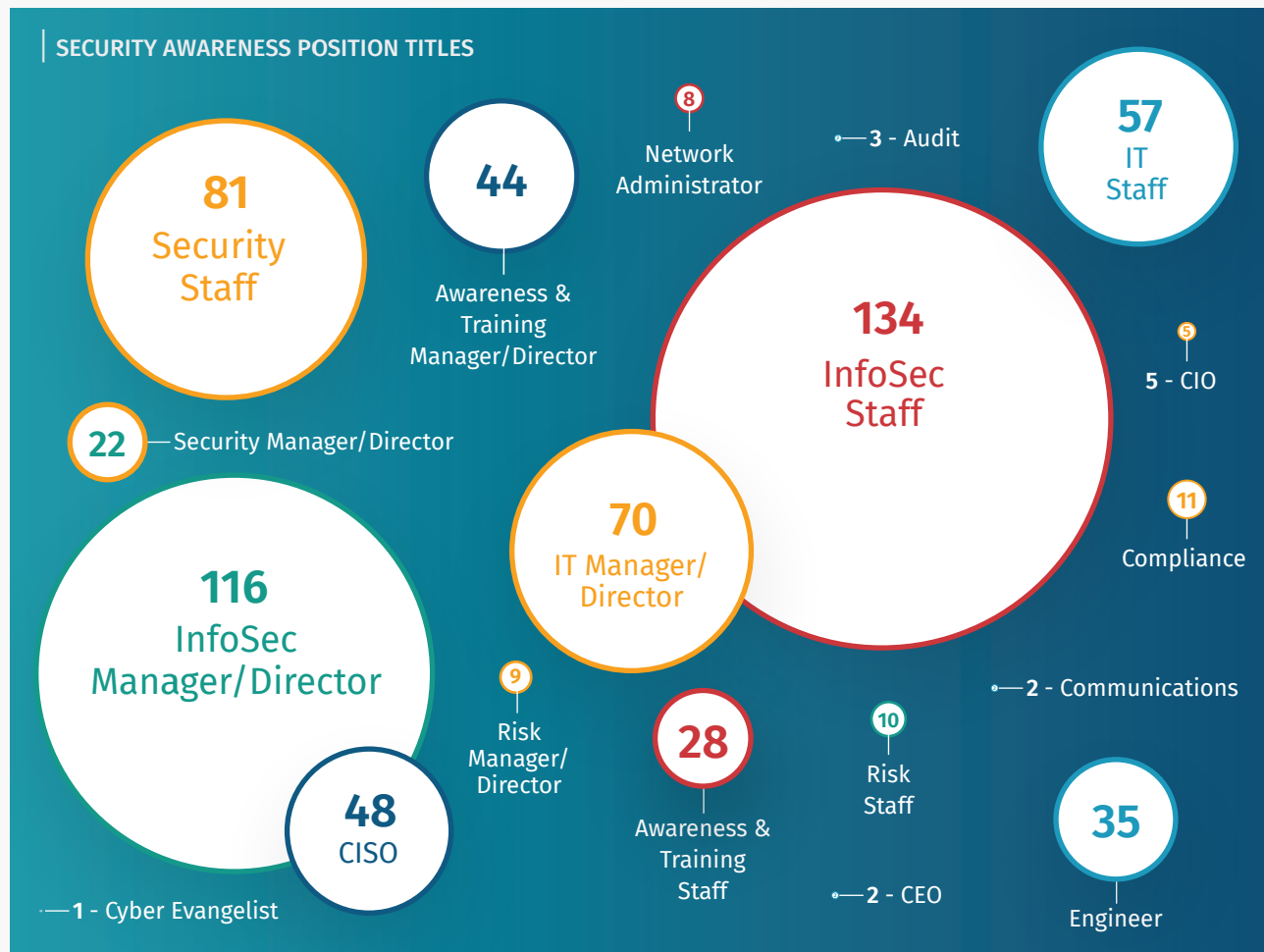
Most security awareness officers report to someone on the technical side of their organization or with most senior levels of leadership. This is beneficial, as it ensures awareness is directly involved with the security and technology teams. However, we want to ensure these individuals are partnering and working with the communication-forward departments, such as human resources.



Job Titles for Security Awareness Professionals

Job titles are an interesting descriptor, but this year's survey has produced some fascinating results. Respondents were given a free form option to submit a title that applied to them relating to security awareness. The goal was to identify trends of the most common titles in this field.

What was the result? The biggest finding was that less than 10% of the titles had the words *Awareness* or *Training* in them. Most titles are technically focused. This once again demonstrates the part-time nature of this role and the overall immaturity of the security awareness industry. There's a lot more growth on the horizon.



Action Item

Position Title

Have your organization demonstrate their commitment to security awareness by assigning the appropriate person with a title that aligns with their goals. In other words, have a title that is focused on managing human risk. Examples of titles used in other organizations include:

- Security Awareness and Education Manager
- Director of Security Outreach and Engagement
- Security Communications and Training Leader
- Security Awareness and Culture Lead

Summary of Key Action Items

Ultimately, security awareness is hard. However, there are some key steps you can take. To recap the takeaway points:

1

FTEs

You most likely need at least 2 FTEs to change behavior at an organizational level. To achieve a truly mature program, including a strong metrics framework, you will need at least 3.8 FTEs. Your FTE numbers may vary depending on your company size, organizational structure, and requirements. However, we recommend you use this as a starting point for organizations with 5,000 or more employees.

2

Title

Demonstrate organizational commitment to the program, not only by having someone dedicated full-time, but ensure they have a title that aligns with their goals. In other words, have a title that is focused on managing human risk. This can include terms such as Security Awareness and Communications Officer, Director of Security Outreach, Security Engagement and Education, or Security Cultural Manager.

3

Leadership Support - Peer Pressure

Overall, security awareness programs are improving in their leadership support. However, if you are struggling to gain or maintain that support, peer pressure can be one of the most effective means. Demonstrate to your leadership how other organizations in your industry have mature awareness programs and continue to invest in them.

4

Partnerships

Build partnerships and collaborate with others in your organization to help you. This is especially important for any key departments that are blockers, such as finance or operations. Do not underestimate the power of building relationships and taking others out to lunch. For operations, get them involved in the planning process from the beginning.

Summary of Key Action Items

– continued –

5

Buy Time

If you have a budget, use that to buy yourself time. Instead of creating materials yourself, hire a graphic designer or license materials from a vendor. Instead of creating a survey, hire a contractor specializing in social science. The more you can delegate, the more time you have to make a difference.

6

Know Your Bias

If you are a technical or security expert, work with others who can help you polish your messaging. Your expertise is a plus as long as you pay careful attention to how it contributes to your program.

7

Soft Skills

Have someone on your awareness team who possesses the soft skills required for effective communication and engagement. This can include training someone on your awareness team to develop the soft skills, partnering with your communications or marketing department, or even have one of their members embedded into your team. Review [Appendix B](#) for more details.

8

Champion

Partner with a strong champion within leadership. Have that leader either help communicate the value of your program to other leaders or have them help you craft your message in the language that business leaders can comprehend and act on. A champion can also be integral in your effort to better understand and address certain blockers to your program.

Appendix A – Hiring Requirements for a Security Awareness Officer

A common mistake organizations often make in hiring a dedicated security awareness resource is that they look for someone who displays a strong technical background, computer science degree, or specific security certifications. The most successful security awareness officers have strong soft skills, often in communications, marketing, or change management backgrounds. They are generally good communicators, effective at building strong partnerships, and love working with people. A strong security background is not required, as these individuals will be working directly with your security team, leverage them for their security expertise. As long as your security awareness officer has a passion and willingness to learn and a strong security team to work with, they do not need to be security experts.

Here is an example of a job description for a security awareness officer:

Security Awareness Officer

This individual is overall responsible for our security awareness and education program. Ultimately, this person's job is to help our security team identify and manage our human risk by changing organizational behavior and ultimately create a secure culture.

Our Security Awareness Program Requirements

This is what we are looking to achieve with our awareness program.

1. Ensure that our security awareness program helps us meet all industry regulations, standards, and compliance requirements.
2. Ensure that our security awareness program identifies the scope of who needs to be trained in the program.
3. Ensure that our security awareness program communicates our security policies and requirements so that people know, understand, and can follow them.
4. Work with the security team to identify the top human risks to our organization and the behaviors we need to change to manage those risks. Ensure that our program is effectively changing these behaviors so our workforce acts in a secure manner, reducing the most risk to our organization. In addition, the security awareness officer should identify if any roles require additional or more specialized training and ensure those roles receive it.
5. Create a positive program that engages people, one that people want to interact with and learn from. In addition, we want to ensure we are focusing on changing behaviors both at home and at work. Ultimately, we want our workforce to demonstrate the same secure behaviors regardless of where they are or the devices they are using.
6. Structure and maintain this program to be long term, so we are not changing just behaviors but ultimately creating a secure culture.
7. Create a metrics framework that can effectively measure and communicate the impact of the program.

Skills and Experience

1. Ability to communicate and market complex messages in a simple, clear and engaging manner within our organization. Should have experience with different methods of communications, such as social media, blogging, videos, online messaging, printed materials, hosted events and other methods. A key part of effective engagement is leveraging multiple methods of communications.
2. Project management experience, the ability to plan, manage and maintain a complex, organization wide program over the longer term.
3. The ability to take the initiative, reach out to and coordinate with different people in different departments. Collaboration and partnering with others, to include people in other countries, is a key factor to success.
4. Understand the concepts of culture and how culture impacts how people both behave and learn.
5. Understanding of learning theory or instructional design, including models such as ADDIE and ARCS.
6. Extensive experience in cybersecurity or information technology is not required. However, you will be expected to continually work with and learn from our security team and stay current with the latest cybersecurity concepts, terminology, and risks.
7. SANS Security Awareness Professional (SSAP) credential or any certifications in Change Management, Instructional Design or Communications will be considered a plus.
8. Formal training related to security awareness and cybersecurity are also a plus.

Appendix B – NIST NICE Framework Mapping

The **NIST NICE Framework (SP800-181)** is a formalized approach to defining the cybersecurity workforce. The purpose of the framework is to enable organizations to effectively identify, hire, track, train, and develop a qualified cybersecurity workforce. It also enables those who wish to enter the cybersecurity workforce to better understand their options and helps those already in the workforce to define and develop their career path.

The framework achieves this by creating a common lexicon, comprised of the following components:

- 7 Categories: Broad grouping of cybersecurity functions.
- 33 **Specialty Areas**: Specific areas of cybersecurity work.
- 52 **Work Roles**: The comprehensive grouping of work, essentially what you or I would refer to as job descriptions.

NIST NICE then defines each work role with a title and description, **tasks** expected for that work role, and the **knowledge**, **skills**, and **abilities** (KSAs) that the respective work role is expected to have.

By creating this specific lexicon, it ensures that everyone is speaking the same language. For example, if you need to hire someone for your incident response team, you can provide the **exact requirements for an incident responder** to your human resources team based on the framework. Similarly, people looking to be hired in such a position know exactly what is expected of them.

Unfortunately, the NIST NICE Framework does not have an adequate work role for security awareness, as defined in the job description above. We have defined one using the framework below.

Work Role Name	Security Awareness & Communications Manager
Work Role ID	OV-TEA-003
Specialty Area	Training, Education and Awareness (TEA)
Category	Oversee and Govern (OV)
Work Role Description	Builds, maintains and measures the organization's security awareness and communications program with the goal of securing the workforce's behaviors and ultimately creating a secure culture.
Tasks	T0001, T0024, T0025, T0030, T0073, T0094, T0101, T0157, T0206, T0224, T0248, T0316, T0320, T0321, T0322, T0323, T0341, T0345, T0352, T0357, T0365, T0367, T0380, T0382, T0384, T0425, T0437, T0442, T0443, T0450, T0451, T0467, T0519, T0520, T0534, T0535, T0926
Knowledge	K0002, K0004, K0115, K0124, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0239, K0243, K0245, K0250, K0252, K0628
Skills	S0052, S0070, S0100, S0101, S0296, S0301, S0356
Abilities	A0004, A0006, A0011, A0012, A0013, A0014, A0016, A0017, A0018, A0020, A0022, A0057, A0070, A0083, A0089, A0105, A0106, A0114, A0119, A0171

A Big Thanks

We would like to take a moment and thank our contributors, the analysts of Kogod Cybersecurity Governance Center (KCGC). The KCGC is a research initiative of American University's Kogod School of Business (KSB) focused on the governance and management of cybersecurity.

Collecting data is easy. Sifting through all the data and creating a report that people can actually use is HARD. A big shout-out to the following who volunteered their time to make this report happen.

Contributors

- **Heng Xu**, Professor of IT and Analytics at the American University's Kogod School of Business
- **Nan Zhang**, Director for the Kogod Cybersecurity Governance Center
- **Hannah Andrews**, Undergraduate Student, School of International Service (SIS) and Computer Science at American University
- **Adefunke Sonaike**, Graduate Student, Public Policy at American University



Authors

Lance Spitzner has over 20 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 founding of the Honeynet Project. Lance has published three security books, consulted in over 25 countries and helped over 350 organizations build awareness programs to manage their human risk. Lance is a frequent presenter, serial tweeter (@lspitzner), and works on numerous community security 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.

Dan deBeaubien is a 25-year veteran of information technology and a former CTO of Michigan Technological University. He has held a variety of posts throughout his career, including Senior Systems Administrator, Senior Telecommunications Engineer and Director of Information Technology Services and Security. Before joining the SANS team, Dan created Michigan Tech's Information Security Office and the positions of Chief Information Security Officer and most recently Chief Information Compliance Officer. He currently serves as Product Director at SANS Security Awareness.

Alyssa Ideboen has more than a decade of experience in writing and communications for organizations in the tech industry. She has authored research and reports on the growth and management of SaaS platforms and software, the rise of OTT technologies, adaptive software development, the use and implementation of electronic medical record (EMR) platforms, and security awareness. She is responsible for the development and education of security awareness materials available at SANS. Prior to working with SANS, Alyssa has served as head of global marketing for a variety of industry-leading training and software platforms.

Dr. Heng Xu is a Professor of IT & Analytics at the American University's Kogod School of Business, where she also serves as the Director for the Kogod Cybersecurity Governance Center. Before joining Kogod, she had a mix of academic and government background, being a professor at Penn State for 12 years, as well as a program director at the U.S. National Science Foundation (NSF) for three years. Dr. Xu's current research focus is on information privacy, data ethics, and data analytics. Her work has received many awards, including the NSF CAREER award in 2010, the Operational Research Society's Stafford Beer Medal in 2018, and a total of 10 best paper awards and nominations at various leading research conferences.

Dr. Nan Zhang is a Professor of IT and Analytics at the American University's Kogod School of Business. Dr. Zhang is a world-renowned expert on database systems and data analytics, having published over 100 research papers and served as a program director at the U.S. National Science Foundation (NSF) for both fields. Before joining Kogod, Dr. Zhang was a Professor of Information/Computer Science at Penn State, George Washington, and UT Arlington. His work has received several awards, including the NSF CAREER award in 2008 and Best Paper Awards or Nominations from IEEE NAS 2010, ICC 2013, ACM CIKM 2013, IEEE ISI 2015, and HICSS 2018 and 2019.

Hannah Andrews is a second-year undergraduate studying International Studies in the School of International Service (SIS) and Computer Science at American University. She has been a Research Assistant at the Kogod Cybersecurity Governance Center for the past year. Ms. Andrews is an Olson Scholar in SIS and has spent her past year conducting independent research on internet governance models, and she received the 2019 Academic Achievement Award for Excellence in Undergraduate Research or Creative Work by a Sophomore. In the Spring, she participated in the Atlantic Council's Cyber 9/12 challenge as the first undergraduate student selected to represent her school.

Adefunke Sonaïke is a Master of Public Policy student at American University, concentrating in Advanced Policy Analysis. Her primary research interests include science, technology, economic, and energy policy. Adefunke received her bachelor's degree in Political Science and Environmental Biology from Columbia University.

Questions? Comments?

If you have any questions or suggestions, we want to hear from you! Drop us an email at securityawareness@sans.org, find SANS Security Awareness on [LinkedIn](#), or reach us on [Twitter](#) at @SANSAwareness.

About SANS Security Awareness

SANS Institute is, by far, the most trusted and the largest source for information security training in the world. With nearly 30 years of experience, SANS information security courses are developed by industry leaders in numerous fields, including cybersecurity training, network security, forensics, audit, security leadership, and application security.


SANS Security Awareness, a division of the SANS Institute, provides organizations with a complete and comprehensive security awareness solution, enabling them to easily and effectively manage their human cybersecurity risk.

SANS Security Awareness builds content that is meaningful for all learners, including relevant and timely awareness topics, while presenting information in proven teaching methodologies and in formats readily digestible for everyone.

SANS Security Awareness has worked with over 1,300 organizations and trained over 6.5 million people around the world. Security awareness training content is translated into over 30 languages and built by a global network of the world's most knowledgeable cybersecurity experts. Organizations trust that SANS Security Awareness content and training is world-class and ready for a global audience.

The SANS Security Awareness program includes everything security awareness officers need to simply and effectively build a best-in-class awareness program.

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



©2019 SANS Institute. All Rights Reserved. This 2019 SANS Security Awareness Report (“Licensed Material”) is for non-commercial use and intended for informational purposes only. The Licensed Material contains copyrighted material, trademarks, and other intellectual property of The Escal Institute of Advanced Technologies, Inc. /dba SANS Institute (“SANS” or “Licensor”) and its affiliates in the United States and worldwide. Licensor hereby grants a worldwide, royalty-free, non-sublicensable, non-exclusive, irrevocable license to copy, display, republish, redistribute, reproduce, and/or share the Licensed Material, in whole or in part, for non-commercial purposes only (“License Rights”). All rights in the product names, company names, trade names, trademarks, logos, service marks, trade dress, slogans, and/or intellectual property rights in the Licensed Material belong to and are exclusively owned by SANS or our licensors or licensees. These License Rights do not transfer title and/or ownership to any product names, company names, trade names, trademarks, logos, service marks, trade dress, slogans, and/or intellectual property rights. The Licensed Material does not constitute legal, financial, professional, or healthcare advice and cannot be used for such purposes. If the Licensed Material is copied, displayed, republished, redistributed, reproduced, and/or shared, in whole or in part, the Licensor must be identified to receive attribution with the Licensor’s copyright notice. The use or misuse of product names, company names, trade names, trademarks, logos, service marks, trade dress, slogans, and/or intellectual property rights in the Licensed Material, except as permitted herein, is expressly prohibited, and nothing stated or implied confers title and/or ownership.



**SECURITY
AWARENESS**