SANS
SECURITY
AWARENESS

2018 SANS Security Awareness Report

Building Successful Security Awareness Programs

Table of Contents
Security Awareness Report

Executive Summary
Key Findings

Executive Summary
Key Findings Include:

The SANS 2018 Security Awareness Report analyzes the data submitted by 1,718 security awareness professionals from around the world to identify and benchmark how organizations are managing their human cyber security risk. The analysis includes how various factors including security awareness program maturity, funding, and staffing combine to make successful programs. Learning what best helps and most hinders security awareness programs enables organizations to make the most of their people, resources, and budget.

1 While many compliance-type programs exist, most awareness programs require at least 1.9 FTEs to substantively change behavior, and, the most mature programs, those with both cultural impact and a metrics framework, require on average 3.6 FTEs. Except the most basic compliance programs, mature and effective security awareness cannot be a part-time effort; having adequate, qualified and dedicated cyber security awareness staff is essential.

2 Time, not budget, are often reported as an awareness officer's greatest challenge. Awareness officers must leverage both budget and partnerships to most effectively utilize the time they have managing their programs.

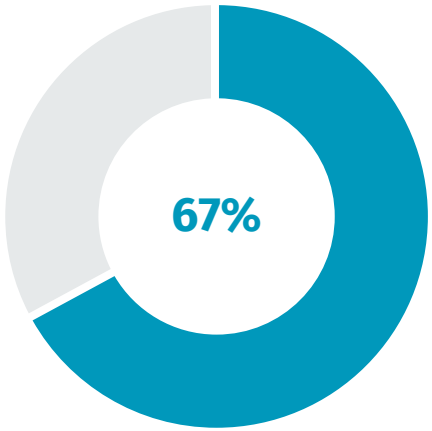
3 Soft skills such as communications and marketing are key to engaging and changing the behaviors of the workforce. Ensure that at least one person on your security awareness staff has soft skill expertise or is partnering with others that have it.

4 While support for awareness programs continue to grow, finance and operations departments are reported to be the biggest blockers. Awareness teams need to communicate the value and impact of their program in business terms and engage key departments from the beginning. Early participants often become collaborators; late joiners come to be critics.

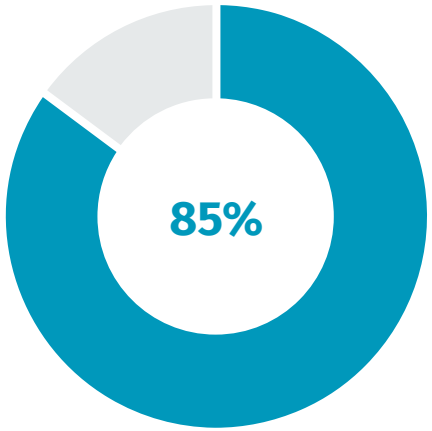
Executive Summary

Overall, the security awareness field is still very immature. The clear majority of security awareness professionals report their program activity as being only a portion of their job responsibilities. Many report they either have no budget or don't know what their budget is, and most lack the skills or background to effectively communicate to and engage with their workforce. However, there are several more encouraging indications that security awareness programs are gaining ground within their organizations.

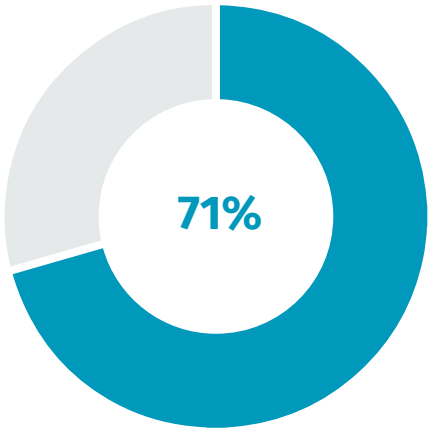
A few key figures that highlight this change include:



Awareness professionals report they have the leadership support they need to effectively run and maintain their awareness programs.



Awareness professionals report their work has a positive impact on the security of their organization.



Organizations identify themselves in the Behavior stage or greater in the Security Awareness Maturity Model©.

About This Report
Overview

The SANS Security Awareness Report was developed to enable security awareness professionals to make data-driven decisions on how to improve their security awareness program and to allow them to benchmark their programs against others. In short, to more definitively answer the question "What makes great security awareness programs successful?"

To accomplish this, The SANS Institute conducts a global survey of security awareness professionals every year. This year, the survey received responses from 1,718 qualified security awareness professionals; spanning 65 countries from around the world; this represents nearly double the responses as the previous year. This report is based on the results of that survey and comparisons with those done in prior years.

An exciting development in this year's report is that the data set is now large enough that it can be used to begin answering some of the more challenging questions relating to the continued successful development of the security awareness industry. We can identify and visualize correlating factors which help or harm programs and begin to see the effect of multiple variables on program development, maturity, and impact, and can do so across different industries.

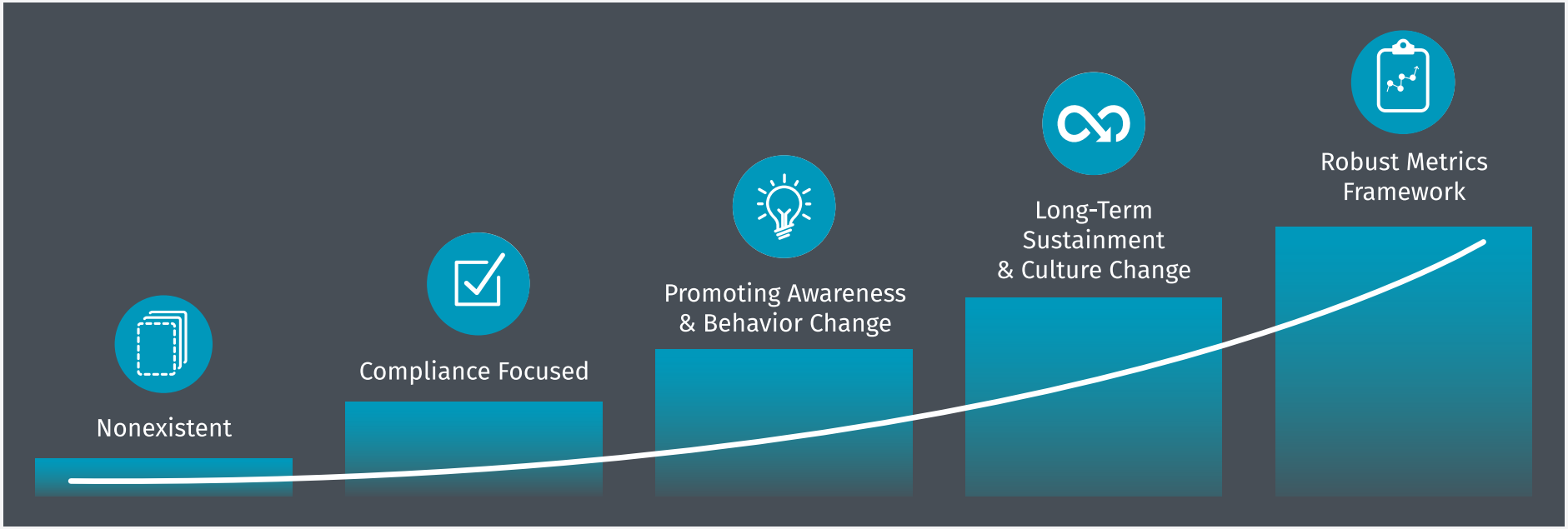
We have significantly increased these correlations, and have attempted to do so in a way that serves to provide awareness professionals visibility into the ingredients of more impactful, mature, and measurable programs. Additionally, you will see that in many cases the conclusions are rarely black or white and the story of a program's success or failure isn't told simply by the data. There are often times when programs follow different paths to success. As a result, throughout the report, we provide that data in an effort to help you draw your own conclusions, as well as to aid your understanding of our analysis and conclusions. As always, SANS welcomes your questions, comments, and suggestions. If you do have questions or feedback on this report or suggestions for next year, please let us know by emailing us at SecurityAwareness@sans.org.

As always, we feel it's very important to recognize the hard work that makes this report happen every year. Ultimately, this report is created by the community and for the community. The efforts of members within the security awareness community, as well as partners at Kogod Cyber Security Governance Center at American University's Kogod School of Business, and team members at SANS Institute who've played a key role in the survey's development and data analysis, are deeply appreciated. Profiles for each team member can be found at the end of this report.

Security Awareness Maturity Model

Security Awareness Maturity Model©
Measuring Success

Maturity Model



Measuring Success

The Security Awareness Maturity Model© is the key measure of program impact and success as established by the level of measurable human risk that can be mitigated by changing end-user behavior. Established in 2011 through a coordinated effort of over 200 awareness officers, the Maturity Model© enables organizations to identify and benchmark the current maturity level of their security awareness program and determine a path to improvement. The most successful, most mature, security awareness programs not only change behavior and culture but can also measure and demonstrate their worth via a metrics framework.

Security Awareness Maturity Model©
Based On 5 Stages

1. Nonexistent:

Program does not exist. Employees have little or no idea that they are a cyber target and that their actions have a direct impact on the security of the organization. They do not know or understand organization policies and easily fall victim to attacks.

2. Compliance-Focused:

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

3. Promoting Awareness & Behavior Change:

Program identifies the training topics that have the greatest impact in supporting the organization's mission and focuses on those key topics. It goes beyond annual training and often includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work and home. As a result, people understand and follow organization policies and actively recognize, prevent, and report incidents. Program success expands to include a reduction in risk related behavior and increased knowledge of policies.

4. Long-Term Sustainment & Culture Change:

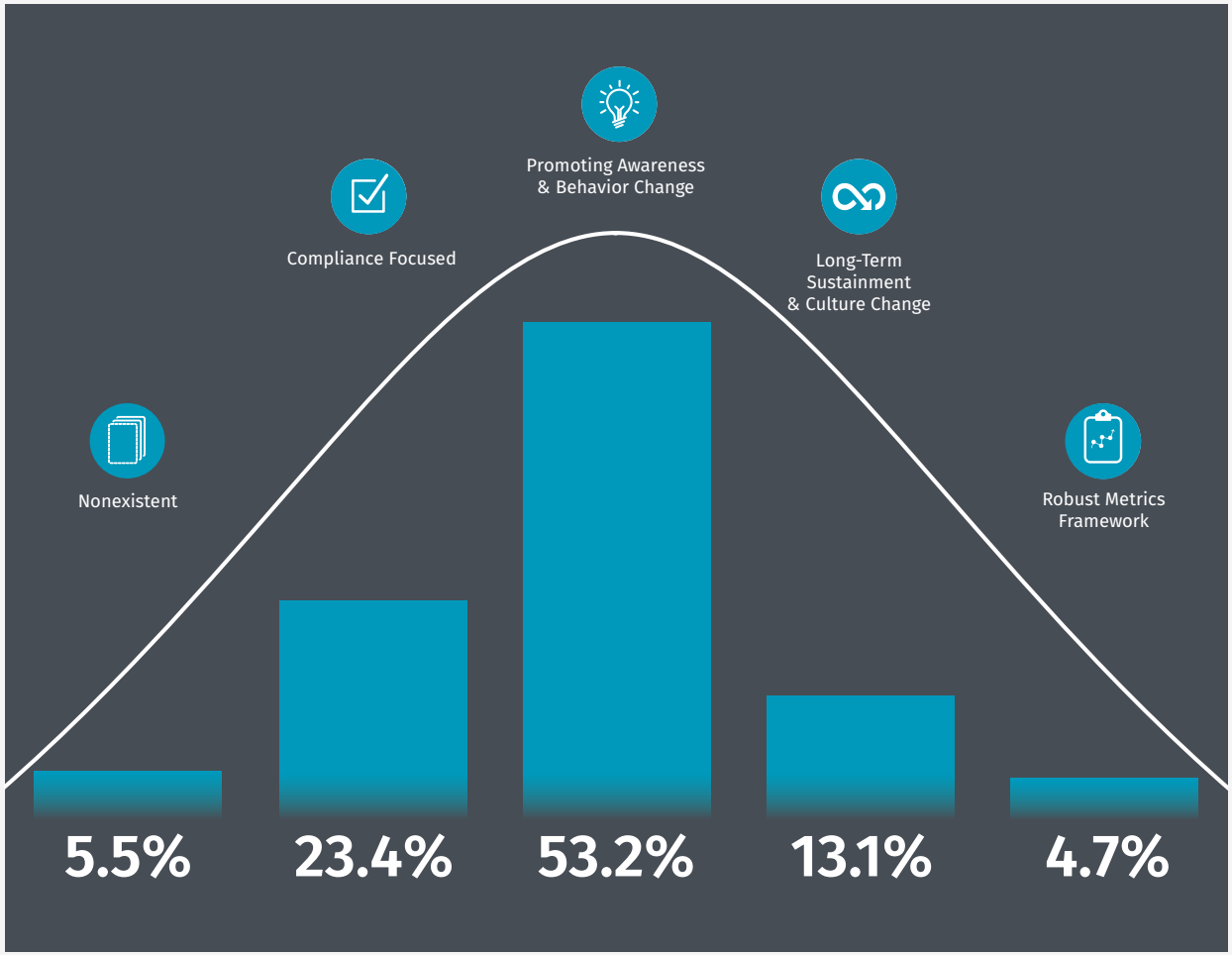
Program has the processes, resources, and leadership support in place for a long-term life cycle, including at a minimum an annual review and update of the program. As a result, the program and the core principals of good cyber security behavior and learning are an established part of the organization's culture. Program success extends to include widespread, cultural acceptance of good cyber-behavior (and rejection of poor behaviors) as well as general understanding and acceptance of the security awareness program and its value.

5. Metrics Framework:

Program is robust enough to provide metrics, such as progress and behavioral impact. As a result, the program is continuously improving and able to demonstrate return on investment. While noting that a metrics framework is listed as the last stage of the model, metrics are an important part of every stage. This stage further reinforces that to truly have a mature program, you must not only sustain a change in behavior and culture but have the metrics to demonstrate it. Success further expands to include metrics that adapt to the security awareness topics at hand which show not only participation, compliance, and behavior improvement, but also indicate changes in comprehension and cyber security competence across the organization.

Security Awareness Maturity Model©
Benchmarking Your Program's Maturity Level

Maturity Model

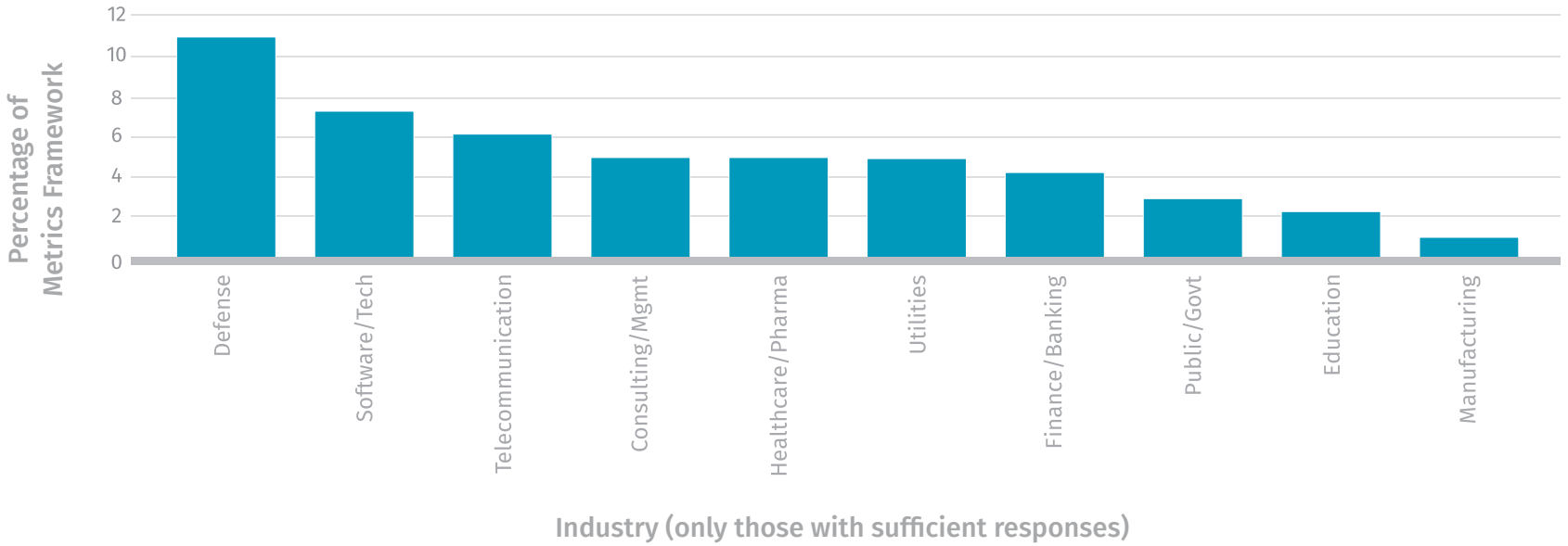


Benchmarking Your Program

The majority of respondents (**53%**) reported that their programs fall squarely in the middle of the Security Awareness Maturity Model© in the "Promoting Awareness & Behavior Change" category and have them using their awareness program to focus on their organization's highest risk issues and reinforcing training throughout the year. In comparison to last year's survey, it also appears that many organizations are making progress along the path to a more fully mature security awareness program.

Security Awareness Maturity Model©
Benchmarking Maturity By Industry

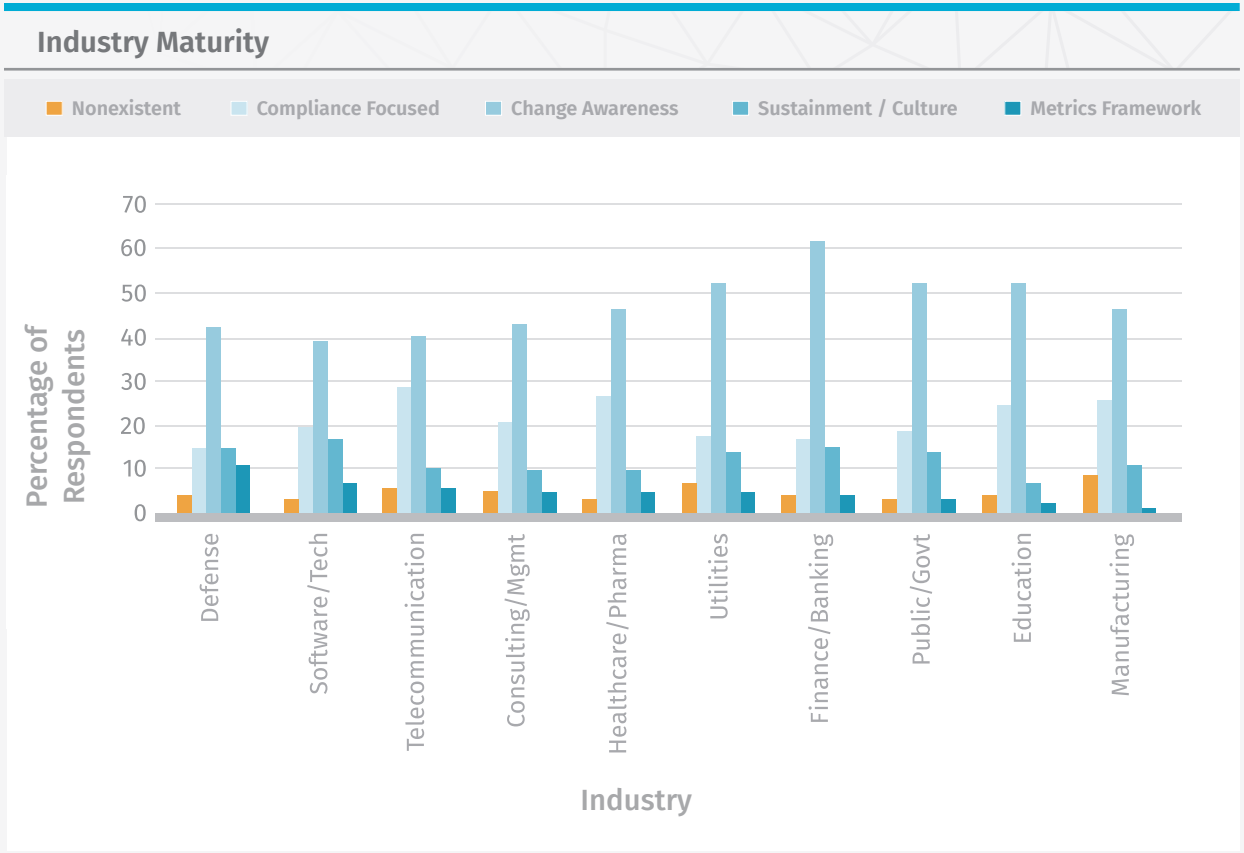
Metrics Framework



Benchmarking Your Program

Organizations within the same industry often face the same advantages and challenges to their awareness programs. While we have over twenty different industries represented in the survey, we've only utilized the data from ten industries, as this set of data is statistically significant. Above we list the maturity of programs within those industries. First, we examined each industry by analyzing what percentage of them achieved the most mature stage of the Maturity Model©, the Metrics Framework stage. Our discovery shows that the defense industry is the most mature, reporting over 10% as the Metrics Framework stage, while the manufacturing industry is the least mature with less than 2% achieving that stage.

Security Awareness Maturity Model©
Benchmarking Maturity By Industry



If we examine these same industries by percentage in all program maturity stages, the data is more complex. While the defense industry is still the most mature overall and the manufacturing industry is still one of the least, the industries in between show a weaker identifiable trend.

Digesting the Data

Questions to Ask

Determine where you fit on the Security Awareness Maturity Model©.
- How mature is your program?
- Does your program align with your industry?

Determine where you want your program to be.
- Which stage do you want your program to reach in the next 1-3 years?
- What changes will you need to make to achieve that level?

Findings
Program Supporters and Blockers

Findings
Program Supporters and Blockers

The majority of respondents reported far more supporters than blockers. Large breaches, such as the Equifax customer data breach, and new regulations, such as the EU's General Data Protection Regulation (GDPR), are likely contributing to a sense of urgency around cyber security and are a key factor to both support and change. The strongest reported support comes from Information Security/Technology departments. Support from these departments is very important as this is where almost 70% of security awareness programs reside.

In previous years, the SANS Security Awareness report has found that Communications departments are the largest blockers to building or maturing a security awareness program. The data reported in this year's report shows that this has also changed and it appears security awareness professionals are getting better at building bridges with their respective communications teams.

This year's most reported blockers? Finance and Operations departments. Most programs have both a significant budget and have an operational impact during program roll out to organizations. While Finance and Operations groups tend to take a measured approach to both budget and operational change, this becomes even more complex at larger and more global organizations. How can you overcome these blockers?

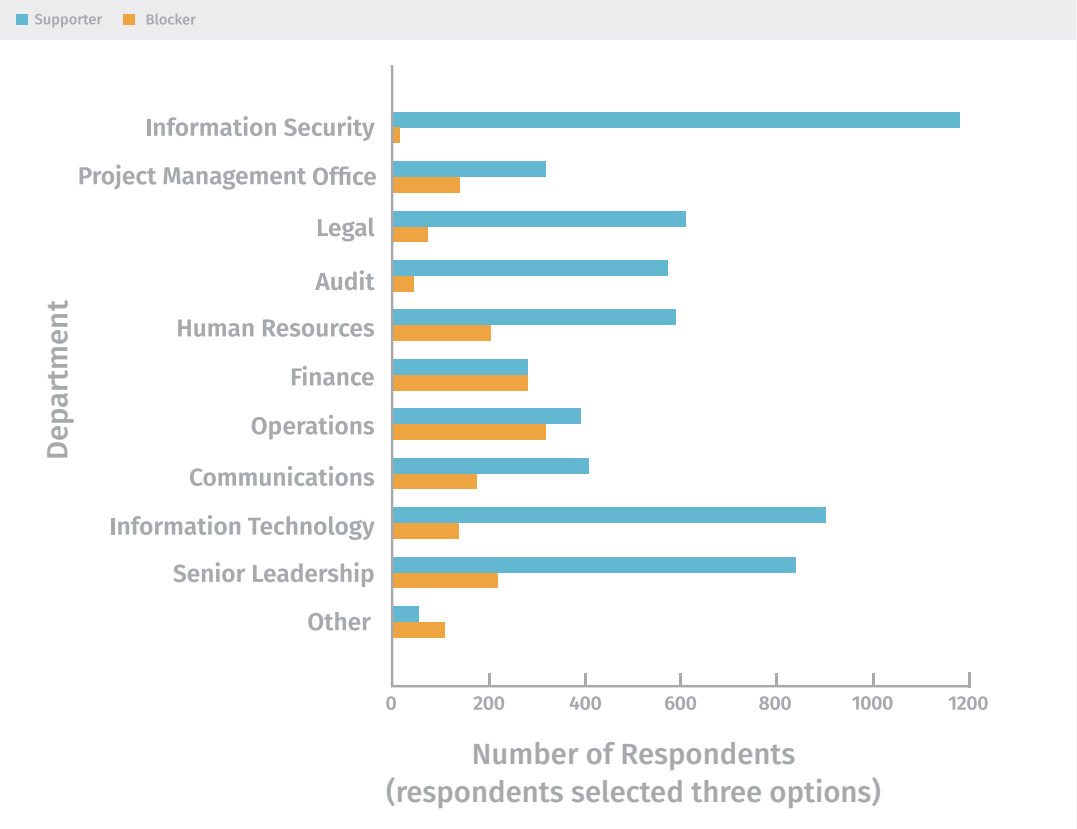
Action Items

Finance: All Security Awareness programs have a cost. Security Awareness professionals need to do a better job of justifying those costs by not only demonstrating the impact but also the value of that impact on the overall organization and its mission. This can include analyzing costs due to past breaches, costs of compliance failure, and cost requirements due to any partner or customer security requirements.

Operations: Security Awareness programs have a significant operational impact. These range from lost-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 the planning process and consider adding them to your Advisory Board.

Findings
Program Supporters and Blockers

Blockers and Supporters for Building a Security Awareness Program by Department



Mature Your Program

Security awareness programs that focus on behavior and cultural change, and have measurable results tend to more effectively pair training needs with trainees. This can reduce time spent on training as well as increase training effectiveness. Metrics can help provide a clearer picture as to both the cost and the benefit of training programs.

Leadership Support

Leadership Support

The allocation of resources, enforceability of programs, identification of key program goals and overall maturing awareness programs all depend on support from senior leadership. Unsurprisingly, the data shows a clear correlation between leadership support and program maturity.

Still having leadership support challenges?

A Key Leader is a Blocker: If you have a senior leader who is a blocker, remember the goal is not to convert every leader into a champion. Some leaders will remain pragmatic. The goal is to move them from a blocking position to a more neutral one, allowing the program to proceed.

Use Your Champions: If you are having challenges getting the support of certain leaders, talk to a senior champion and see if they have any suggestions on how to communicate the value of security awareness to executives. The ability to deliver resource needs and value statements at a board level often needs to be honed; quite often it's not what your awareness program is doing that is the issue, it's how you are communicating it.

We had a Breach: Remember the common cyber security expression "Never let a good data breach go to waste." **Most security incidents and data breaches have some human component.** If you have an internal incident, a public mishap, or a known near-miss that was human-related, use it to help drive the justification for your program. These events often draw your leadership's attention. You can use them as a teachable moment to help express how baseline cyber security awareness training programs can help mitigate the problems and are necessary to fill the gaps that security technology can't. Another option: document all human-related incidents in the past six months or compare similar incidents that have happened to other organizations in your industry.

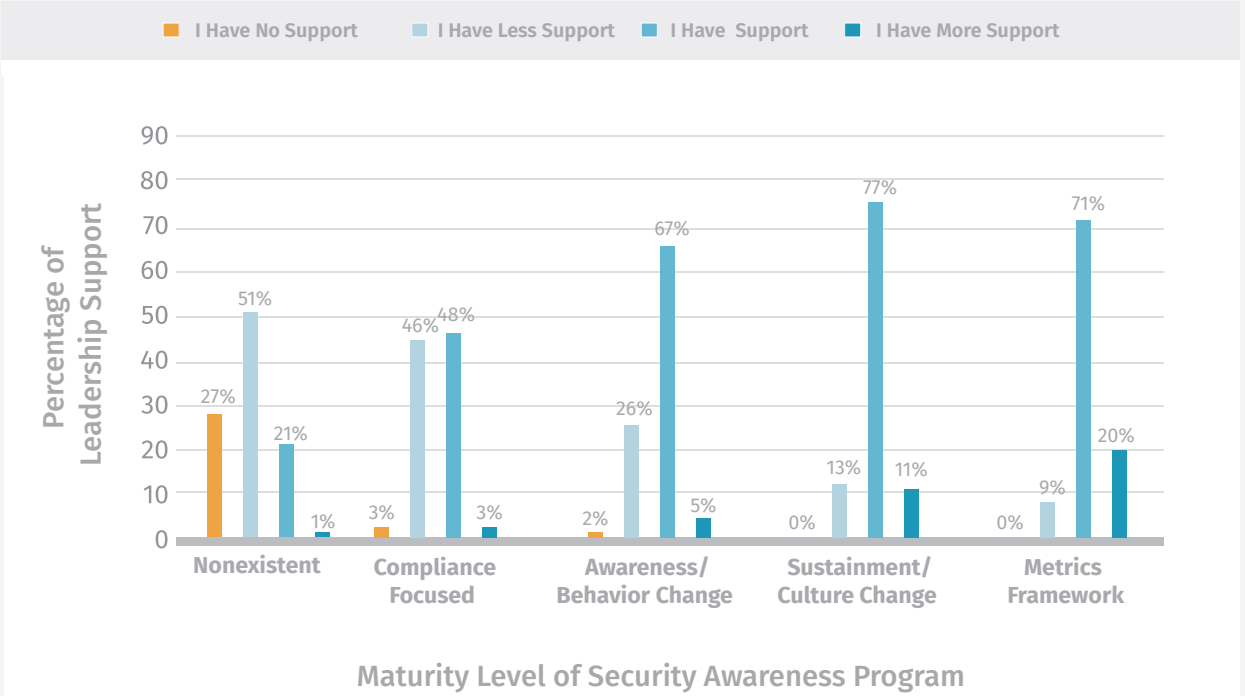
Make Time for Metrics: Dedicate a certain amount of time each month for collecting and communicating with leadership about the impact/value of your security awareness program. A good starting point is 4 hours a month. That does not mean you spend 4 hours every month talking to leadership. It means you spend 4 hours every month collecting the data and success stories that demonstrate the impact your program is having, building an executive report or presentation that communicates in business terms, that your leaders value, what your program is doing.

Leadership Support
Impact on Maturity

Maturity Model

When communicating with leadership, use the Security Awareness Maturity Model© to help demonstrate where your program is, where you want to take it, and the path to achieving that goal. Leaders understand maturity models, leverage it to demonstrate you have a goal and a plan to achieve that goal. Connect the stages of maturity with the terms and values of your organization's leadership and show how more mature programs more effectively and efficiently reduce the risks they worry about.

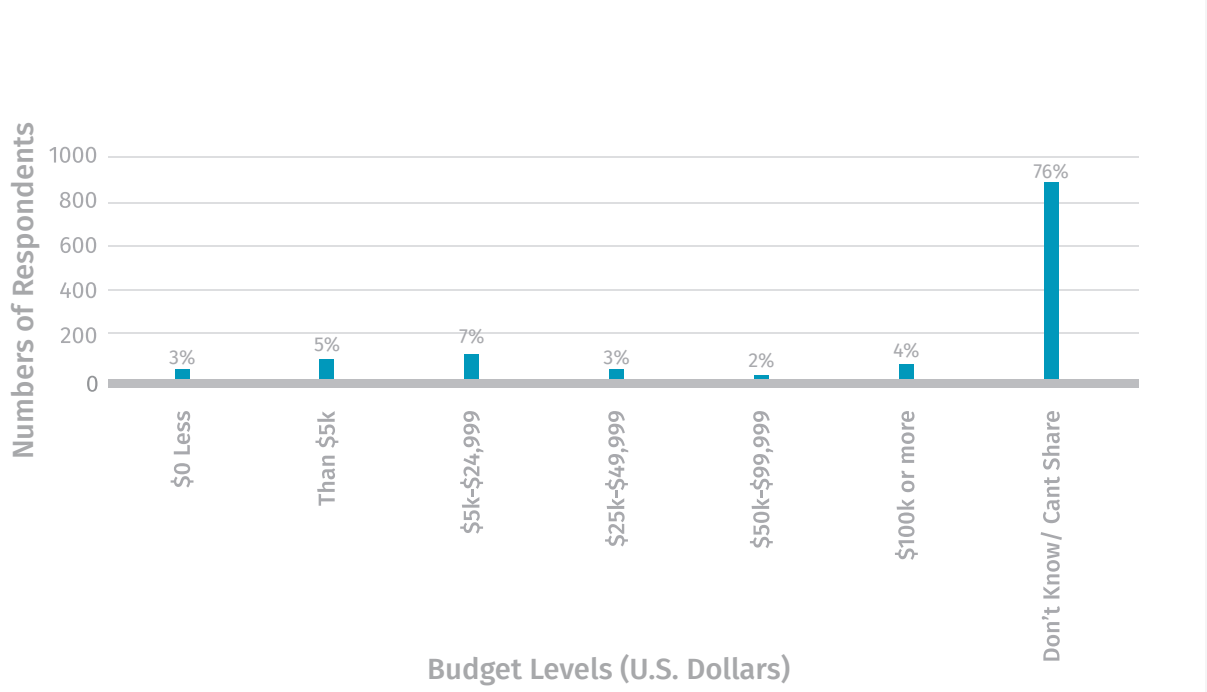
Impact on Program Maturity



The graph demonstrates the direct correlation between leadership support and the maturity of awareness programs.

Budget

Respondents per Budget Level



Budget analysis for the 2018 report was challenging because the majority of respondents either did not know or could not share their 2018 security awareness training budget. Unlike leadership support, the data did not show a strong correlation between budget and maturity of an awareness program. These findings are similar to the information gathered last year. The lack of understanding around budget continues to be concerning and contributes to the immaturity of many security awareness programs and organizations.

Action Item

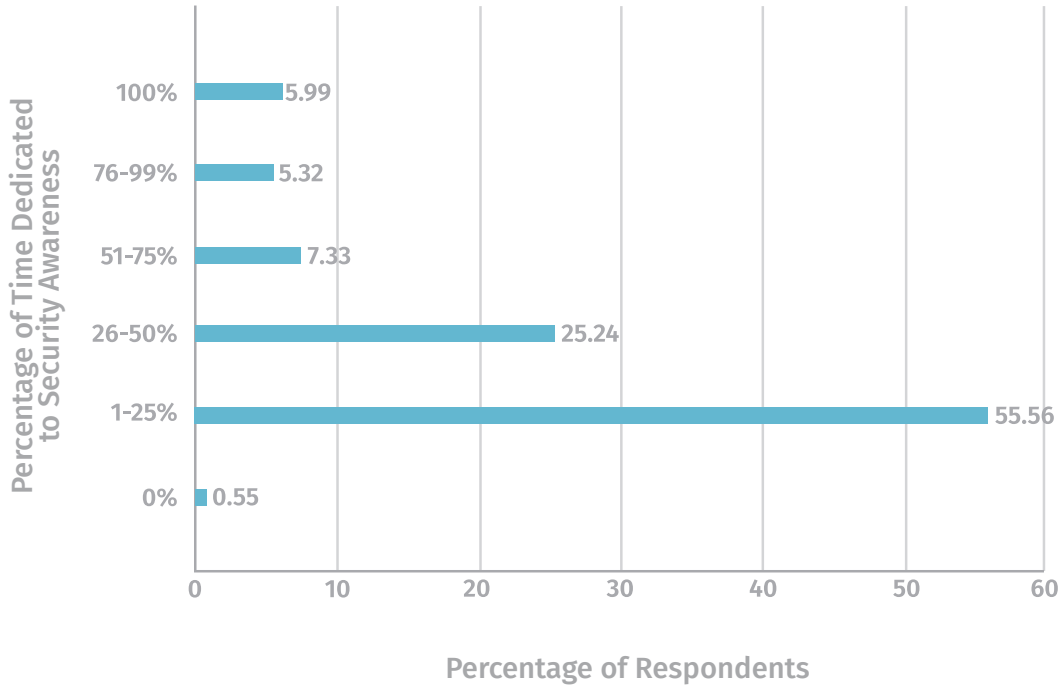
Ask for Budget

Not sure what your budget is? Ask. However, as you will see later in the report, time, not budget is typically the most critical resource. If you can only have one or the other, go for time.

Time is The Most Valuable Resource

Time is The Most Valuable Resource
Overview

Time Dedicated to Security Awareness



Continuing the trend from 2017, respondents' data clearly indicates that the lack of staff-time is the number one challenge faced by security awareness organizations. Over 80% of respondents reported spending less than half of their time dedicated to awareness programs and most organizations categorize security awareness a part-time job. This lags significantly behind staffing levels of more conventional security roles such as those in incident response, security operations centers and members of endpoint security teams which are typically well staffed with full-time employees. Given the overall increase in security incidents involving human error, the trend toward understaffed security awareness programs is particularly concerning.

A better metric is the combined number of full-time employees (FTEs) dedicated to a security awareness program which can be calculated by adding up the time spent by individual contributors on the management and operation of their security awareness programs. **Programs with higher combined FTE counts showed a strong correlation toward maturity.** Remember, awareness is not a technical solution, it's a human solution, it requires talking to, engaging and collaborating with others, and getting the message to a broad audience; all of this takes staff time. How many FTE's you should have depends on what level of maturity you want to achieve. This table shows the average number of combined FTE staff reported by program maturity level.

Time is The Most Valuable Resource
Program Staffing

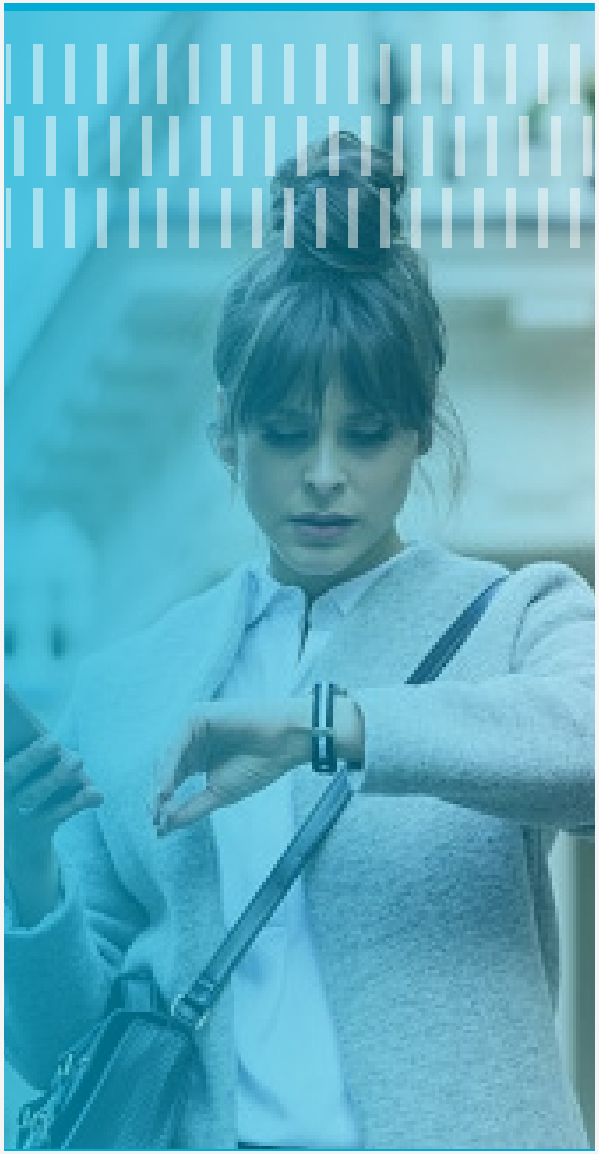
Average Number of FTE's Per Maturity Level

Maturity Stage	Average FTE
Nonexistent	0.81
Compliance Focused	1.60
Awareness/Behavior Change	1.93
Sustainment/Culture Change	2.70
Metrics Framework	3.67

The data also shows that the number of combined FTE staff required once a program reaches more than 5,000 trainees tends to level off. Many common activities in security awareness program operation, such as loading people into a Learning Management System, creating materials such as newsletters or infographics, or launching a phishing assessment operate at a program level, scale well and require the same effort regardless of your trainee base.

While this is a general guideline, it should be noted that some program complexities require more staffing than others. If your organization has numerous remote or global offices, complex translations or regulation requirements, and/or unique target training groups, it will probably require more staff. In addition, data reported for programs at the highest two stages of the maturity model show a dramatic increase in required FTE staffing. This is likely due to the more advanced activities which can be time intensive, such as building an Ambassador Program.

Struggling with Time?
Action Items



Staffing

Identify the maturity level you want to achieve FIRST, then identify how you will get the people to achieve that level. Can't get the support you need? Show your boss this report. Remember, achieving a more mature program without staffing is a very difficult task.

Partnerships

Are there other groups within your organization who can help build your program? Often, other departments such as communications, project management or marketing can provide not only the expertise you need but also the manpower.

Buy Time

If staffing up isn't an option, but you have the budget, use it to buy yourself time. Don't create the monthly newsletter yourself, contract someone to do it for you or license materials from a vendor. Instead of creating a survey, hire a contractor that specializes in social science. The more you can delegate, the more time you have to create partnerships, work with others and ultimately make a difference.

Community

Reach out and leverage the security awareness community which has resources, tools, and advice which can also be used within your program.

Program Initiatives

In this year's survey, a new question was presented to respondents. They were asked to identify what security awareness initiatives they employed and how impactful they were. Of the programs reporting in the two most mature stages of the Maturity Model these were the top initiatives used:

- Phishing
- Targeted Leadership Training / Briefings
- Computer Based Training (CBT)
- Newsletters / Posters
- Events / Speakers

Looking to Broaden Your Awareness Program?

Action Items

CBT / Phishing

This is where many organizations start their awareness program. More mature programs typically expand into and require more manual activities, such as ambassador programs, lunch-n-learns or personalized leadership briefings. This helps explain why achieving the last two stages of the maturity model require such a dramatic increase in FTE support.

Prioritize Risks

Begin your awareness program with a human risk assessment, then identify and prioritize your top human risks. This enables you to make the most of your initiatives, which will most likely be limited.

Free Resources

Consider publicly available resources to augment your program; such as SANS Security Awareness free OUCH! Newsletter, blog articles, posters, etc. which can be found and utilized to flush out programs.

Find a Community

Most awareness program officers have developed resources and techniques to expand or enhance their programs; many share and discuss these on community forums and at security awareness summits and meetings.

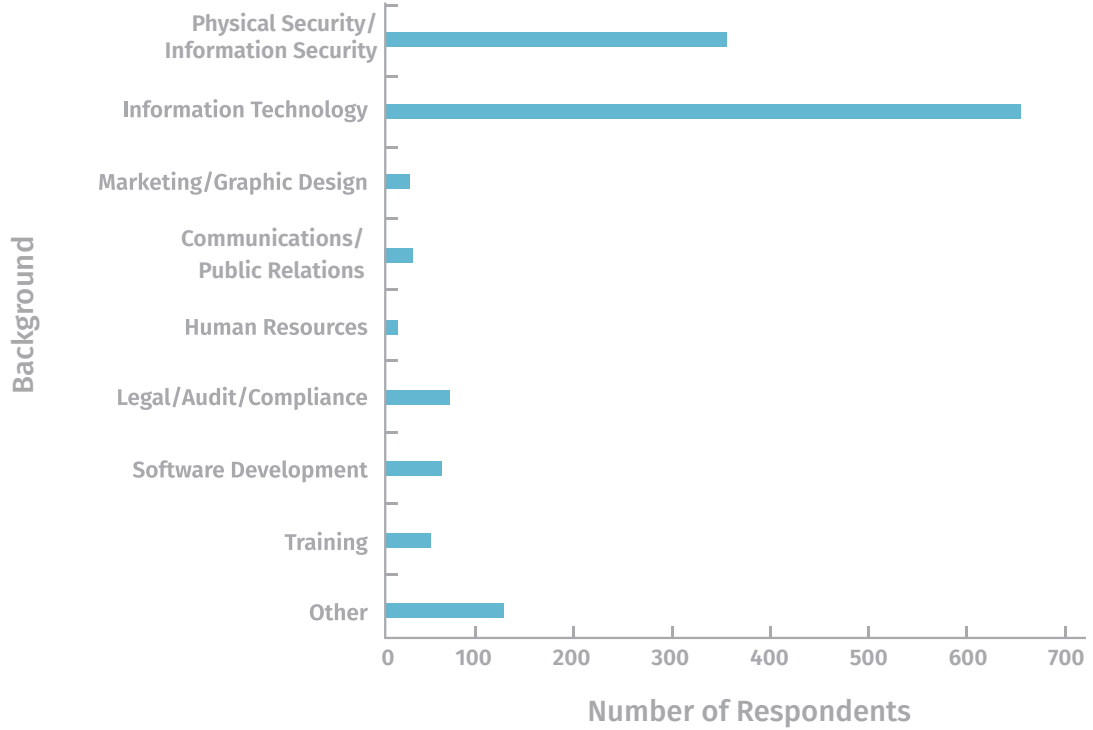
Demographics of Security Awareness Professionals

Demographics of Security Awareness Professionals
Background

Consistent with last year's report findings, the 2018 report shows that a clear majority of awareness professionals come from a technical background with less than 20% of individuals coming from non-technical fields such communications, marketing, legal or human resources.

While technically skilled professionals have some advantages, in that they have a solid understanding of technology and human-related risks, this can also create a challenge. These same individuals often lack the skills to effectively communicate those risks and engage employees in a way that changes behavior.

Which background describes your role before you became involved in security awareness?



In addition, staff most familiar with the technology often need to overcome what is known as, 'The Curse of Knowledge', which is a form of cognitive bias. 'The Curse of Knowledge' means that the more expertise an individual has on a given subject, the more difficult it is for him or her to teach or communicate about it, as they tend to project their intrinsic knowledge on the subject onto their audience. Security professionals perceive security as simple because technology is a part of their daily lives. These same people then assume security must be simple for everyone else in their organization and they often build their awareness programs based on these misconceptions. As a result, what they communicate can be mismatched with what their audience needs. The reported data shows a direct correlation between program maturity and staff with key soft skills in areas such as communications and marketing.

Demographics of Security Awareness Professionals
Background

Maturity Stage	Percentage of All Respondents with Soft Skills*
Nonexistent	1.19%
Compliance Focused	1.68%
Awareness/Behavior Change	3.70%
Sustainment/Culture Change	5.03%
Metrics Framework	13.89%

Working to Communicate Your Program More Effectively

Action Items

Soft Skills

Be sure you have someone on your awareness team that has the soft skills required for effective communication and engagement. This can include training someone on your awareness team to have soft skills, partnering with your communications or marketing department, or even have one of their members embedded into your security awareness team.

Biases

Often knowing you have a bias is enough to effectively counter it; if your team is technically skilled and/or from an IT or InfoSec background, be aware of these biases and work to remember target audiences. Test your communications on non-technical staff before rolling them out broadly and assess effectiveness and engagement.

Communications Plan

Most mature programs contain a specific framework which manages not only technical content but also the messaging and engagement of learners and leaders at all levels. Don't stop at "what" you communicate, include "how" you do it as well.

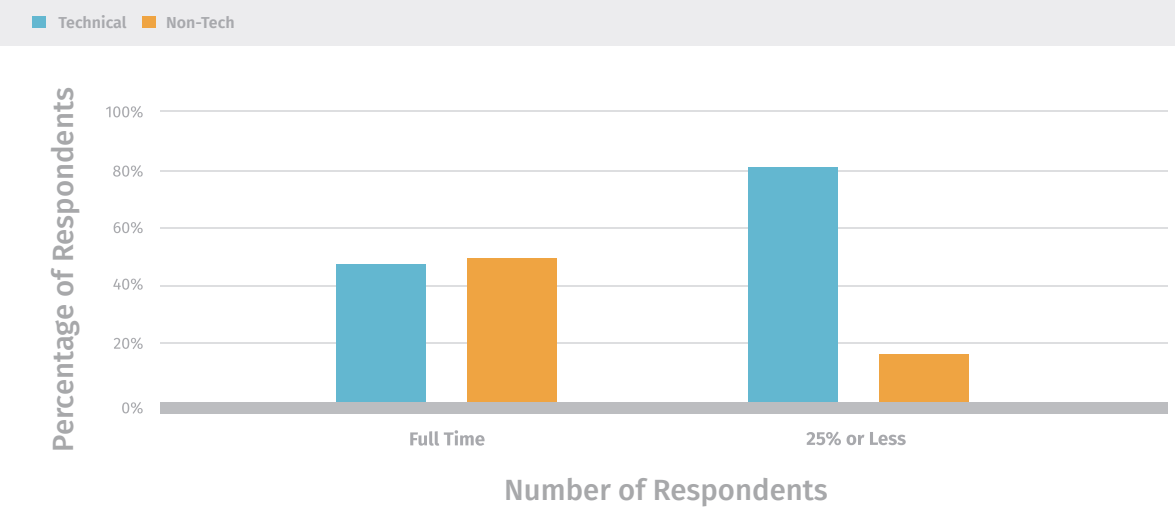
*Soft skills are defined as backgrounds in communications, public relations, marketing, or graphic design.

Time Dedicated to Programs Related to Staff Background

A security awareness professional's background was shown to have a strong correlation to the percentage of their time dedicated to their awareness programs. The more technical your background, the more likely you are dedicated part-time to security awareness; less technical staff, those with a marketing or communications background spent, on average, almost twice the time working on their programs. One hypothesis explaining this: when newer programs are formed, the staff responsible for running them are randomly selected, typically from the IT or the Security Team. As such, security awareness is simply added to their myriad of other responsibilities.

Using time from classic technology or technical-security teams results in many programs being staffed by technical individuals who can dedicate only minimal amounts of their time. Awareness programs are "just another thing" they have to do in addition to a myriad of security efforts. Instead, if an organization hires staff specifically dedicated to awareness, it's far more likely that person will be selected, at least in part, for their essential soft skills, such as communications.

Percentage of Time & Tech/Non-Tech Background

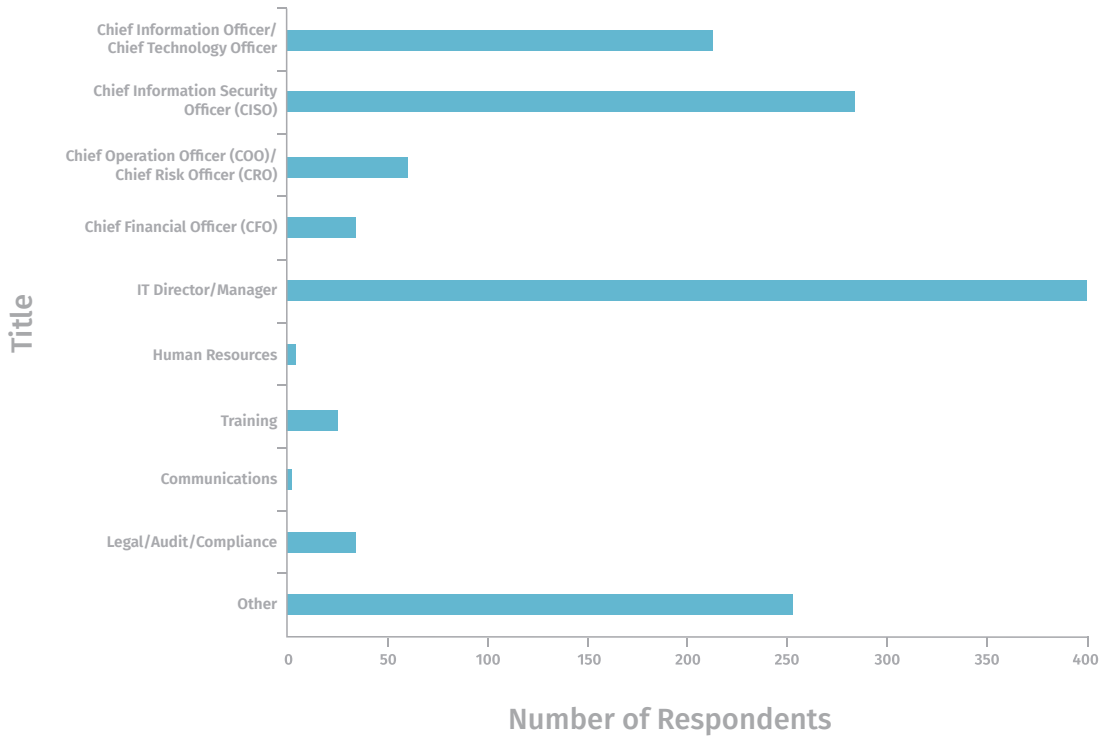


Based on the reported data, overall programs show 27% of security awareness professionals are women. In contrast, for programs with dedicated full-time to security awareness, 58% were female. **This does not mean women are better at security awareness; it most likely reflects that women represent a high percentage of many soft-skilled fields, such as communications and marketing, and, as a result, are more likely to be hired for a dedicated awareness position when those soft-skills are a hiring priority.** This also explains why women have a stronger presence in security awareness than many other cyber security fields. As a side note, among women who took the survey, more had technical skills background than non-technical.

Reporting Structure

Most security awareness professionals report to someone on the more technical side of their organization, the most popular being CIO, CISO or IT Director. The data did not identify any specific reporting structure to be the most successful. Security awareness program staff were found to report to a wide variety of individuals.

What title best describes the person to whom you report?



Need Help Building a Program with Wide Support?

Action Items

Partnering

The data shows it's not as important who security awareness professionals report to, but that who they report to supports the growth and maturity of the awareness program. Also, no one department can provide all of the resources you need for a successful program. Regardless of whom awareness professionals report to, they will have to partner with other departments of the organization.

Engage your peers

Consider attending a regional or national security awareness event or summit. These events bring together the community of security awareness professionals and provide a bounty of partnerships and program information.

Security Awareness Position Titles

In an effort to identify trends relating job titles to security awareness program staff, the 2018 survey asked respondents their job title. To get unbiased input, the data was gathered via a free-form text entry field thus allowing respondents to submit whatever title applied to them. **The findings were that less than 5% contained the word "awareness" and the largest percentage of titles contained "InfoSec," or "IT."** In many cases, this is connected to the part-time nature of many awareness workers and implies that the field of security awareness is not mature enough in most cases to have clearly defined and named roles.

Worried About Your Title?

Don't be!

Because of the immature nature of the cyber security awareness field, very little consistency of professional job titles was found. Be less concerned about what your title is and more concerned that you have the time you need dedicated to managing your security awareness program. In addition, make sure that whoever you report to is very clear on your security awareness responsibilities.

Position Title Identification by Respondents

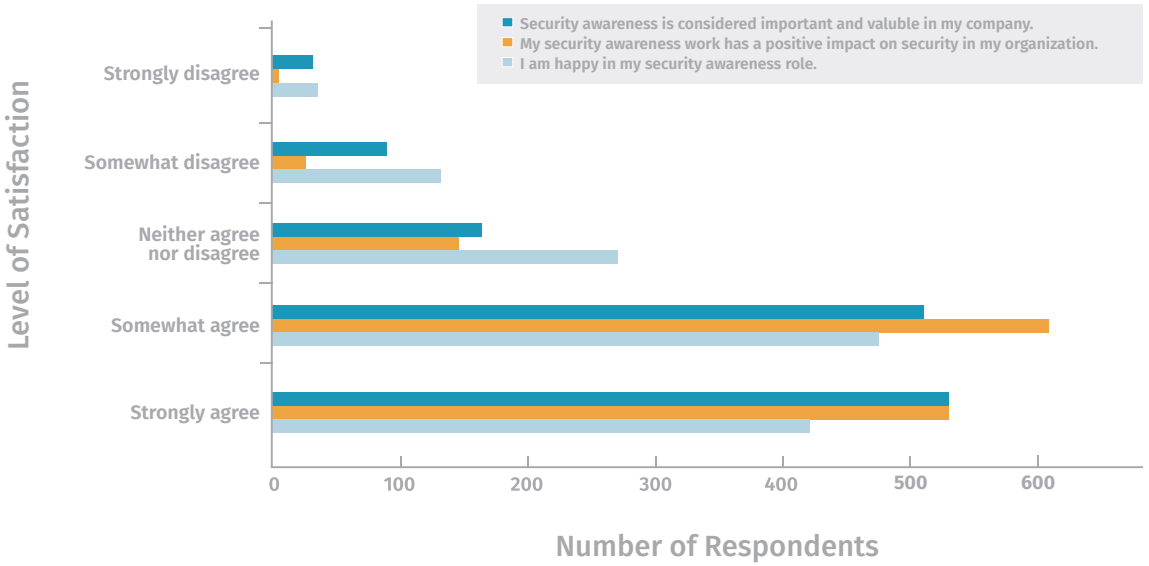
Title Categories	Number of Respondents
InfoSec - Staff	265
InfoSec - Manager/Directory	264
IT - Manager/Director	178
Other	81
Engineer	79
Consultant	67
IT - Staff	66
Chief Information Security Officer (CISO)	50
Legal/Audit/Compliance	43
Awareness & Training - Manager/Director	42
Chief Information Officer (CIO)/ Chief Technology Officer (CTO)	24
Risk - Manger/Director	21
Awareness & Training - Staff	21

Title Categories	Number of Respondents
Operations/Physical Operations	16
Communications	14
Training	13
Customer Support/Service	12
Risk - Staff	11
Chief Executive Officer (CEO)	8
Faculty	7
Chief Security Officer (CSO)	6
President	5
Owner	3
Human Resources	3
Chief Financial Officer (CFO)	1
Chief Operating Officer (COO)/ Chief Risk Officer	1

Security Awareness Job Satisfaction

This year, questions were added to the survey to establish the job satisfaction and impact of security awareness professionals. Overall, role satisfaction appears positive with the majority of respondents reporting somewhat or strong agreement as to their value, impact, and happiness. There is a very strong correlation between an organization's program maturity and strong agreement with the questions related to job satisfaction. **The most mature programs are run by organizations in which their staff feel valuable and their work is having an impact.**

Security Awareness Job Satisfaction



Summary of Key Action Items

Summary of Key Action Items

Ultimately, security awareness is a challenging industry – but well worth the effort. There are key steps you can take to help build your organization's program.

FTEs

You need at least 1.9 FTE's to change behavior at an organizational level. To achieve a truly mature program, including a strong metrics framework, you will need at least 3.7 FTEs. Your FTE numbers may vary depending on your size, organizational structure, and requirements. However, we recommend you use this as a starting point for organizations with 5,000 or more people.

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.

Buy Time

If you have the 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 that specializes in social science. The more you can delegate the more time you have to make a difference.

Soft Skills

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.

Time for Metrics

Dedicate a certain amount of time each month for collecting and communicating to leadership about the impact/value of your security awareness program. A good starting point is 4 hours a month. That does not mean you spend 4 hours every month talking to leadership. It means you spend 4 hours every month collecting the data and success stories that demonstrate the impact your program is having, then make sure you communicate that every month in business terms that leaders value. By leaders we mean not only your CISO but other departments, such as Finance and Operations.

Champions

Find yourself 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 understand and act on.

A Big Thanks

We would like to take a moment and thank our contributors. 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:

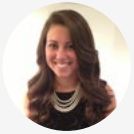
The Kogod Cybersecurity Governance Center (KCGC)

The Kogod Cybersecurity Governance Center (KCGC) is a research initiative of American University's Kogod School of Business (KSB) focused on the governance and management of cyber security. Through multidisciplinary research and collaboration, KCGC aims to promote responsible cyber security governance by providing today's leaders with actionable and well-supported guidance that will help them overcome challenges and maximize opportunities arising from the cyber security issues that are essential to their core stakeholder responsibilities. For further information about the Center, visit www.american.edu/kogod/research/cybergov.

KOGOD SCHOOL of BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC

Rachel Sawyer

Rachel Sawyer is the Operations Coordinator at the Kogod Cybersecurity Governance Center at American University's Kogod School of Business. She manages Center activities, including research, publications, and events and also oversees student research assistants. She has a background in teaching and academic strategic planning both in the US and abroad, as the recipient of a Fulbright Fellowship to Kazakhstan. She holds a BA in Linguistics from Georgetown University and is currently a first-year MA student in the International Training and Education Program at American University's College of Arts and Sciences.



Zoë Bludevich

Zoë Bludevich is a second-year MBA student at the Kogod School of Business. She received her BA in Government from St. Lawrence University. Prior to attending Kogod, she was a Litigation Paralegal at Ropes & Gray, LLP where she worked with Global Fortune 500 clients on white collar crime, government enforcement, and foreign corrupt practice cases. As a student at Kogod, she co-authored a case study exploring the organizational behavior and human resources complexities of integrating a robust cyber management program within the Washington, DC area power supplier, PEPCO.

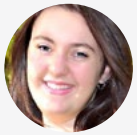
Mike Giampiccolo

Mike Giampiccolo is currently an undergraduate student in the Kogod School of Business, where he is pursuing a BS in Accounting with a minor in Information Technology. His primary research interests in cyber security include the implications of cyber breaches on businesses and their economic growth and the rising need for legislation and policy surrounding cyber laws and regulations. Additionally, he is interested in how the government will be tackling the issue of cyber-crime over the next few years.

A Big Thanks

Karen Amethyst Mascariñas

Karen Amethyst Mascariñas is a current graduate student in the Ethics, Peace, and Global Affairs Program at American University's School of International Service and a research assistant for the Kogod Cybersecurity Governance Center. Her research interests focus primarily on the wide-ranging ethical implications of emerging technologies on global society. She is particularly interested in considering how cyber, automation, and artificial intelligence will impact current and future conceptions of human rights narratives.



Elizabeth Victoria

Elizabeth Victoria is a member of the junior class studying International Studies while focusing on national security, the Middle Eastern region, and the Arabic language. In 2017, Elizabeth interned with the Eurasia Center, which resulted in a website publication discussing recent terrorism trends in Europe. After graduation, Elizabeth hopes to remain in Washington and work as a counter-terrorism/intelligence analyst for the government.

Christine Miyashiro

Christine Miyashiro is a senior from Sacramento, CA receiving a dual degree in Political Science and Musical Theater at American University. Christine participated in the Atlantic Council's 2018 Cyber 9/12 Student Challenge in Washington, D.C. where she made the semifinals after developing national security policy recommendations tackling a simulated cyber catastrophe. In 2017, she conducted research on cyber security for a California State Assembly Member as an intern at the Asian Pacific Islander American Public Affairs Association. Christine previously enjoyed working as a Teaching Assistant and an Orientation Leader at AU.

Rebekah Lewis

Rebekah Lewis is a practitioner-scholar of cyber policy, law and governance. Her diverse and deep experience includes serving as the Director of the Kogod Cybersecurity Governance Center at American University's Kogod School of Business and as a practicing attorney, both in the private sector at Latham & Watkins and at the U.S. National Security Agency. Rebekah also has experience internationally with the International Telecommunication Union (ITU).

Report Authors

Lance Spitzner

Lance Spitzner has over 20 years of security experience in cyber threat research, system defense 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. In addition, Lance has published three security books, consulted in over 25 countries and helped over 350 organizations build programs to manage their human risk. Lance is a frequent presenter, serial tweeter (@lspitzner) and works on numerous community security projects. Before working in information security, Lance served as an armor officer in the Army's Rapid Deployment Force and earned his MBA from the University of Illinois. He works with SANS as a subject matter expert and senior instructor for security awareness.

Dan deBeaubien

Dan DeBeaubien is a 25-year veteran of Information Technology and former CTO of Michigan Technological University. He has held a variety of posts throughout his career including Sr. Systems Administrator, Sr. 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.

About SANS Security Awareness

SANS Institute is by far the most trusted and the largest source for information security training in the world. With over 25 years of experience, SANS information security courses are developed by industry leaders in numerous fields, including cyber security 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' cyber security risk. 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 20 languages and built by a global network of the world's most knowledgeable cyber security 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 security awareness program:

- Expert-authored training, tools, and content for easy compliance, better behavior change, and a more secure culture.
- The Advanced Cybersecurity Learning Platform (ACLP) ensures the right employees receive the right training at the right time. The ACLP automates a number of tasks, saving time and ensuring organizations follow a proven roadmap to success.
- Managed services support security awareness officers from program startup to measuring success.
- The world's largest and most engaged community of cyber security professionals, so you benefit from quick access to relevant and actionable information.

Whether seeking check-the-box easy compliance or industry-leading content, training, and services, organizations benefit from SANS Security Awareness' unwavering commitment to helping organizations effectively understand, manage, and measure their human cyber risks. To learn more, visit https://www.sans.org/security-awareness-training.