2017
SECURITY AWARENESS REPORT

It's Time to Communicate

SANS SECURITY AWARENESS

Table of Contents

Report Summary

Don't have a lot of time? Then this page is for you. Capitalize on the key findings from the 2017 Security Awareness report - use it to help you achieve success in your awareness program.

During our research for the SANS 2017 Security Awareness report, we uncovered two main drivers why awareness programs thrive or fail. In addition, we uncovered a surprising key finding.

1. Time is critical

In last year's report, we identified lack of resources as a key blocker. This year we narrowed that down more and discovered that time, not budget, is the critical resource for success. What does time specifically mean? We define it as the combined effort of people who contribute to an awareness program, measured as total number of full-time employees (FTEs). For example, if you have two people each working half time on your awareness program, combined their efforts are one FTE. Far too many organizations view awareness as a part-time job, crippling their awareness team's ability to effectively get things done. We found the **minimum number of FTEs required to change behavior at an organizational level was 1.4 FTEs**, while the most successful awareness programs had **at least 2.6 FTEs dedicated to awareness.**

2. Communication is the most important soft skill

Last year we learned that a lack of soft skills was prevalent in the development of awareness programs. This year, we've defined that as a **lack in communication skills.** This includes the ability to effectively communicate to and engage employees, as well as the ability to effectively communicate to and demonstrate value to leadership.

Surprise Finding!

Women are twice as likely as men to be dedicated full-time to security awareness.

Ultimately, we, the security community need to stop blaming employees as the security problem and start blaming ourselves. It's up to us to understand what the root causes are in failing to change human behavior and address those issues. The rest of this report is dedicated to doing just that. We dive deep into the first two points listed above and outline pivotal steps you can take to address them. Additionally, we give you the opportunity to benchmark your awareness program against others from research gathered from the community.

About This Report

Overview and Analysis

Before we begin, let's discuss a bit of background about the third annual SANS Security Awareness Report. The purpose of this report is to enable security awareness professionals to make data driven decisions on how to improve their security awareness program and benchmark their program against other organizations.

To accomplish this, we've conducted a global survey of security awareness professionals every year. Last December, 1,084 qualified people from 58 different countries responded to the survey, well over twice as many from the previous year. By qualified people we mean professionals who help build, manage or contribute to their organization's security awareness program.

This report is based on the results from that survey. If you have any questions or suggestions on this report, please contact us at **sth-community@sans.org**.

Contributors

We'd like to recognize several important people that contributed to the creation of this report. The content that comprises this report was developed by the community and for the community. Check out the full bio of each of these amazing folks at the end of this report. We'd like to especially recognize the team from the Kogod Cybersecurity Governance Center at American University's Kogod School of Business.

Sahil Bansal
Senior Manager
Information Security - Genpact

Jessica Fernandez
InfoSec Communications Consultant
Warner Bros. Entertainment Inc.

Mark J. Lucas
Lead System Administrator
California Institute of Technology

Joanna Lyn Grama
Director of Cybersecurity and IT GRC Programs
EDUCAUSE

Valerie M. Vogel
Senior Manager, Cybersecurity Program
EDUCAUSE

Ingolf Becker
University College London

Jonathan Homer
Infrastructure Protection Specialist
Information Security – Consultant

Zoë Bludevich
Research Assistant
The Kogod Cybersecurity Governance Center at American University's Kogod School of Business

Aria Chehreghani
Research Assistant
The Kogod Cybersecurity Governance Center at American University's Kogod School of Business

Michael Giampiccolo
Research Assistant
The Kogod Cybersecurity Governance Center at American University's Kogod School of Business

Taylor Heywood
Research Assistant
The Kogod Cybersecurity Governance Center at American University's Kogod School of Business.

Rebekah Lewis
Deputy Director
The Kogod Cybersecurity Governance Center at American University's Kogod School of Business

Measuring Security Awareness Success

Our intent with this report is to help you identify what successful awareness programs are doing right. We've also examined what failing or immature awareness programs could be doing better. Our findings are based on a substantial data set and rigorous analysis completed by both the security awareness and academic community, so you can have confidence that they are accurate and meaningful.

Defining Success

What does it mean to have a prosperous and thriving awareness program? In the SANS community, we define it using the **Security Awareness Maturity Model**. Developed in 2011 by over 200 awareness officers, this model enables organizations to easily identify where their security awareness program is currently at, where a qualified leader can take it, along with an outlined path to get there. The model is based on five different stages, each stage building on the previous one, as defined below. In the survey, we asked: "What stage is your awareness program in?" The data extrapolated was compared with other results provided. The Maturity Model defines five main areas that an awareness program falls under.

Non-Existent: A program doesn't exist. Employees have no idea that they are a target, that their actions have a direct impact to the security of the organization, don't know or understand organization policies, and easily fall victim to attacks.

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

Promoting Awareness & Behavior Change: The program identifies the training topics that have the greatest impact in supporting the organization's mission and focuses on those key topics. The program goes beyond just annual training and includes continual reinforcement throughout the year. The 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: The 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. Thus, the program and cyber security is an established part of the organization's culture.

Robust Metrics Framework: The program has a robust metrics framework to track progress and measure impact. Consequently, the program is continuously improving and able to demonstrate return on investment. Important to Note: When we say "metrics framework", it doesn't imply that the methods of measurement are limited to the last stage of the model. We believe that 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 framework in place to demonstrate that change.

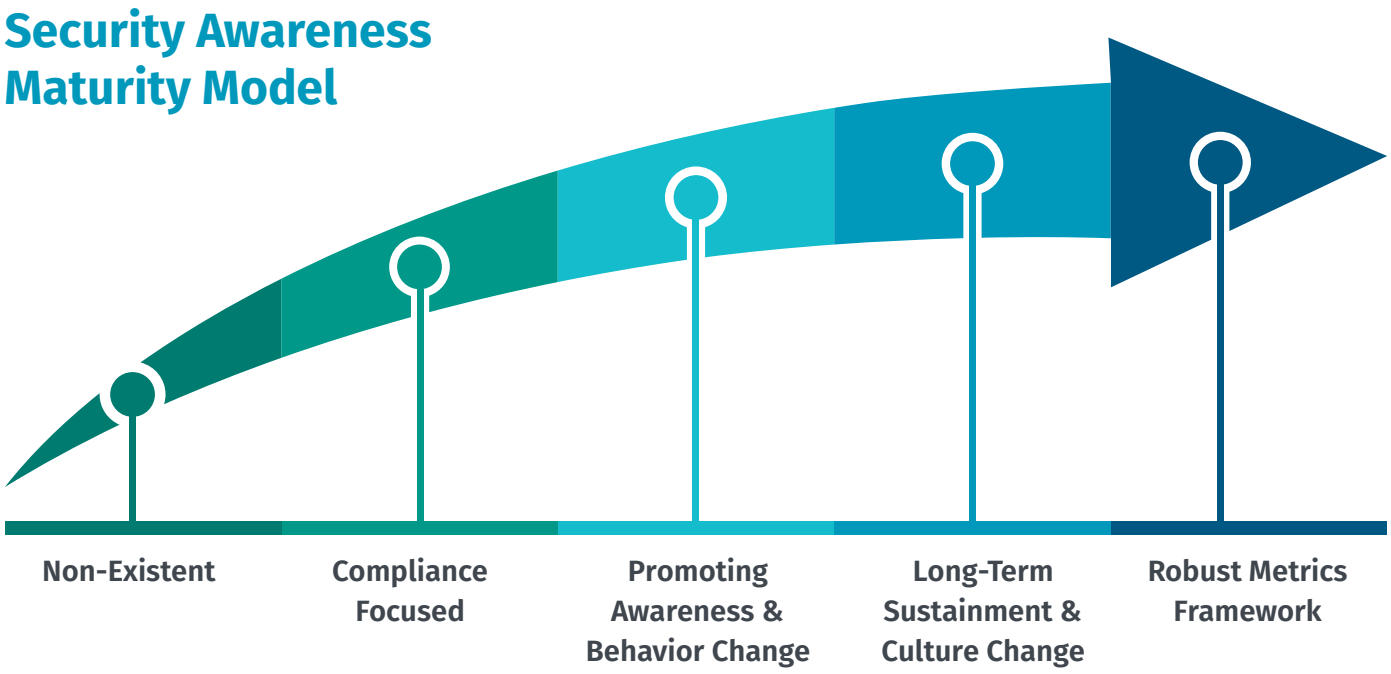

Fig. 1 - The Security Awareness Maturity Model

Maturity Level of Awareness Programs

How mature is the average security awareness program? Overall the numbers were very similar to last year, within 3 percentage points. It's heartening to see that more than half of respondents are currently promoting awareness and behavior changes, and are well on their way to establishing long term, sustainable programs.

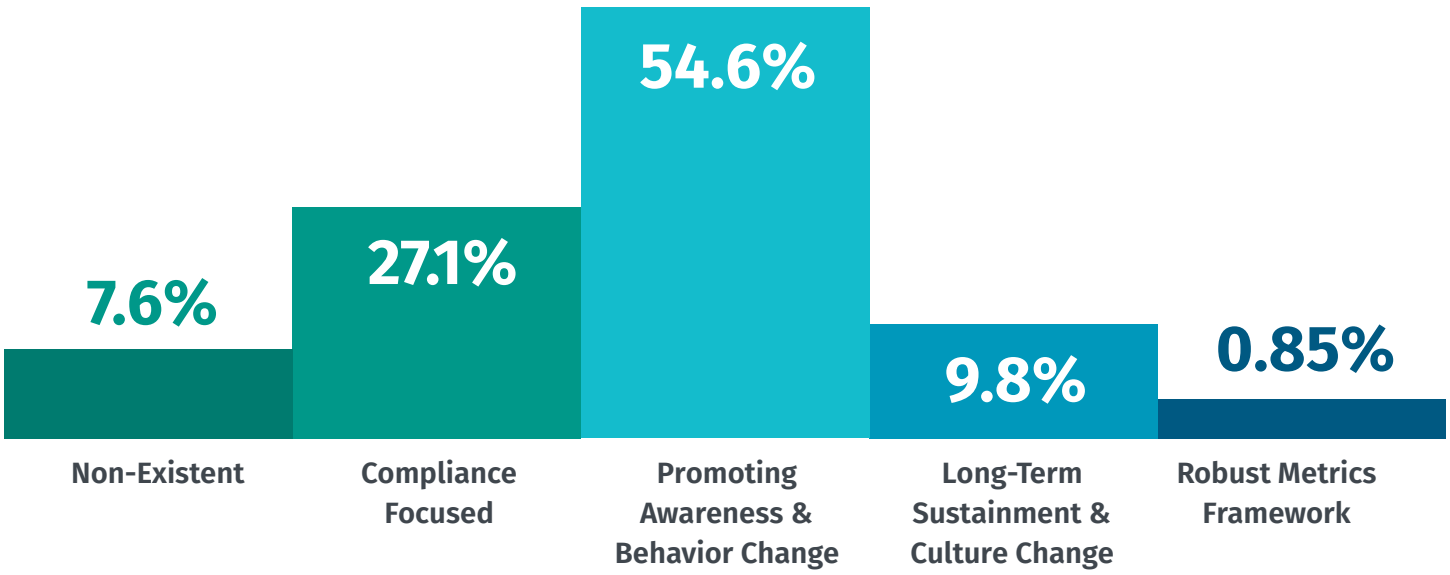

Fig. 2 - How mature is the average security awareness program?

What is Your Single, Biggest Challenge?

As with last year's report, we started the survey by asking awareness professionals what are the biggest challenges they face. We wanted to know what are the most common problems people are dealing with. How could we, as a community, help solve them? We asked the question, and heard a resounding response.

Fig. 3 - Community Challenges Survey Word Cloud

Overwhelmed? Yeah, so were we. Fortunately, the research team from the Kogod Cybersecurity Governance Center at American University dug into the details, evaluating the free form responses, to provide a breakdown for us, as you can see in the chart on the next page.

Major Challenges	Responses	%
Communication	113	15.98%
Employee Engagement	101	14.29%
Time	95	13.44%
Culture	85	12.02%
Resources	83	11.74%
Upper Management Support	80	11.32%
Other	66	9.34%
Money	42	5.94%
Enforceability of Program	31	4.38%
Staff	11	1.56%
Total	707	100%

Fig. 4 - By the Numbers: Major Security Awareness Challenges

Findings

Two findings pop out. First, communication is the number one challenge, followed closely by engagement. Working with organizations around the world, we found these two are very closely related, as poor communication is often a leading cause for failing to engage people.

The second finding is resources: although some respondents simply wrote "resources" as a challenge with no further description, those who did provide a more detailed description identified "time," and not "budget," as the most limiting resource. Based on this data, **the two biggest challenges security awareness professionals face are sufficient time and effective communication.**

Now that we understand the biggest challenges awareness professionals face, let's examine them in more detail and find a way to address them.

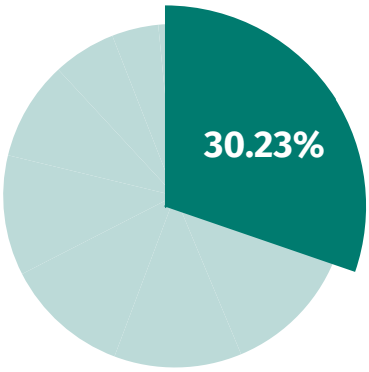

Fig. 5 - Communication + Employee Engagement

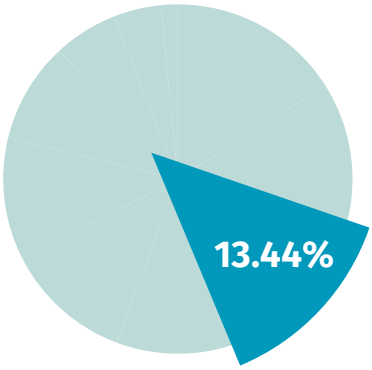

Fig. 6 - Time

The Importance of Time and Security Awareness

Overview

This year, as with last year, the data shows an overwhelming response from awareness professionals - they lack the resources needed to get the job done. 58% of respondents report the lack of resources hinders growth of security awareness programs within their organization.

Awareness is not a technical solution, it's a human solution. You need to talk with, engage, and collaborate with others - and that takes time.

However, since we had more data to work with this year, we dug deeper. That narrowed it down to time. The more time you have, and the more people you have helping you, the more successful your awareness program is. This makes sense. If you have all the budget in the world, and all the leadership support to back it up, but awareness is only 15% of your time, how can you plan, execute, measure and maintain your program? Remember, awareness is not a technical solution, it's a human solution. You must be talking with, engaging, and collaborating with others - and that just takes time. Seems like common sense, right? But let's look at what the data tells us, and share some insight on what you can do with it.

The Problem of Time

First, let's review the problem. Awareness is far too often a part-time job. Sadly, these numbers have stayed pretty much the same as in our 2016 report. Only 8% of awareness professionals are dedicated full-time to awareness. Instead, over 75% of awareness professionals spend 25% or less of their time on awareness. This is staggering. Imagine if your Incident Response team, Security Operations Center or Endpoint Security teams only focused on these responsibilities part-time, how good would your organization's security be?

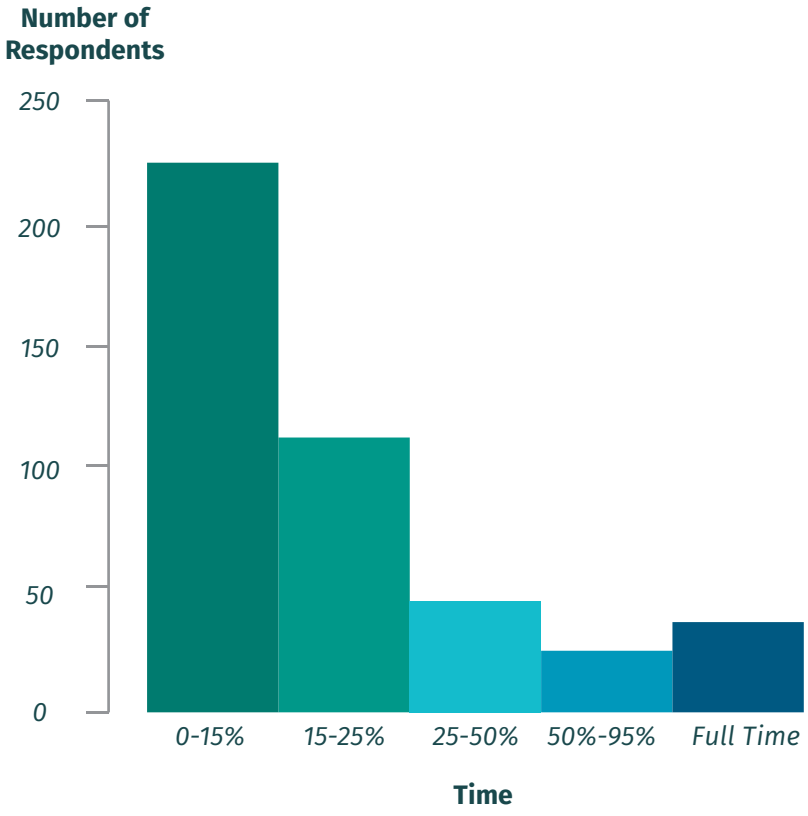

Fig. 7 - What percentage of your time is focused on security awareness?

Combine Full-Time Employee Assets

However, we should be careful before we jump to too many conclusions with the information listed above. Many organizations have multiple people involved in their awareness program, many of whom may be part-time. It's important to note that when someone says they work only 15% of their time on their awareness program, they could, in fact, be part of a larger, combined team effort. Which is why we asked awareness professionals what their total Full-Time Employee (FTE) manpower is dedicated to their awareness program. For example, if you have two people working half-time on an awareness program, combined their efforts are one FTE.

When someone says they work only 15% of their time on their awareness program, they could, in fact, be part of a larger, combined team effort.

We then compared that number to the maturity of their awareness program. The data was obvious, the more total FTEs you have dedicated, the more successful your awareness program will be, even if those FTE hours are divided among different people.

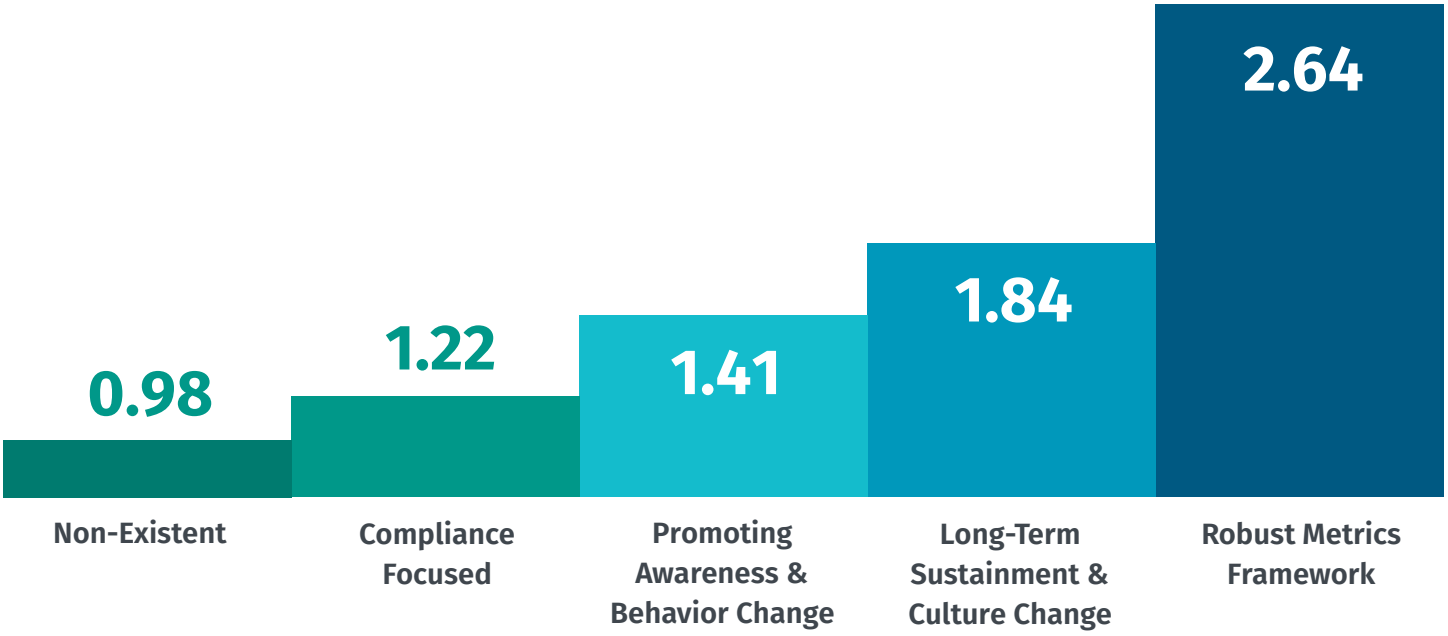

Fig. 8 - Average Number of FTEs by Maturity Level*

**This shows the minimum number of FTEs you need dedicated to awareness to achieve each maturity level. Organizations larger than 5,000 people most likely need more FTEs. Assumptions made as follows: 4+ answers were counted as 4, less than one response was counted as 0.5*

At the most basic level, you need at least 1.4 FTEs to begin changing organizational behavior. To achieve a truly mature program, including a strong metrics framework, you will need at least 2.6 FTEs. Remember, these numbers are an average. For larger organizations (5,000 or more people) or organizations that are highly regulated or with a low-risk tolerance you most likely need to increase those numbers. Long story short, if you have fewer than 1.4 FTEs dedicated to your awareness program, it's likely you're just checking the box for compliance purposes.

How Many FTEs is Standard in an Awareness Program?

Here is a breakdown of average number of FTEs per organization size. These numbers aren't an indication of success. We offer this information to help you benchmark your program to others based on your organization's size.

Organization Size	Average Number of FTEs
1 - 500 People	1.28
500 - 1000 People	1.30
1000 - 5000 People	1.24
5000 - 25,000 People	1.58
25,000 - 100,000 People	2.09
100,000 People or More	2.45

Fig. 9 - Average Number of Security Awareness FTEs per Organization Size

**This graph doesn't represent what we recommend for the number of FTEs dedicated to awareness. Instead, it shows the average number of FTEs organizations currently have. Refer to Figure 8 for FTE recommendations.*

Long-Term Planning

We then asked another question, *how detailed of an awareness plan do you have for next year?* Is the plan for your awareness program ad-hoc based, or do you have a comprehensive plan that identifies your top human risks? How will you communicate the key behaviors that will manage those risks? How well-prepared you are for next year is an indicator of how successful your program will be. It's not surprising, the more time you have, the more detailed your plan is for next year.

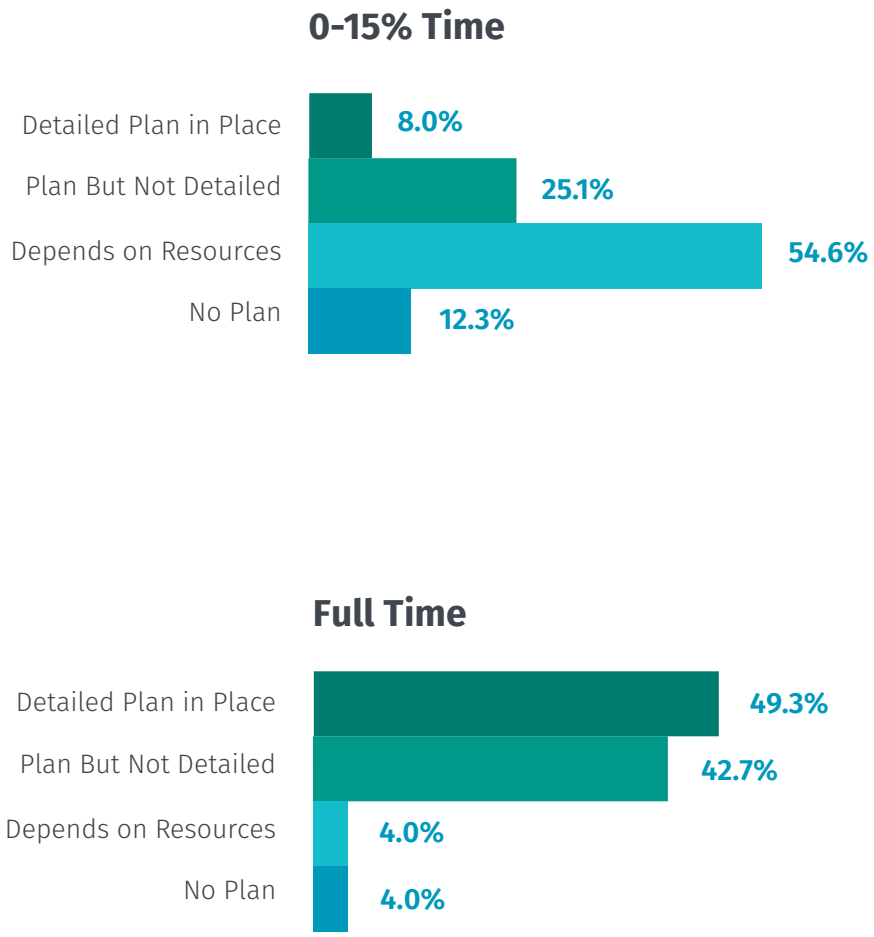

Fig. 10 - Time Spent on Security Awareness Planning

Money is NOT the Problem

It may seem like a bold statement, but you can't just throw money at a human-based problem. When we surveyed the community, we specifically wanted to know how big their budgets were for next year's awareness programs. The results were enlightening. The data shows us that while budget does have an impact on the maturity of your program, the correlation of **money and maturity** isn't nearly as compelling as the correlation between **time and maturity**. In fact, if you look at the fourth column below, "Promoting Awareness and Behavior Change" you'll see a relatively equal distribution across all levels of budgets.

Long story short, if you don't have time to get the job done, no amount of money is going to ensure a successful awareness program.

Budget	Non-Existent	Compliance Focused	Promoting Awareness & Behavior Change	Long-Term Sustainment & Culture Change	Robust Metrics Framework
Less than $5K	9.87%	**27.63%**	**44.74%**	6.58%	0.99%
$5K - $25K	2.65%	**19.58%**	**59.79%**	10.05%	0.00%
$25K - $50K	6.41%	**20.51%**	**56.41%**	6.41%	1.28%
$50K - $100K	4.84%	**20.97%**	**53.23%**	**12.90%**	0.00%
$100K or more	0.00%	16.92%	**43.08%**	**24.62%**	1.54%
I do not know	7.97%	**25.90%**	**40.64%**	5.58%	0.80%

Fig. 11 - Budgets per Security Awareness Maturity Level

It's important to mention that many respondents didn't know what their security awareness program budget was at all. More than a quarter of respondents indicated that they were uncertain of their budget, and this data has gone up slightly from last year's report. This is puzzling: why do so many awareness professionals not know their own budgets? Is there a lack of transparency or accessibility of that information? Could there be a communication blocker between the awareness officers and the executive responsible for budgeting?

Many respondents didn't know what their security awareness program budget was at all.

This might be an indicator of lack of support. **We believe it comes back to the issue of communication.** It's one of the key challenges that security awareness professionals face.

Recommendations

Too many organizations treat security awareness as an afterthought; someone (often in IT) is randomly assigned the responsibility of awareness without the time or support to be successful. To create a secure culture, security awareness needs to be recognized as a profession, just like other security fields, and provide those professionals the resources (both personnel and budget) to be successful.

Full Time Employees

You need at least 1.4 FTEs to begin changing behavior at an organizational level. To truly achieve a mature program, including a strong metrics framework, you'll need at least 2.6 FTEs. Remember, these numbers are averaged across all organizations, in all industries and sizes. Most likely you'll need to increase the number of FTEs for organizations that are larger (5,000 or more people), for those that are highly regulated, and those organizations with a low-risk tolerance.

Partnerships

Build partnerships! We can't stress this enough. Collaborate with others in your organization to help you. A critical partnership is one you can make with your communications department, as they can help communicate the importance of your program (as we cover in the next section) and help you achieve adoption. Other groups may also help you as you build a program. These include marketing, project management, human resources, graphic design teams - even a help desk may provide support. Don't underestimate the power of building relationships within your organization. Take them out to lunch and talk to them.

Buy Time

If you have budget, use that to buy yourself time. Appropriate the budget to a graphic designer to help create materials. Hire a contractor specializing in social science to help you build surveys. The more you can delegate, the more time you have to plan, maintain, and measure.

Ambassadors

For awareness programs that are more mature, consider building a security ambassador program. Ambassadors are a network of volunteers throughout your organization to help engage fellow employees and push your message out.

Curious about building an ambassador program?

Check out this webcast on Security Ambassadors
https://www.youtube.com/watch?v=IeMTH3ZDziM

Communication is Critical

Overview

Last year we found that a lack of soft skills was a significant blocker to a successful awareness program. We recognize that a variety of soft skills are needed (such as collaboration, planning, project management, instructional design, etc.) but one stood out as more important than the rest - communication. We want to be clear – communication means having the ability to talk to and engage employees, as well as having the ability to connect with leadership and demonstrate the organizational value of security awareness. Let's take a closer look.

What's Your Background?

Did you know? An overwhelming majority of awareness professionals come from a technical background. 80% in fact. Less than 8% have a soft skills background such communications, marketing, training or human resources. Those with a technical background have an advantage because they possess a strong understanding of the technical and human risks. They know what behaviors are the most effective in managing those risks. However, these same individuals often lack the skills or training necessary to effectively communicate those risks and engage employees in a manner that effectively changes behavior.

80% of security awareness professionals come from a technical background - but less than 8% have a soft skills background.

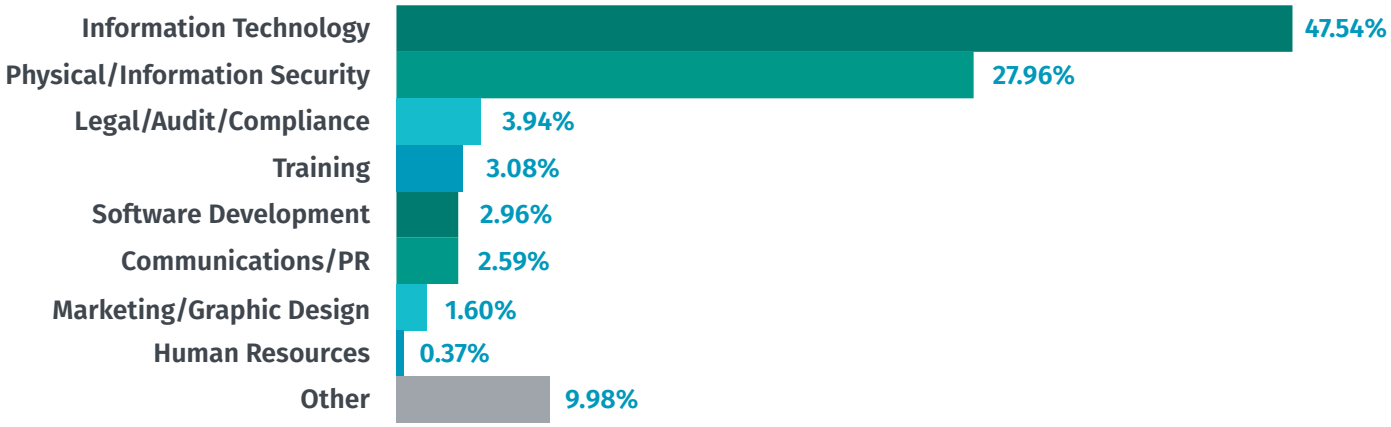

Fig. 12 - Which most closely describes your role before you became involved in security awareness?

Additionally, those most familiar with technology often suffer from a concept called the **Curse of Knowledge**. This is a type of cognitive bias. It means that the more of an expert an individual is at something, the more difficult it is to teach or communicate that topic to others, as the individual projects his/her knowledge onto the target 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. They then often build their awareness program based on these misconceptions. As a result, what they communicate may result in a complete mismatch from what people in the organization actually need. Making matters worse, when a security professional communicates to leadership, they often do so using technical terms. This is a mistake and an essential breakdown in communication. Security professionals must speak to leaders in the vernacular they are accustomed to maintain support. The recent **Cyber Balance Sheet Report, provided by Cyentia Institute** offers insight on communicating about cyber security to Board members:

> ***"The cyber security program might run on bits and bytes, but Directors want none of that in the Boardroom. Notice how soft rather than hard skills dominate the list of tips from CISOs and Board members."***

No Communication = A Blockade

You might feel like saying "that's not really an issue," if awareness professionals are poor at communicating, because your communication's department can do the talking and engaging. Unfortunately, for a second year in a row, we see that **the communications department is the biggest blocker** for awareness professionals.

Over 40% of the 2017 respondents indicated that they had "No Blockers" - an improvement of more than 17 percentage points over 2016

The good news is that this year, we saw a drop in the percentage of people reporting communication as a blocker, but the bad news is communication is still the biggest blocker to achieving a successful program. Our hope is that we'll begin to see more partnerships between security awareness professionals and communication departments as programs mature.

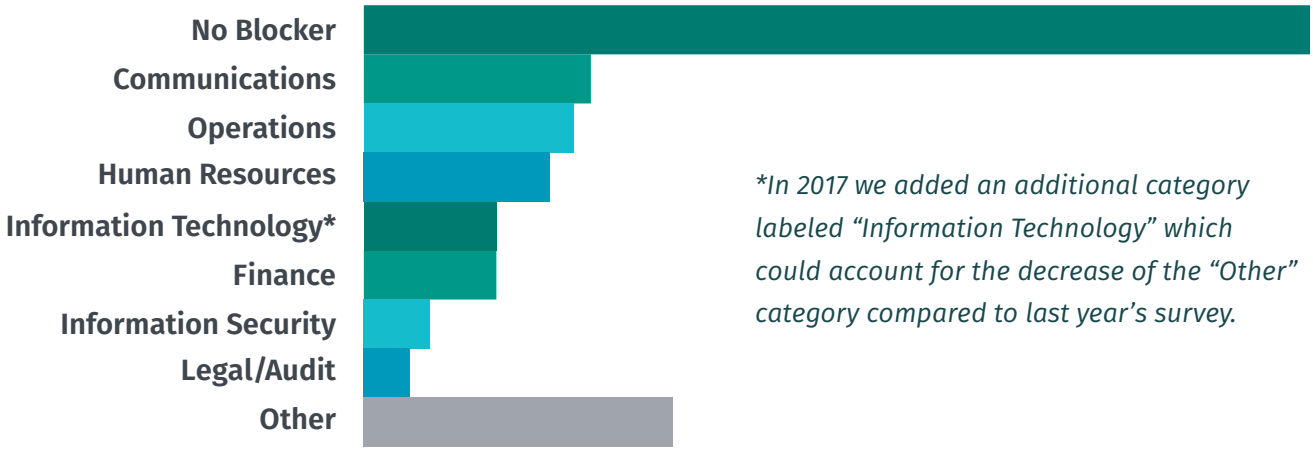

Fig. 13 - What individual/role/department is the biggest blocker to your program?

Leadership Support

One of the things we want to emphasize about communication is that it goes both ways; up the leadership ladder as well as down. Traditionally awareness professionals focus on communicating to employees because that's where they most often want to change behavior. But they also need the support from leadership. As we saw from the year prior, the data again proved this year that the more leadership support an awareness program has, the more likely the awareness program will succeed.

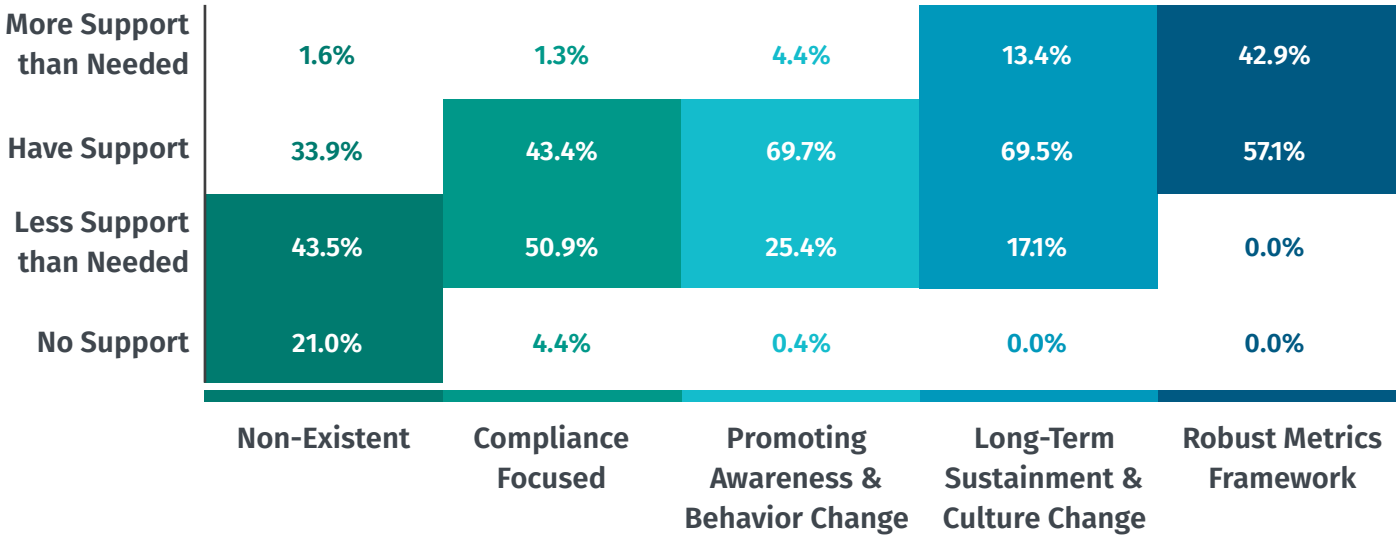

Fig. 14 - Leadership Support by Security Awareness Maturity Level

Still not fully sold on the importance of leadership support? Here is the kicker - the data screams loud and clear, the more leadership support you have, the fewer blockers you have. In other words, leadership provides you with the credibility you need to break down barriers and collaborate with other departments in your organization. It's critical to success.

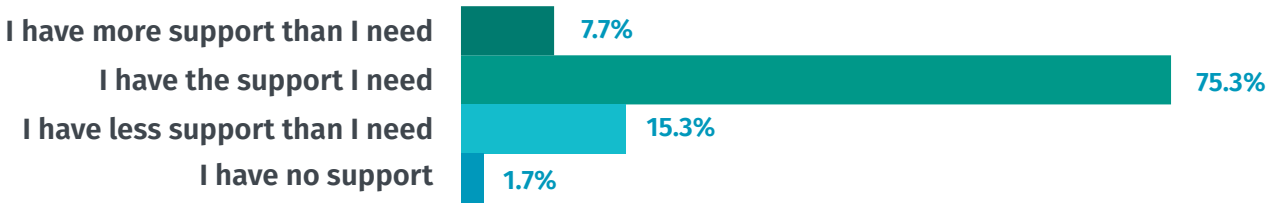

Fig. 15 - No Internal Blocker

Combined, these two graphs demonstrate a strong need for leadership support to create mature, sustainable information security programs. One reason so many programs fail to receive the necessary support is that awareness officers are not effectively communicating the value of their awareness program to organizational leadership.

Recommendations

To review, when we say communication, we mean the ability to engage employees with a meaningful message, identify and deliver the right content to the right people, and leverage multiple communication methods. We also believe that communication includes the capability to communicate to leadership the value and impact of the awareness program. What can you do to increase communication around your security awareness program?

Leadership

Dedicate a certain amount of time each month for communicating to leadership about your security awareness program (i.e. 4 hours a month). That doesn't mean you'll spend 4 hours every month talking to leadership. It means you'll spend 4 hours every month collecting the data and success stories that demonstrate the impact your program is having. You should then ensure you're communicating in business terms that leaders value.

Champion

Find yourself a strong champion within the leadership team. Have that leader help communicate the value of your program to other leaders. Ask them if they'll aid you in crafting your message in the language that business leaders understand and will act upon.

Partnership

Don't have the skills you need to effectively communicate? Then partner with those that do. Work with the communications team and see if they'll have someone partner with your security team, perhaps even embed someone in security. Don't have a communications department? Then try working with someone in marketing or the public relations team.

Communications Training

Learn the skills you need to effectively communicate. If you don't have the skills today, it's critical you gain them to help gain adoption for your awareness program.

Human Resources

Work with human resources to better understand your organizational culture and connect with new hires.

Build and Bridge – Effectively Communicating Your Ideas

A favorite book in the security awareness community: *"Made to Stick: Why Some Ideas Survive and Others Die"* by Dan and Chip Heath. It's about getting making your ideas "sticky", transforming the way you've traditionally communicated to teams to gain better traction.

Demographics and Additional Information

Gender

We had a hunch this year – and decided to ask respondents their gender. Our theory, based on all the different security awareness events we've participated in, is that there is a far higher percentage of women in security awareness than other cyber security fields. The data definitely pointed to a higher percentage of women, 30% in fact.

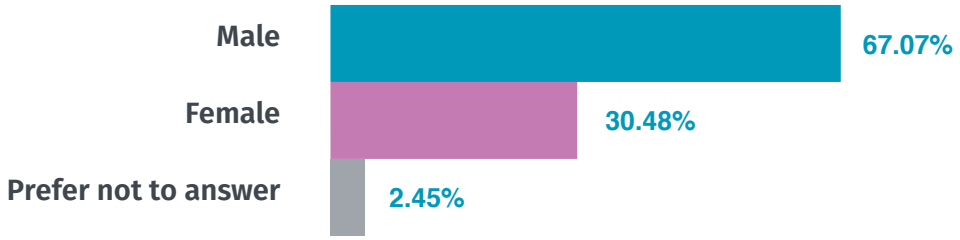

Fig. 16 - Women in Cyber Security

However, 30% was lower than we expected. We expected something more along the lines of a 50/50 ratio. After examining the data further, we uncovered some startling information. While there is a lower percentage of women involved in awareness than we expected, there are far more women actively involved in leading awareness programs. We found that if an individual is dedicated full-time to security awareness, they are twice as likely to be a woman. Furthermore, if an individual spends 15% or less of their time dedicated to awareness, they are three times as likely to be a man.

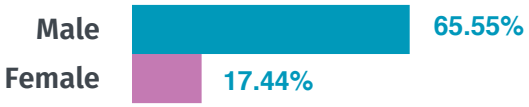

Fig. 17 - Security Awareness Professionals Dedicated Less Than 15% of Time to Program

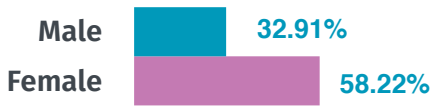

Fig. 18 - Security Awareness Professionals Dedicated to Programs Full Time

One hypothesis that explains this: if an individual spends 15% or less of their time on security awareness, most likely someone randomly selected that person from the IT or security team to add awareness to their other responsibilities. However, if an organization hired someone specifically to be dedicated full-time to awareness, then most likely, the organization sought someone with strong soft skills such as communication.

Women were twice as likely as men to have that background in soft skills. On the flip side, men were three times as likely to have a technical background.

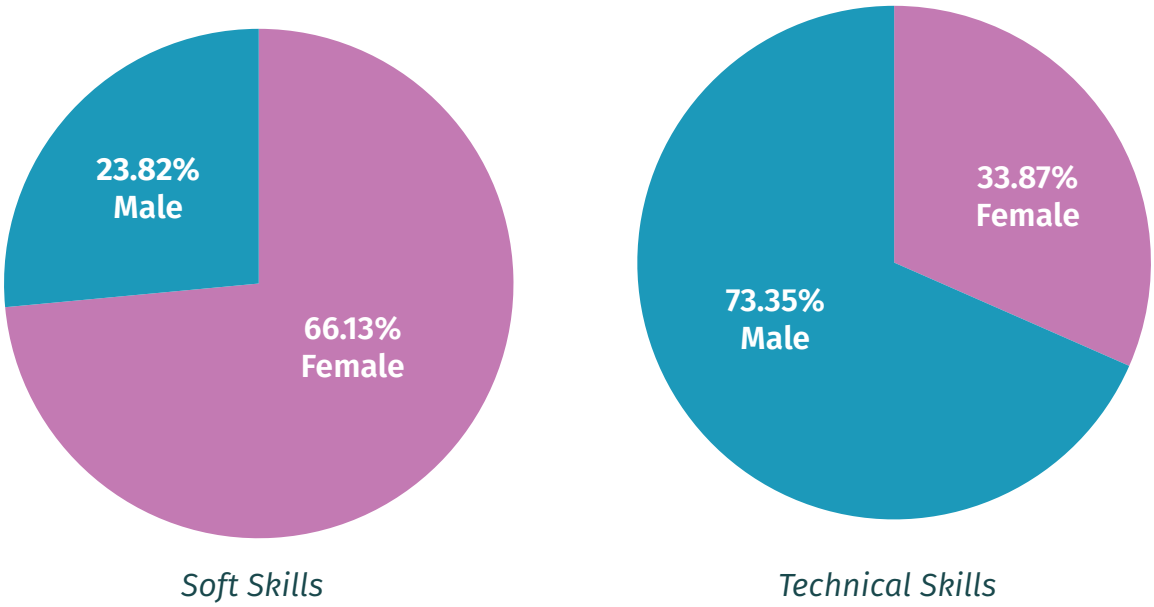

Fig. 19 - Soft Skills and Technical Skills – Gender Percentages

What the data implies is that as awareness programs mature, and organizations begin to hire people full-time for their awareness program, they are tapping people with soft skills, as that is where many security awareness programs are weakest, and they are currently finding these skills in female professionals.

Industries

We struggled with industries last year as we were educational heavy, due to our partnership with EDUCAUSE. However, we're happy to report a better distribution of respondents spanning across multiple industries this year. We're still not sure if the graph below represents which industries are most actively deploying awareness programs or if the industries represented are then ones we happen to be most actively reaching with our survey. Our guess is it's a bit of both. In the future, we hope to start releasing reports that are specific to different industries. One example is **EDUCAUSE's derivative report on the higher education sector**, which is based on our 2016 data.

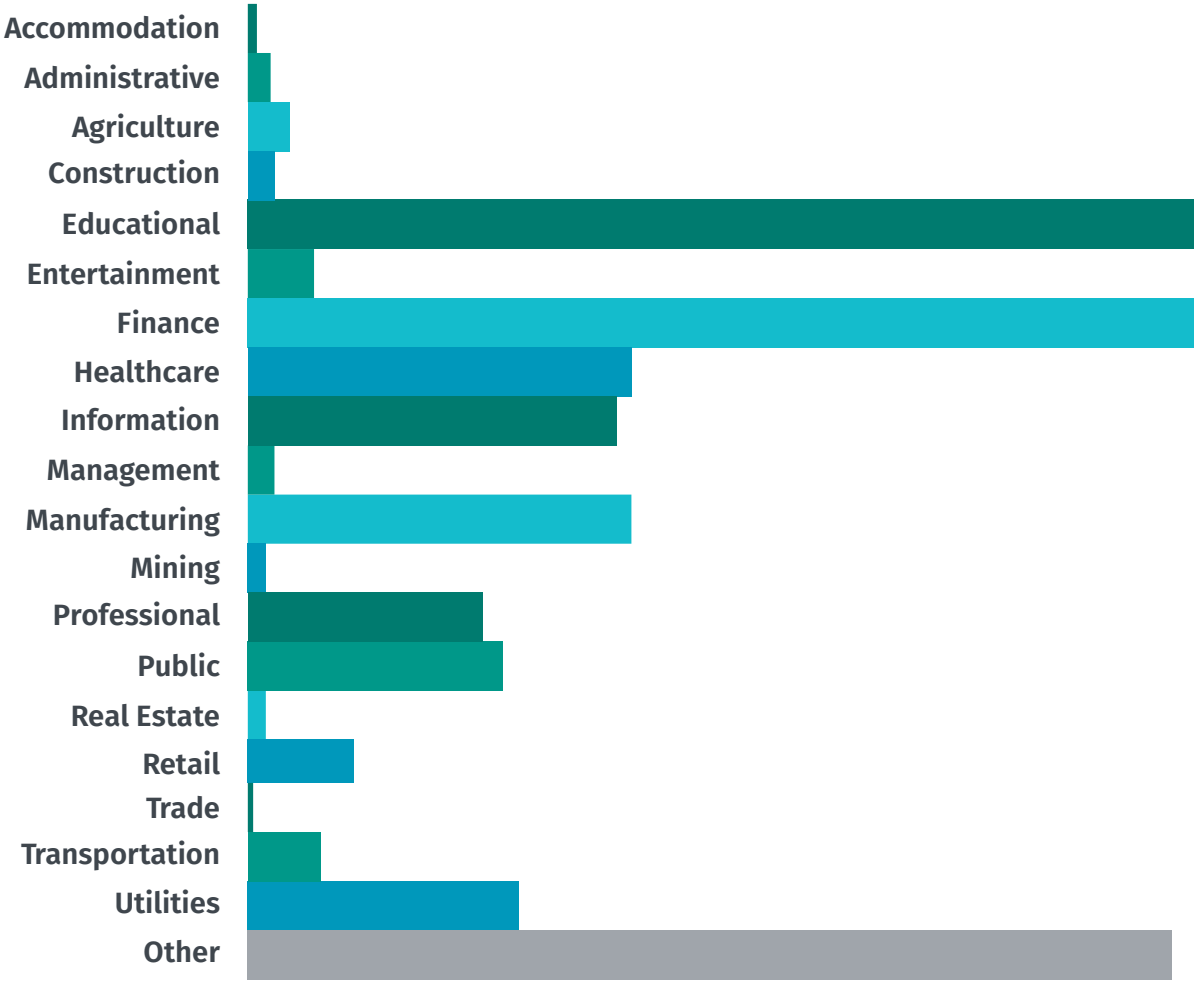

Fig. 20 - What industry is your organization in?

**Please note we us the same industry list as Verizon DBIR.*

Industries

How global was this survey? 67% of respondents are from organizations in the United States and 33% were outside of the United States.

Fig. 21 - Global Survey Response Distribution

Conclusion

Ultimately, security awareness is hard. However, there are some key steps you can take to improve your program. Whether you're able to dedicate your time fully to the improvement and success of your awareness program or if you only have a small part of each week to focus on it – there are two major takeaways identified as critical to a thriving program. Time and Communication. Without these two important pieces, it'll be difficult to get legs to your program and successfully protect your organization and the people within it.

Recapping on the importance of time, we've outlined that to have a thriving program you need:

1. **FTEs:** You need at least 1.4 FTEs to begin changing behavior at an organizational level. To achieve a truly mature program, including a strong metrics framework, you will need at least 2.6 FTEs.
2. **Partnerships:** Build partnerships and collaborate with others in your organization to help you.
3. **Buy Time:** If you have budget, use that to buy yourself time. Hire people to help you get your awareness program off and running.
4. **Ambassadors:** For awareness programs that are more mature, consider building a security ambassador program. This is when you build a network of volunteers throughout your organization to help engage fellow employees and push your message out.

Communication is highly-valued in starting, growing, and expanding a security awareness program.

1. **Leadership:** Dedicate a certain amount of time each month for communicating to leadership about your security awareness program. Make sure you communicate to leaders every month in the vernacular that business leaders will value.
2. **Champion:** Find yourself a strong champion within leadership. Use that leader either to help communicate the value of your program to other leaders, or have them help you craft your message in the language that is actionable to other leadership.
3. **Partnership:** Don't have the skills you need to effectively communicate? Then partner with those that do.
4. **Communications Training:** Learn the skills you need to effectively communicate. Just because you may not have the skills today, doesn't mean you won't have them next year.
5. **Human Resources:** Work with human resources to better understand your organizational culture and connect with new hires.
6. **Target Audiences:** As your awareness program matures, begin to identify different target groups in your organization. Organize your communications plan based on what resonates best for each target group (such as IT admins, developers, field engineers, faculty, doctors, etc.).

A Big Thanks

We'd 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 very big shout-out to the following who volunteered their time to make this report happen.

Sahil Bansal

Sahil leads the security awareness, training and culture change initiatives at Genpact. He is a B.Tech, MBA and has done courses on Social Psychology, Behavior Economics, marketing and branding. At present, he is helping Genpact information security team to look at the problem from a people perspective. He has also worked with other IT giants like Infosys and HCL Technologies in the past.

Jessica Fernandez

Jessica specializes in making the complicated work of securing information SIMPLE for the everyday user. Working in many different industries, Jessica helps employees to understand their role in securing information through security training and award-winning awareness campaigns. With a background in Marketing and Communication, Jessica works to grow internal branding for Information Security groups, which is pivotal in translating cyber security in a way that is engaging and palatable. Running a communications and change management company, Jessica works as an independent consultant for the Warner Bros.' InfoSec team, developing thought provoking awareness campaigns, video content and eLearning which included the Put Yourself in the Picture awareness video series and Superhero Academy trainings winners of the learning and InfoSec community awards, Brandon Hall and CSO50.

Joanna Lyn Grama

Joanna Lyn Grama, JD, CISSP, directs the EDUCAUSE Cybersecurity Initiative and the IT GRC (governance, risk, and compliance) program. Joanna has expertise in law, IT security policy, compliance, and governance activities, as well as data privacy.

Valerie M. Vogel

Valerie M. Vogel is a senior manager for the EDUCAUSE Cybersecurity Initiative, overseeing the Higher Education Information Security Council (HEISC) and the annual Security Professionals Conference. She has served as a community manager for information security and privacy professionals in higher education for over 15 years.

Ingolf Becker

Ingolf is a finishing PhD student at University College London under the supervision of Angela Sasse and Sebastian Riedel. His work borrows ideas from Machine Learning and Natural Language Processing and applies them to Security Problems in novel ways. This approach allows him to disseminate complex problems, and find patterns in large amount of data that previously required lengthy manual analysis. His recent focus has been on studying the relationship between business processes and security in organizations by working with security and awareness professionals as well as ordinary employees alike.

Jon Homer

Jonathan Homer, CISSP, has spent the last 15 years working in various areas of Cyber Security and Information Technology, specializing in incident response, industrial control systems, internet and digital telecommunications architecture, and security awareness. He has a background in organizational change management, disparate data reconciliation, project management, and continuity planning. Jon is well known for his communication skills and was the author of the nationally renowned "Who's in Your PC?" security awareness campaign, and the "Neutron Works" end-user utilization initiative. He previously managed a cross-cutting team across five different security-related departments as well as overseeing various Organizational Change Management initiatives.

Mark Lukas

Mark Lucas is a 19-year veteran at the California Institute of Technology's Information Management Systems and Services department. During his tenure, his technical skills have grown to include multiple products from Microsoft, Cisco, VMware and Amazon Web services. A four-year member of Toastmasters International, Mark recently earned his Distinguished Toastmaster Award. Last year, Mark began his Masters of Information Security Management at the SANS Technology Institute. In his spare time, he and his wife Karen attempt to keep up with their children Xavier and Emily as they follow in their father's footsteps, hacking Minecraft and their mother's, traveling and hiking to new locations in search of rare Pokémon.

A Big Thanks

We'd 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 very 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 cybersecurity. Through multidisciplinary research and collaboration, KCGC aims to promote responsible cybersecurity governance by providing today's leaders with actionable and well-supported guidance that will help them overcome challenges and maximize opportunities arising from the cybersecurity issues that are essential to their core stakeholder responsibilities. For further information about the Center, visit **www.american.edu/kogod/cybergov**.

Zoë Bludevich

Zoë Bludevich is a KCGC Research Assistant and MBA student at KSB. 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 on white collar crime, government enforcement and foreign corrupt practice cases. As a student at Kogod, she co-authored a case study exploding the OBHR complexities of integrating an Information Technology Department within the Washington D.C. area power supplier, PEPCO.

Aria Chehreghani

Aria Chehreghani is a KCGC Research Assistant and a graduate student in the United States Foreign Policy and National Security program at American University's School of International Service. He received a BA in Journalism from the University of Maryland, College Park. Aria's research interests include the intersection of cybersecurity with the policymaking process and the utilization of cyberwarfare by both state and non-state actors. His other research interests include combating the threat of Boko Haram, the Sinai Province, and diminishing the recruitment process of terrorist groups on social media. Aria is additionally studying the Persian language.

Michael Giampiccolo

Mike Giampiccolo is a KCGC Research Assistant and an undergraduate student at KSB, where he is pursuing a Bachelor's of Science in Business Administration with dual specializations in Accounting and Information Technology. His primary research interests in cybersecurity 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 cybercrime over the next few years.

Taylor Heywood

Taylor Heywood is a KCGC Research Assistant and an undergraduate at American University (AU), triple majoring in Computer Science, Applied Mathematics, and Business Administration. Outside of working at the KCGC, she also works as a teaching assistant in AU's Computer Science Department and is a competitive member of the AU Mock Trial Team. She serves on the executive board of the AU Chapter of the Association for Computing Machinery (ACM) and is a member of Upsilon Pi Epsilon and Betta Gamma Sigma. She is most interested in developing novel ways to communicate complex cyber security concepts to those without a technical background and researching ways to improve information security without impacting efficiency or convenience.

Rebekah Lewis

Rebekah Lewis, JD, CISSP, CIPP/US, is an Executive in Residence and the Deputy Director of the Kogod Cybersecurity Governance Center (KCGC) at American University's Kogod School of Business (KSB) in Washington, D.C. In addition to her role with the KCGC, Rebekah also teaches Cybersecurity Governance at KSB. She previously served as a cybersecurity and information assurance attorney for the U.S. National Security Agency and practiced law as an associate in the Washington office of Latham & Watkins.

About SANS Security Awareness

SANS Institute is the by far 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 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 has worked with over 1,400 organizations and trained over 8 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 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 security awareness program:

SANS Security Awareness has worked with over 1,400 organizations and trained over 8 million people around the world.

- 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 several of these tasks, saving time and ensuring organizations follow a proven roadmap to success.
- Managed services support security awareness officers from program start up to measuring success.
- The world's largest and most engaged community of cybersecurity 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's unwavering commitment to helping organizations effectively understand, manage, and measure their human cyber risks. To learn more, visit **SecuringtheHuman.sans.org**.

SANS SECURITY AWARENESS

securingthehuman.sans.org | info@securingthehuman.org