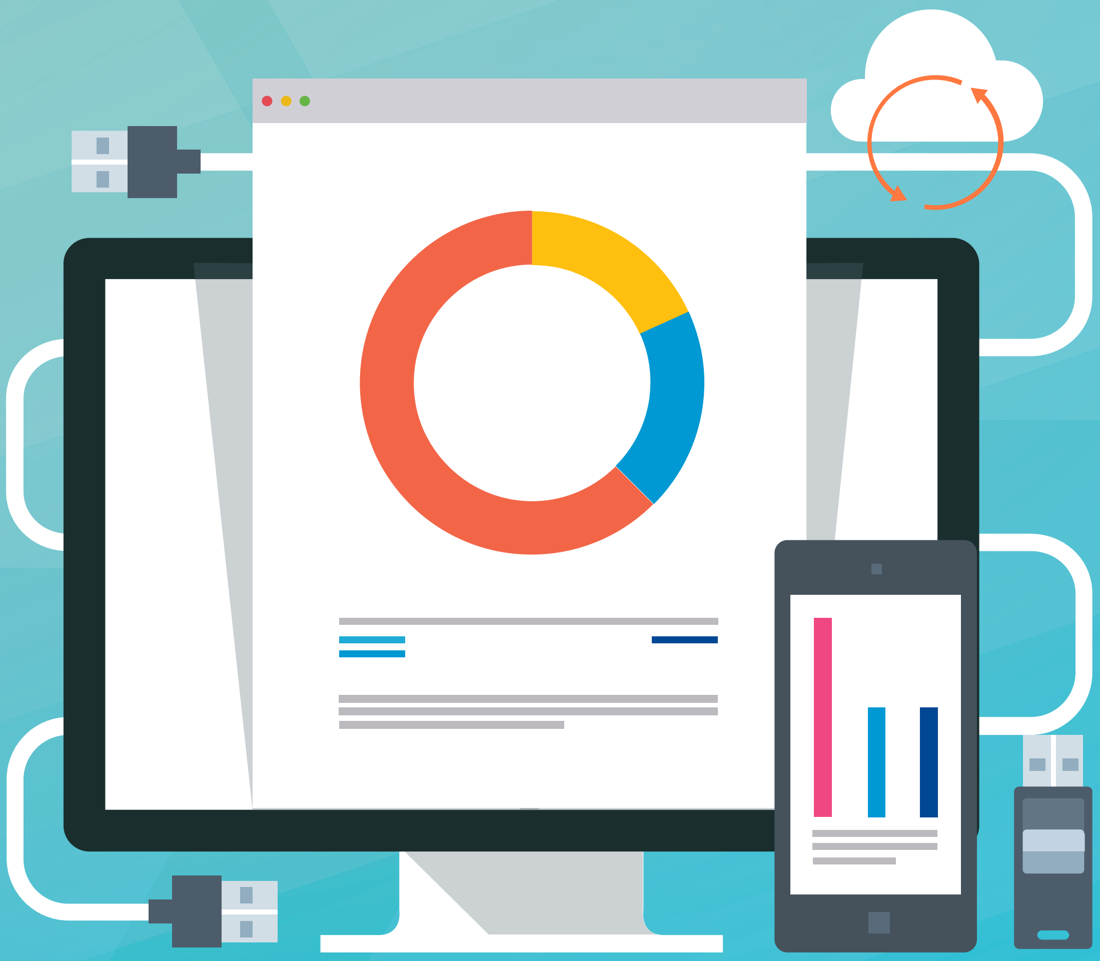
Security Awareness Report



Awareness Is Hard: A Tale of Two Challenges

2016

SANS Securing The Human

Contents

Report Summary 3

About This Survey 4

Your Biggest Single Challenge 5

Resources, Support, and Time (or Lack Thereof) 7

The Geeks Have Inherited Awareness (Is That Good?) 15

Demographics and Additional Information 21

Conclusion 24

A Big Thanks 25

About SANS Securing The Human 27

Report Summary

Don't have a lot of time? Then just read this page. The SANS Securing The Human 2016 Security Awareness survey uncovered two key findings:

1. **SUPPORT IS ESSENTIAL:** Security awareness teams are not getting the support they need to be successful. Over 50% of awareness personnel surveyed have a budget of $5,000 or less or don't know what their budget is. Less than 15% of awareness personnel are dedicated full-time to their job. While this is an improvement from last year's 10%, we are concerned that is still too low. In fact, 64% of people reported spending less than a quarter of their time on awareness. Finally, 35% report not having the executive support they need. Why is all of this important? Because the data shows a strong relationship between the amount of support you have and the maturity of your security awareness program. We need to do a better job of educating leadership that security cannot be solved by technology alone; it must also address the human factor. Key steps to achieving this include demonstrating to leadership that you have a proven roadmap to creating a secure culture and the metrics to show leadership the impact your program is having.

2. **SOFT SKILLS ARE LACKING:** Last year, we reported that soft skills are lacking in security awareness personnel. By soft skills, we mean skills such as communications, change management, learning theory, and behavior modeling. The data told the same story this year: over 80% of security awareness personnel have a technical background, with skills such as debugging network traffic, building websites, or securing a server. However, this also means that many security awareness teams don't understand the proven concepts and techniques in changing behavior and culture. In addition, we identified communications as one of the key soft skills lacking. By communications, we mean engaging employees with a meaningful message, delivering the right content to the right people, leveraging multiple communication methods, and building a roadmap that pulls this all together. One successful approach is embedding someone from your communications department into your security team. A second option is to train your awareness team on the new skills they will need. A third option is to contract or hire someone with strong soft skills. Long story short, you not only need security expertise on your awareness team, but you need soft skills, starting with communications.

Security awareness is hard. Today's security awareness teams don't have the support, time, and resources they need to be successful and/or are missing the skills and experience to effectively engage and train their organization.   The rest of this report is dedicated to better understanding these two challenges and their different solutions.

About This Survey

Welcome to the second annual SANS Securing The Human Security Awareness Report. The purpose of this report is to enable security awareness officers to make more informed decisions on how to improve their security awareness programs and compare their program to other organizations in their industry. To accomplish this, we conducted a survey in November 2015. 369 people responded to it, twice as many as the previous year. This increase shows not only a more committed group of awareness professionals, but a growing demand for integrating security awareness into organizations. This report is based on the results from that survey.

Before we continue, we would like to recognize several very smart and hardworking volunteers who made this report possible. You can find the full bio of each of these amazing folks at the end of this report.

- **Bob Rudis**: Chief Security Data Scientist, Rapid 7
- **Lance Hayden**: PhD Managing Director - Security Culture Practice, Berkeley Research Group
- **Grace Kretschmer**: MSIS Candidate at the University of Texas, School of Information
- **Angela Sasse**: Professor, University College of London
- **Ingolf Becker**: PhD Student, University College of London
- **Jon Homer**: Cyber Security Data Analyst

If you have any feedback, questions, or suggestions on this report, please reach out to us at <sth-community@sans.org>. We are especially interested in knowing what questions you want asked for next year and what you want to know that will help you. With that said, let's get started.

In last year's report, we provided the data and results in the order the survey was taken. This year, we decided on a different approach. This year, the data tells a story, a tale of two challenges. As such, we will start our story at the beginning – your biggest single challenge.

Your Biggest Single Challenge

One of the key things we wanted to understand was what were the biggest challenges security awareness officers faced. What problems are they dealing with and how could we, as a community, help solve them? So we literally asked that question: what is the single biggest challenge you are facing? We received over 100 different topics, as can be seen in the word cloud below.

Overwhelmed? Yeah, so were we. Fortunately, Ingolf Becker from University College of London dug into all the free responses and categorized them into 12 categories, which you can see below. The first seven categories represent 93% of all the responses, so we will focus there.

Categorization of Biggest Challenge Awareness Programs Face

Problem Category	Number of Responses	Percentage
Resources	50	19%
Adoption	48	19%
Support from management	47	18%
End user support	27	10%
Finding time to take part	24	9%
Content	23	9%
Not enough awareness staff	22	9%
Non-mandatory	9	3%
Legal department	4	2%
Non-punishable	2	1%
Translations	1	.05%
Metrics	1	.05%

The first thing you notice is that the first seven categories fall into two general groups: lack of resources, support, and time and/or not having an impact. People are either constrained in their ability to execute (highlighted in blue, 46%), and/or are failing to deliver the needed impact (highlighted in grey, 47%). And that is the crux of our story, our "tale of two challenges." The rest of this report is dedicated to understanding these two challenges and identifying potential solutions.

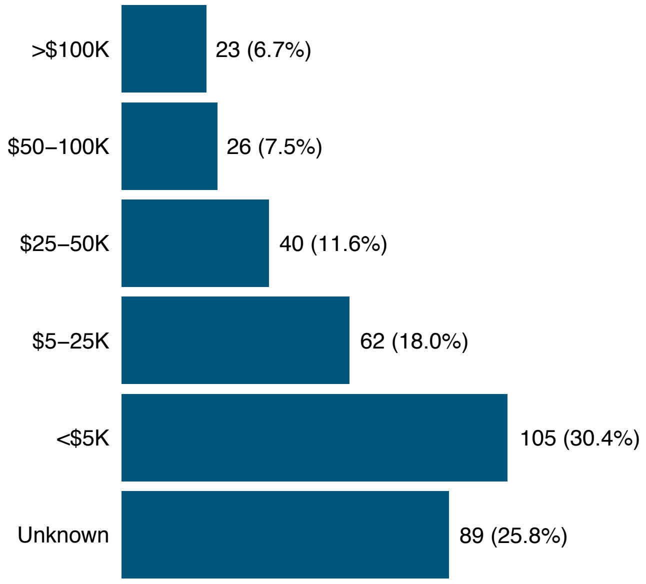
Resources, Support, and Time (or Lack Thereof)

For those who read last year's report, this should not be a surprise: the data again shows that many awareness personnel lack the resources, support, and/or time they need to get the job done. Overall, it looks like things have improved from last year, but not nearly enough. Ingolf defined these three categories as follows.

- **Resources:** A shortage of technical resources and money.
- **Support from Management:** Superiors do not see the necessity for the awareness campaigns and/or fail to collaborate and facilitate.
- **Not Enough Awareness Staff:** Self-explanatory.

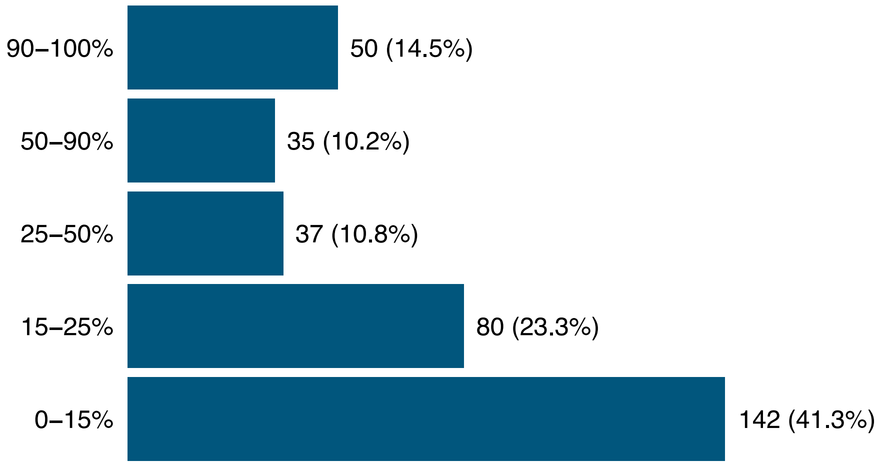
Regarding budgets, over 50% of respondents reported either having a budget of $5,000 or less or they did not know if they had a budget. Only 25% reported a budget of $25,000 or more. Oddly enough, you would expect that larger organizations would have the bigger budgets of $25,000; however, we saw those budgets distributed pretty evenly across all organization sizes.

Estimated Budget for 2016



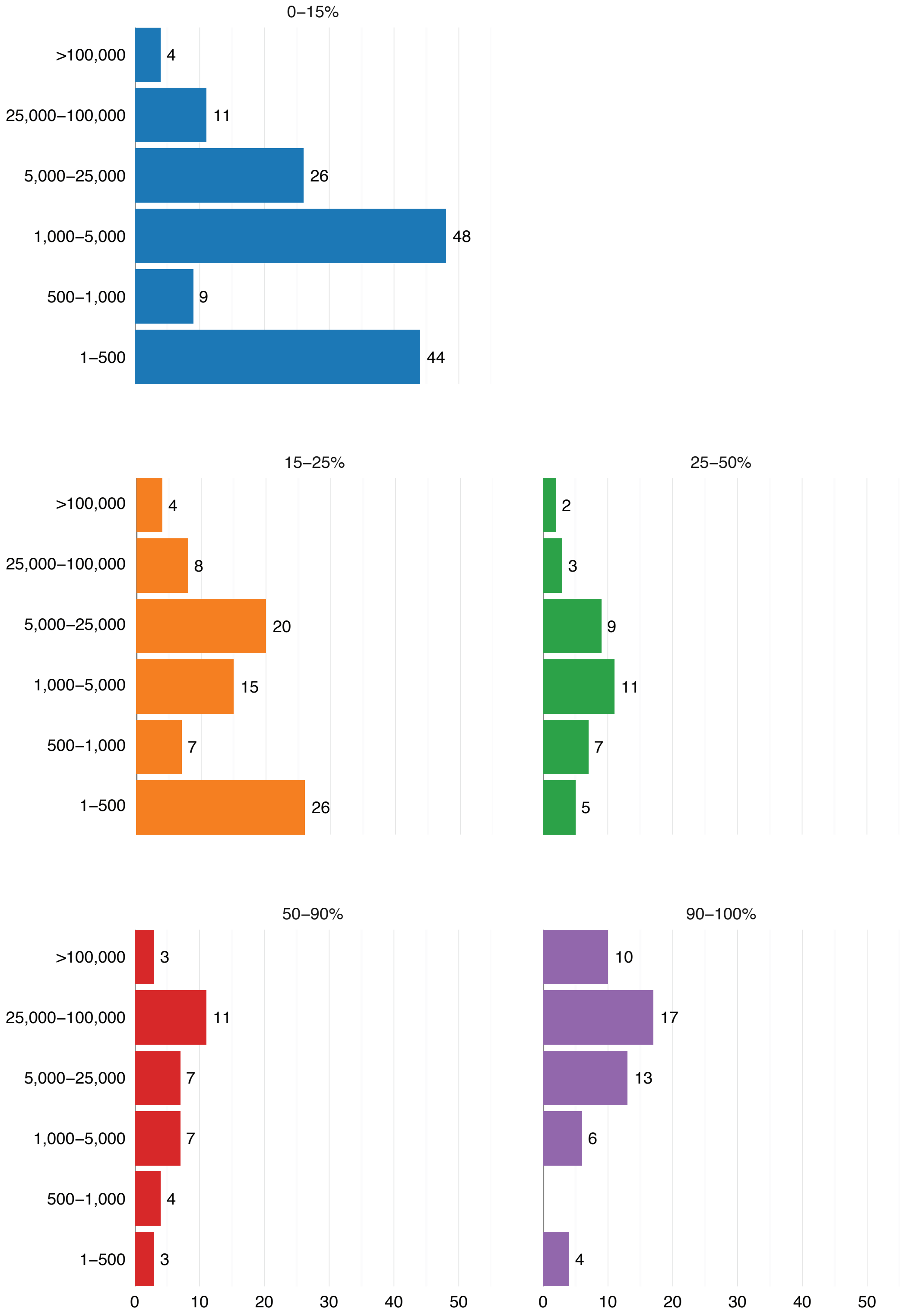
Second, how much time do people spend on their awareness program? Too often, we see people thrown into the position as one of their many responsibilities. Less than 15% of respondents work in awareness full time. While this is an improvement from last year's 10%, over 65% of respondents reported that they spend 25% of their time or less on awareness. A majority of people working on securing the human element are, at best, spending 10 hours a week on it. Imagine how good your organization's security would be if your incident response or network security team spent no more than 10 hours a week at their job.

Time Dedicated to Security Awareness



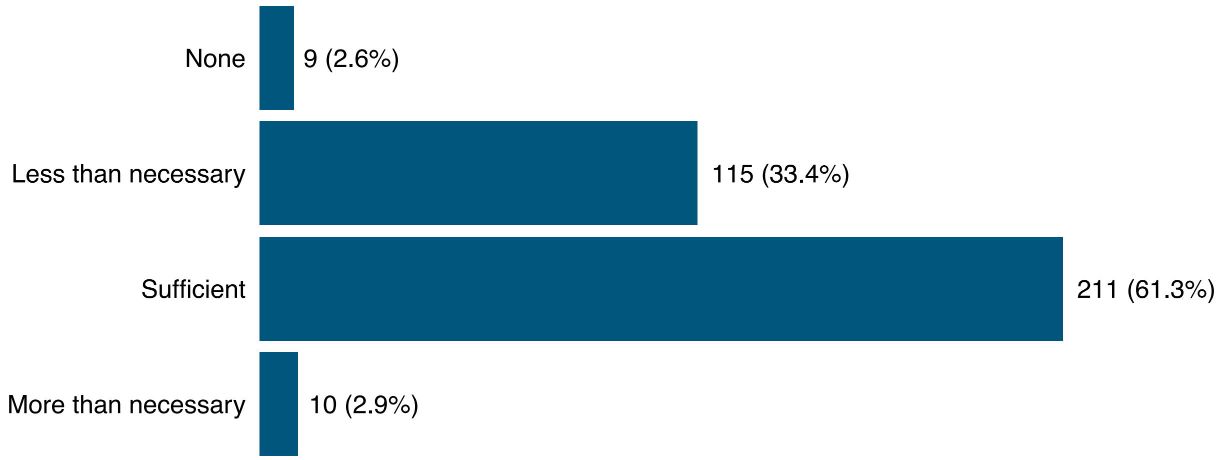
This problem is not limited to small organizations. The number of people who work on security awareness part time is spread throughout organizations of all sizes. Whether that implies that their combined efforts are part time as well is hard to say, but it's safe to say that lots of people are given security awareness as something to do on top of their other jobs and not in a dedicated way.

Time Focused on Awareness by Organization Size



Finally, do awareness programs have the executive support they need? It was encouraging to see over 60% of people reporting they have the support they need. However, over 35% still do not have the support they need to be successful.

Level of Executive Support

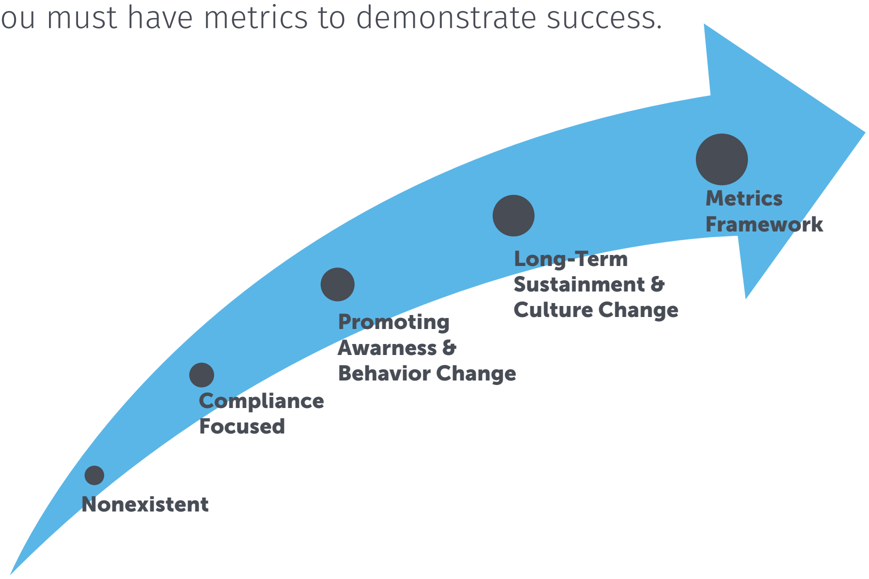


Of the three categories Ingolf identified (resources, time/staff, and executive support), the data showed that support had the greatest impact to a program's success. Research by Grace Kretschmer found a strong relationship demonstrating that the more executive support a security awareness team has, the more mature their security awareness program is. Maturity within the security awareness industry is measured using the Security Awareness Maturity Model.

Established in 2011, this model enables organizations to identify where their security awareness program is currently at, where a qualified leader can take it, and the path to get there. The model is based on five different stages, each stage building on the previous one.

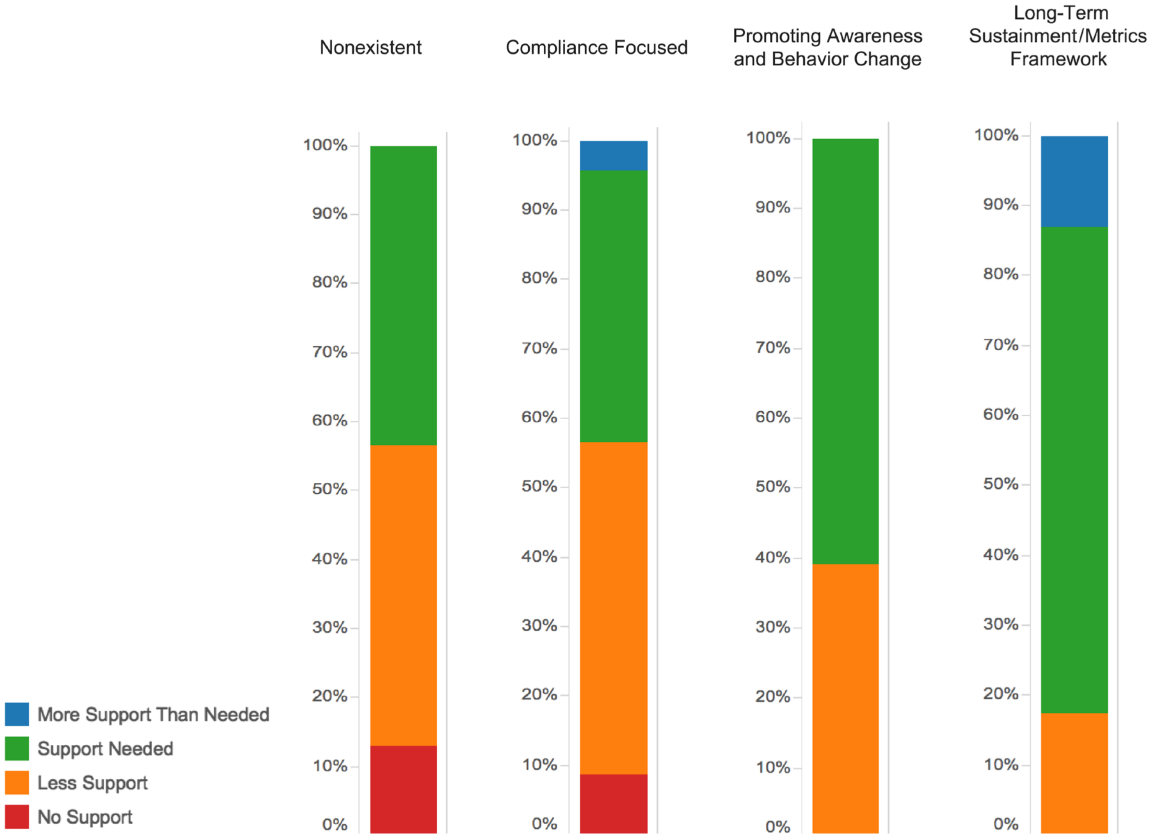
Security Awareness Maturity Model

- **Nonexistent:** Program does not exist. Employees have no idea that they are a target, that their actions have a direct impact to the security of the organization, do not know or understand organization policies, and easily fall victim to attacks.
- **Compliance Focused:** Program is designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad hoc basis. Employees are unsure of organizational policies and/or their role in protecting their organization's information assets.
- **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. Program goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work, home, and while traveling. As a result, people understand and follow organization policies and actively recognize, prevent, and report incidents.
- **Long-Term Sustainment & Culture Change:** Program has the processes, resources, and leadership support in place for a long-term life cycle, including (at a minimum) an annual review and update of the program. As a result, the program is an established part of the organization's culture and is current and engaging.
- **Metrics Framework:** Program has a robust metrics framework to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment. This stage does not imply metrics are not part of every stage (they are). This stage reinforces that to truly have a mature program, you must have metrics to demonstrate success.


Nonexistent
Compliance Focused
Promoting Awarness & Behavior Change
Long-Term Sustainment & Culture Change
Metrics Framework

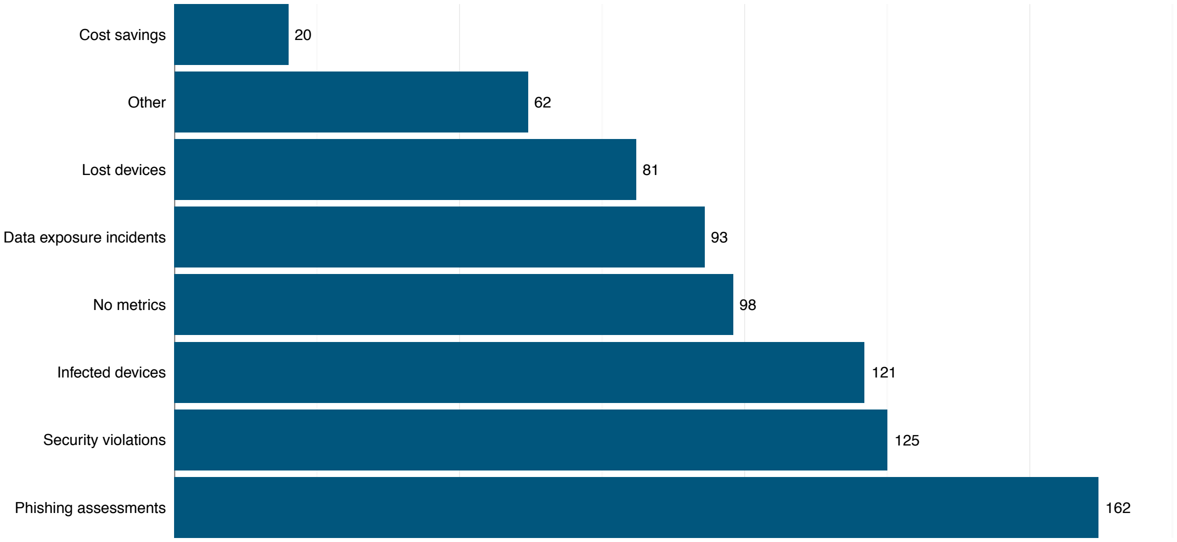
Grace identified that nonexistent maturity programs have the highest concentration of no executive support. In contrast, the two most mature levels (culture change and metrics framework) have zero instances of no support. Executive support has one of the strongest influences on the level of maturity for a security awareness program, as you can see in the graph below.

Mapping of Maturity vs. Executive Support



Finally, we asked what metrics organizations use to measure their awareness program. We believe that one of the key reasons leadership support is lacking for awareness programs is there are too few metrics that demonstrate the human problem and/or the impact awareness has in solving those problems. Not surprisingly, phishing assessments were the top metric. Phishing is not only a common top human risk, but phishing is an effective, quantitative method to measure the risk. However, phishing is just one of many human risks organizations deal with. We need to do a better job of measuring additional human risks and the value of the program to organizations.

Most Common Metrics



Recommendations

Far too often, security awareness programs are an afterthought; someone is randomly assigned the responsibility of awareness without the time, resources, or support they need to be successful. In addition, security awareness can often be just a "checkbox" function for compliance purposes, designed either to meet an audit requirement or to make people acknowledge policies for accountability reasons. We propose three approaches to this problem:

- **Mindset:** People in our industry, from executives on down, often view cybersecurity as purely a technical or IT issue. We need to do a better job educating leadership that cybersecurity is also a human problem. As long as we continue to only invest in technical solutions, we will continue to lose the security battle.

- **Roadmap:** We often find that leadership understands that people's behaviors are a risk to the organization. The problem is when leadership feels that an awareness program is not the solution. Awareness officers need to demonstrate they have a proven roadmap to creating a secure culture, a roadmap based not only on learning theory, behavior modeling, and change management, but also on the lessons learned from others.

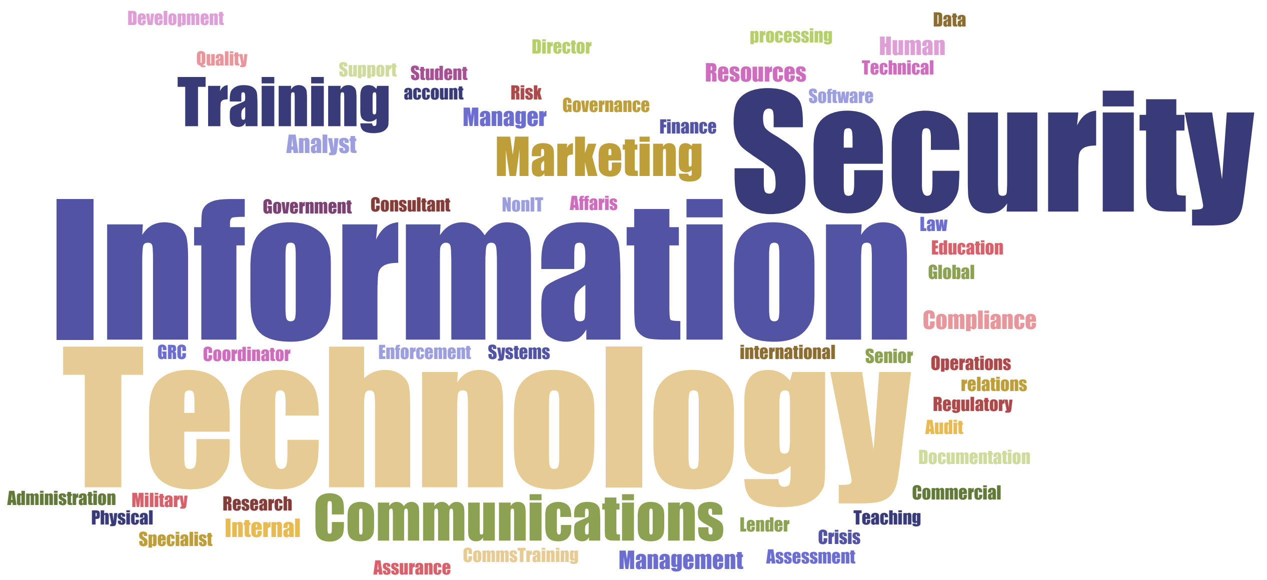
- **Metrics:** It's hard to demonstrate the effectiveness of awareness when you can't measure human risk, nor demonstrate the impact you are having. This is beginning to change as our community develops new ways to measure secure behaviors and cultures. Methods to accomplish this include knowledge assessments, culture surveys, and additional behavioral measurements. Ultimately, stronger metrics are needed to help tell our story and demonstrate the value of awareness.

The Geeks Have Inherited Awareness (Is That Good?)

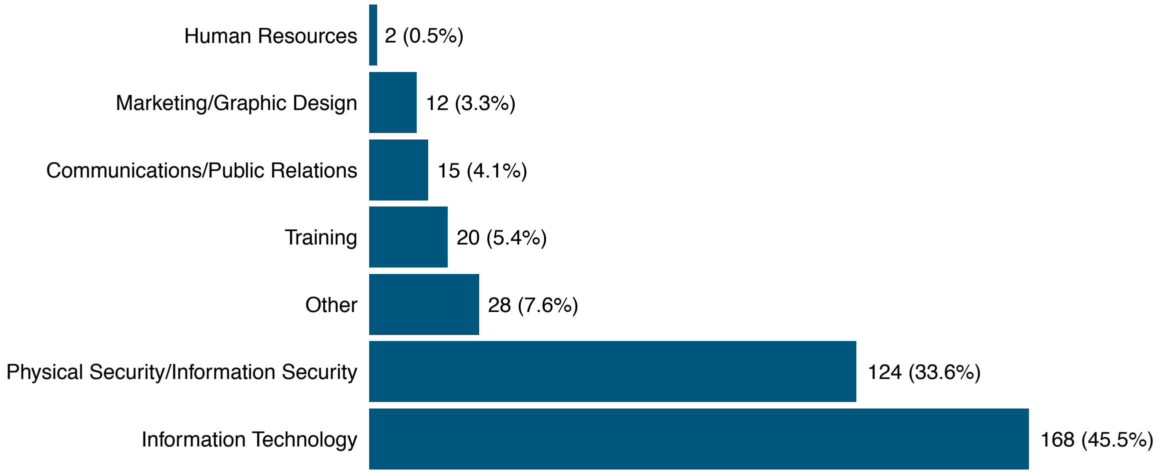
For the tale of our second city, we are seeing that even if an awareness team has the resources they need, many of them are still unable to make the impact they want. Why is this, and what can you do about it? First, we return to the original question, "What is your single biggest challenge?" Ingolf categorized answers into four categories related to not having an impact:

- **Adoption:** Users fail to change their behavior through training.
- **End User Support:** The people supposed to take part in the awareness campaign do not feel it is necessary and are generally unwilling to take part.
- **Finding Time:** End users struggle to find time to take part in awareness campaigns; they are always a low priority.
- **Content:** Participants struggle to create appropriate content.

We begin by evaluating the people leading security awareness programs. Turns out, the vast majority of awareness people are geeks; 79% have a highly technical background, as we can see in the word cloud and bar graph below.



Role Before Becoming Involved in Awareness

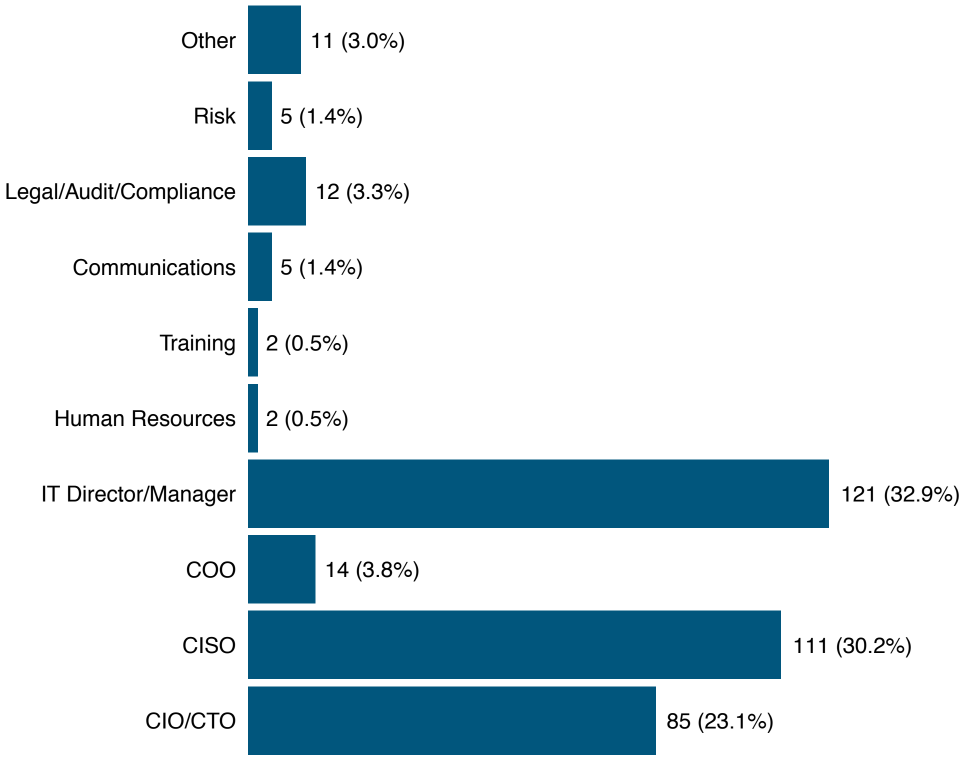


A big part of any security awareness program depends on soft skills, particularly communication. Security awareness practitioners need to explain to people WHY awareness is important to them (so they care) and WHAT to do in simple terms they can understand. And yet the very people communicating these programs often lack fundamental soft skills. In fact, technical people, especially those with a security background, may be the least qualified to communicate awareness, as they suffer from what is called the curse of knowledge.

Curse of knowledge is a cognitive bias. It means that the more of an expert you are at something, the more difficult it is for you to teach or communicate that topic, as you project your knowledge onto your target audience. Security professionals perceive security as simple because security is a part of their daily lives. These same people then assume security must be simple for everyone else in their organization. They then build their awareness program based on these assumptions. As a result, what they communicate is a complete mismatch from what people need, which is something many technical people have a hard time understanding. A common example is passwords. Security professionals are constantly telling people to create and use complex passwords. When people fail to do so, security teams think it must be because people are not motivated, so they spend time on explaining why it's important. In reality, the problem is not motivation, but most people find complex passwords both confusing and difficult. Instead of constantly reminding people it's important, we need to focus on how to make passwords easier, such as explaining passphrases, how to use password managers, or what two-factor authentication is.

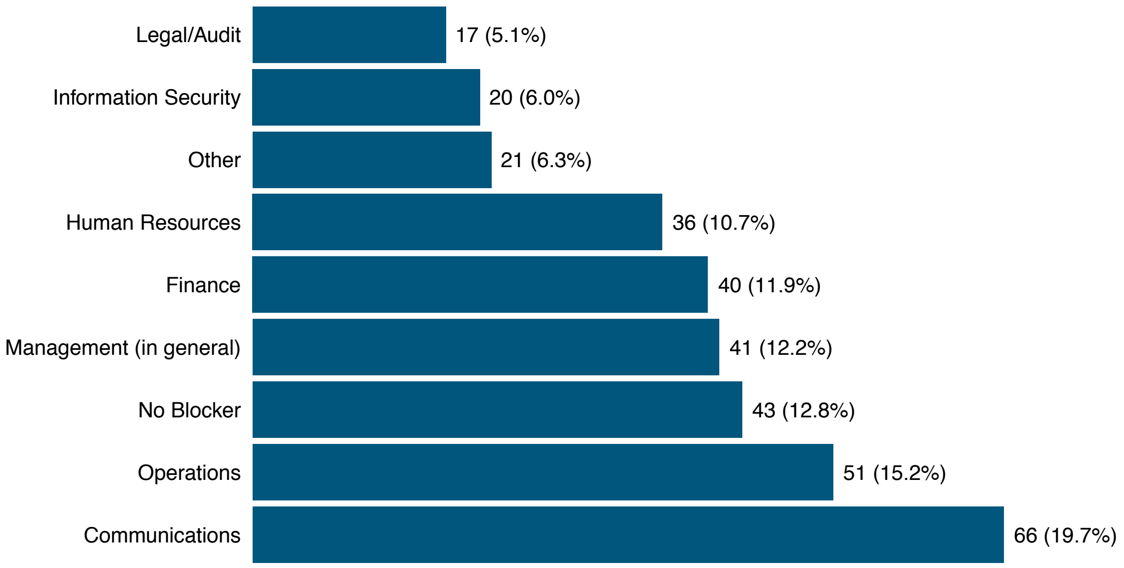
It is especially concerning to see that only 4% of awareness practitioners have a communications background in a position where communication is so critical. In addition to a mismatch of skills, over 90% of awareness programs are tied to and reporting up through technical departments, as seen below.

Reporting To



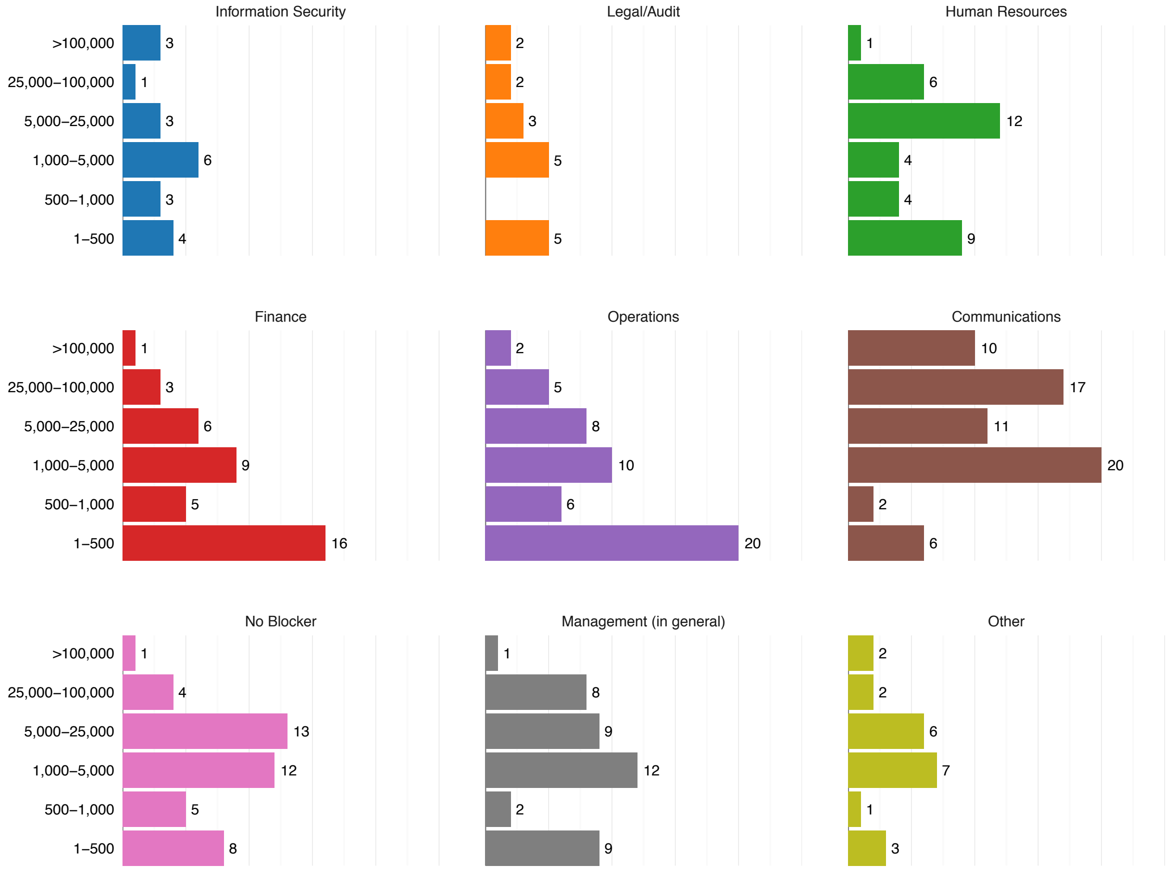
Biggest Blocker

Should security awareness reside here? We do not know. However, if your awareness team is within a technical vertical, you must have good relations with your organization’s communications department. Which leads to the next question: who is your biggest blocker? Communications was identified as the number one blocker in security awareness programs.



Interestingly, communications becomes a larger roadblock as organization size increases, especially for organizations with 1,000 people or more. This can be partially attributed to the fact that smaller organizations often do not have a communications department or policies defining internal communications processes.

Biggest Blocker by Organization Size



So we have highly technical people reporting to a highly technical department whose main job is to communicate to their organization, and yet their communications department is their biggest blocker. Are we beginning to see what could be wrong here, and can we then understand why awareness programs may fail?

Recommendation

Prepare your security awareness team for success. While many security awareness teams know WHAT behaviors need to be changed, most do not know HOW to do that. Begin by ensuring that members of your team have the soft skills they need to be successful, including communications, change management, learning theory, and behavior modeling.

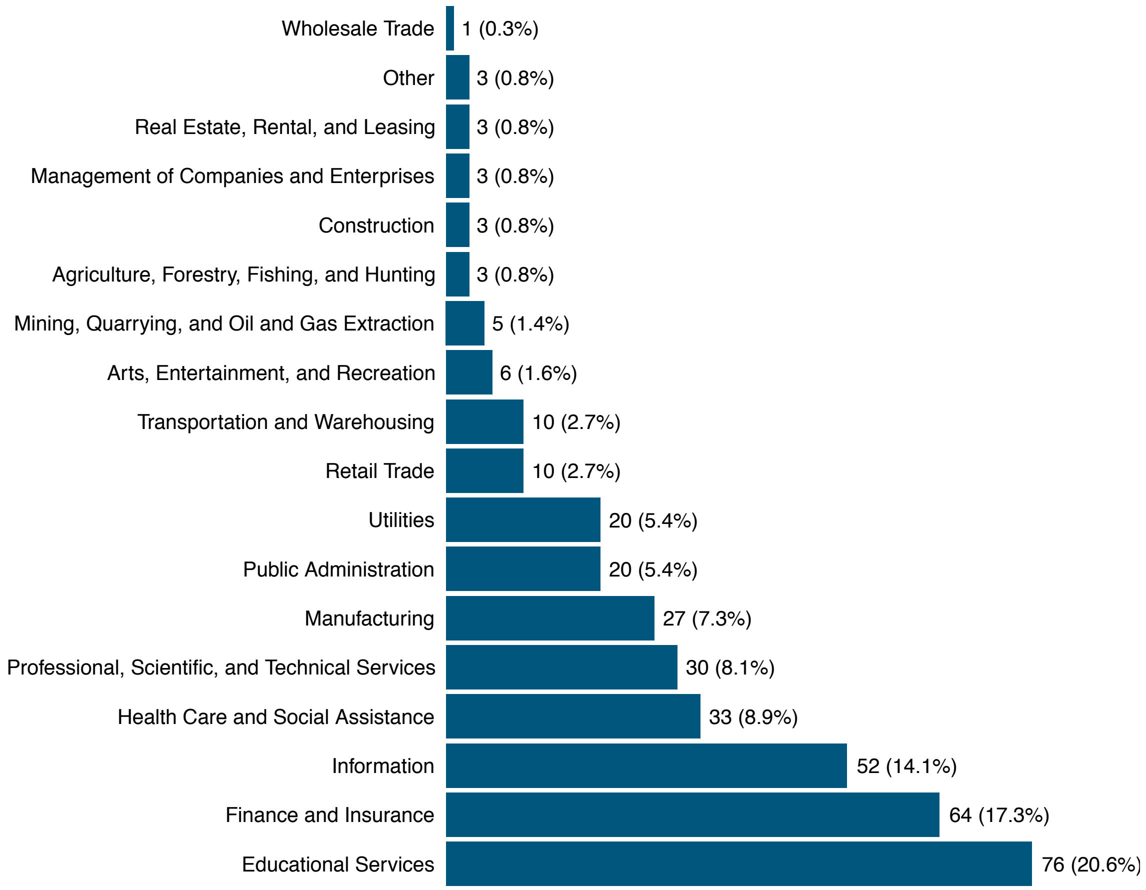
- **Communications:** Our impression is that communications is one of the most critical soft skills. By communications, we mean the ability to engage employees with a meaningful message, identify and deliver the right content to the right people, leveraging multiple communication methods, and building a roadmap that pulls this all together. In fact, we are beginning to see organizations use the title Security Communications Officer. One approach is to embed someone from your communications department into your awareness team. An alternative option is providing your existing awareness personnel the training they need to develop their soft skills, with an initial emphasis on communications. A third option is to contract or hire someone with the soft skills you need. Regardless of the path you choose, as soon as you start planning your awareness program, involve your communications department. The earlier you bring your communications department into the planning process, the more of an enabler they become.

- **Engagement:** Start your program by explaining to people why they should care about security awareness. Instead of rationalizing the need for cybersecurity with statistics and numbers, engage people at an emotional level. Have meaningful conversations and engagements where employees become an active part of the security program instead of just a target of information.

Demographics and Additional Information

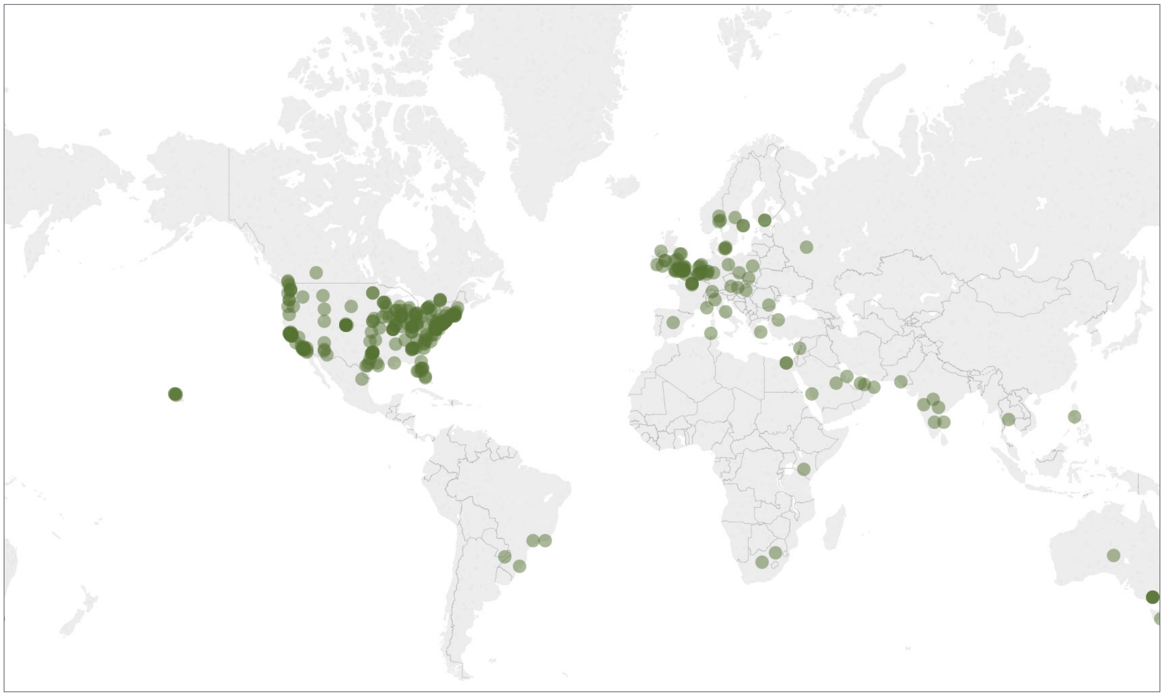
Let's take a look at who took this survey. First, what industries are deploying awareness programs? As the survey data only covers two years, we are not sure if our data is a good representation of which industries are adopting awareness or if this represents whom we are reaching with our survey. For now, our best guess is it's a little bit of both. This year's biggest difference is the high number of Educational respondents (20.6%). This year, we reached out to not only the security community about the survey, but also to specific industries, including the education community through EDUCAUSE. EDUCAUSE is an IT association specific to the education community. So the graph below does not so much imply that universities have the highest percentage of awareness programs, but that EDUCAUSE helped promote the survey within the education community. Next year, we intend to broaden the survey even further, including distribution through other industries and sectors.

Respondents by Industry



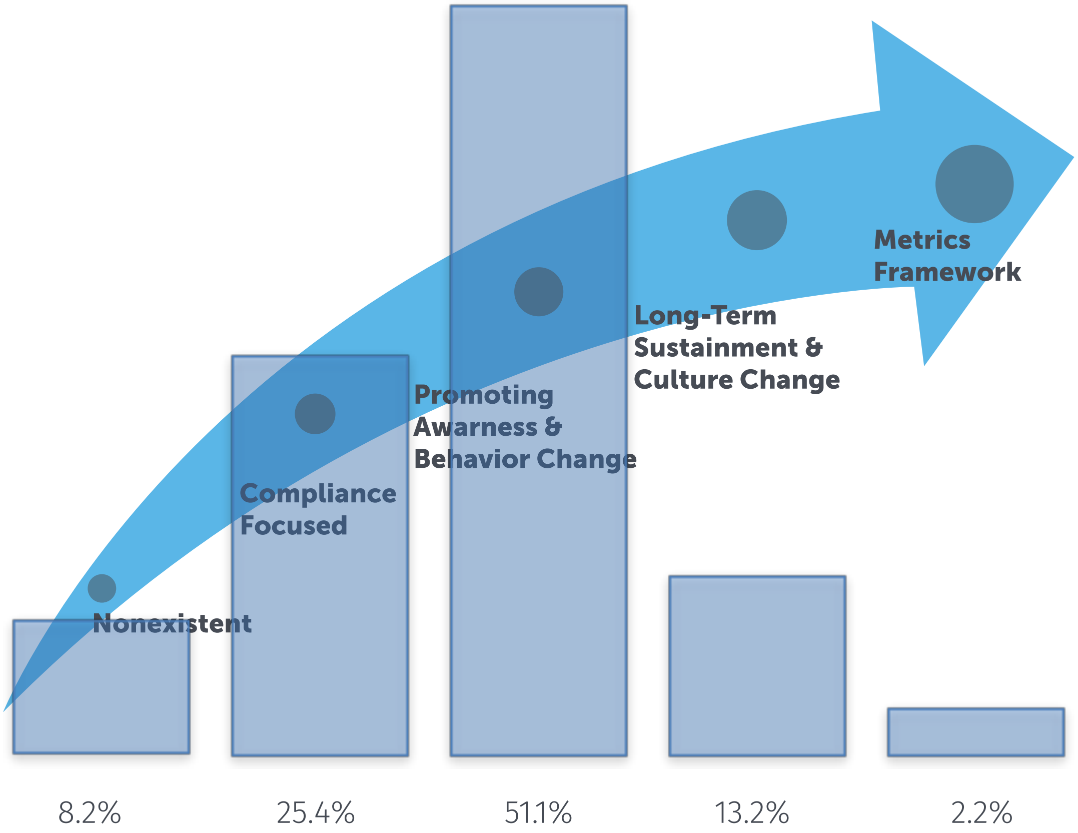
In addition to industries and sectors, we want to know how global the survey is. Last year, the vast number of respondents were U.S.-based organizations. This year, we improved our global reach, with 70% of respondents being in the United States and 30% being outside the United States. Just like industries, our goal next year is to reach a broader and more global community.

Respondents by Country



Finally, how mature is the average security awareness program? As we discussed earlier, we define maturity by the Security Awareness Maturity Model. 33% of organizations are just now starting their awareness program or are still focused on just compliance. 51% have an awareness program that is starting to change behavior. This is a definite improvement from last year, when only 39% of awareness programs were changing behaviors. Only 2% of organizations are truly mature, as they are changing both behavior and culture and have the metrics to prove it.

Maturity Level of Security Awareness Programs



The data shows awareness programs are maturing from last year, but there is still a long way to go. The challenge for many organizations will be moving beyond securing behaviors and instead creating an enduring, secure culture, and having the metrics to demonstrate it.

Conclusion

While security awareness is still in its infancy, signs of maturity are emerging. Organizations appear to be receiving slightly more support than last year, and there has been an improvement in the average maturity level. In addition, we are beginning to have a better understanding of what our top challenges are and how to best address them. Ultimately, security awareness is hard. To recap the key takeaway points:

- **SUPPORT IS ESSENTIAL:** Security awareness teams are not getting the support they need to be successful. Over 50% of awareness personnel surveyed have a budget of $5,000 or less or don't know what their budget is. Less than 15% of awareness personnel are dedicated full-time to their job. While this is an improvement from last year's 10%, we are concerned that is still too low. In fact, 64% of people reported spending less than a quarter of their time on awareness. Finally, 35% report not having the executive support they need. Why is all of this important? Because the data shows a strong relationship between the amount of support you have and the maturity of your security awareness program. We need to do a better job of educating leadership that security cannot be solved by technology alone; it must also address the human factor. Key steps to achieving this include demonstrating to leadership that you have a proven roadmap to creating a secure culture and the metrics to show leadership the impact your program is having.

- **SOFT SKILLS ARE LACKING:** Last year, we reported that soft skills are lacking in security awareness personnel. By soft skills, we mean skills such as communications, change management, learning theory, or human behavior. The data told the same story this year, over 80% of security awareness personnel have a technical background, with skills such as debugging network traffic, building websites, or securing a server. However, this also means that many security awareness teams don't understand the proven concepts and techniques in changing behavior and culture. In addition, we identified communications as one of the key soft skills lacking. By communications, we mean engaging employees with a meaningful message, delivering the right content to the right people, leveraging multiple communication methods, and building a roadmap that pulls this all together. One successful approach is embedding someone from your communications department into your security team. A second option is to train your awareness team on the new skills they will need. A third option is to contract or hire someone with strong soft skills. Long story short, you not only need security expertise on your awareness team, but you need soft skills, starting with communications.

A Big Thanks

We would like to take a moment and thank our volunteers who made this happen. Collecting data is relatively easy. Sifting through all the data and creating a report that people can actually use is HARD. So a big shout-out to the following:

Bob Rudis: Chief Data Scientist, Rapid 7

Bob Rudis has over 20 years of experience using data to help defend global Fortune 100 companies and is currently [Master] Chief Security Data Scientist at Rapid7. He was formerly a Security Data Scientist & Managing Principal at Verizon, overseeing the team that produces the annual Data Breach Investigations Report. Bob is a serial tweeter (@hrbrmstr), avid blogger (rud.is), author (Data-Driven Security), speaker, and regular contributor to the open source community (github.com/hrbrmstr). He currently serves on the board of directors for the Society of Information Risk Analysts, is on the editorial board of the SANS Securing The Human program, and was co-chair of the 2014 Metricon security metrics/analytics conference. He was chosen as one of SANS's "People Who Made a Difference in Security in 2015" and holds a bachelor's degree in computer science from the University of Scranton.

Lance Hayden: PhD Managing Director - Security Culture Practice, Berkeley Research Group

Dr. Lance Hayden has over 25 years of experience in information security, beginning as a HUMINT operations officer with the CIA. Since then, he has focused on helping organizations measure and improve security strategy, culture, and behavior. He is the author of the books "IT Security Metrics" and "People-Centric Security: Transforming Your Enterprise Security Culture" and regularly contributes to conferences and security publications. He lives and works in Austin.

Grace Kretschmer: MSIS Candidate at the University of Texas, School of Information

Grace Kretschmer will complete her master's in information studies at the University of Texas at Austin in May. In her program, she has focused her studies on data analysis and human-computer interaction. She is specifically interested in how data analysis can improve the functionality and effectiveness of security awareness programs.

Angela Sasse: Professor of Human-Centred Security in the Department of Computer Science at University College London

Since 1996, Prof. Sasse has been researching usability issues of security systems, and published research on effectiveness and usability of authentication mechanisms, access control mechanisms, user attitudes and perceptions to computer security, and human and financial cost of security mechanisms. She chairs the Cybersecurity KTN on Human Vulnerabilities in Security Systems and teaches a master's-level course at UCL, Oxford University, and the Defence Academy. Angela was elected a Fellow of the Royal Academy of Engineering in 2015.

Ingolf Becker: PhD Student, University College of London

Ingolf graduated in Mathematics from Imperial College London before switching to Computer Science at UCL. He is currently studying for his PhD with Angela Sasse and Sebastian Riedel. His research interests focus on usable security in organizations, machine reading, and banking security. As part of UCL SECReT, Ingolf is particularly interested in interdisciplinary research.

Jon Homer: CyberSecurity Data Analyst

Jonathan Homer, CISSP®, is a specialized cybersecurity analyst with a business background. He has over 15 years of experience presenting in the boardroom and on the speaking circuit. With a background in both technical and human performance, Jon has supported numerous departments of the U.S. Federal Government during his career. He is well known for his communication skills and is the author of the nationally renowned "Who's In Your PC?" security awareness campaign, the comedic "Murder at INL" educational activity, and the "Neutron Works" end user utilization initiative.

About SANS Securing The Human

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 Securing The Human, 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 Securing The Human 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 cybersecurity experts. Organizations trust that SANS Securing The Human content and training is world class and ready for a global audience. The SANS Securing The Human 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 the 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 Securing The Human's unwavering commitment to helping organizations effectively understand, manage, and measure their human cyber risks. To learn more, visit https://securingthehuman.sans.org.

securingthehuman.sans.org