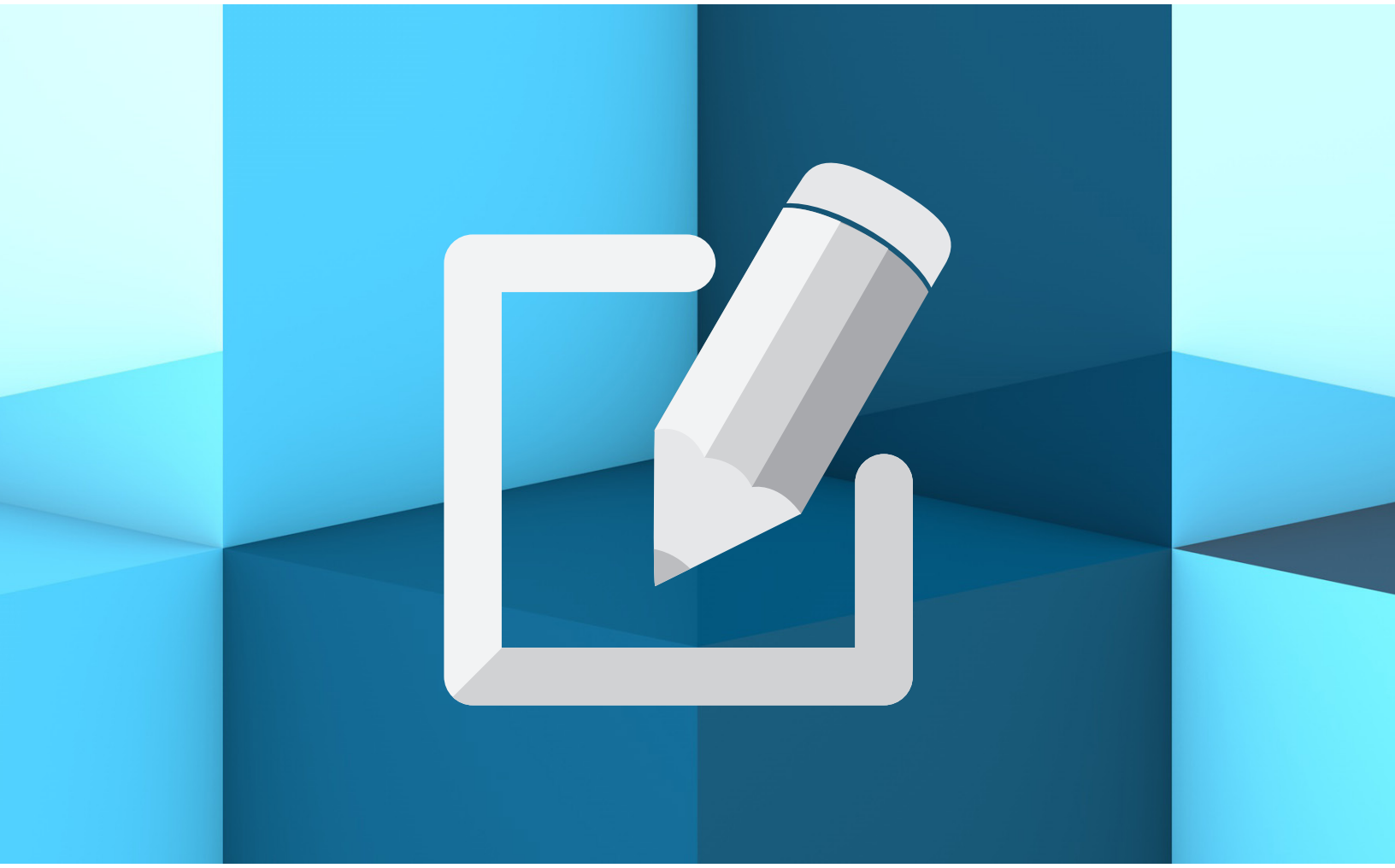
SANS Securing The Human

2015 Security Awareness Report



Executive Summary

The SANS Securing The Human 2015 Security Awareness survey uncovered three key findings, all of them related:

1. **SUPPORT IS ESSENTIAL**: We found a direct correlation: the more time and resources security awareness officers have, the more mature their program is. Unfortunately, only 5% of the respondents work on their security awareness program full time. In addition, the vast majority of security awareness budgets are under $10,000. It is clear that security awareness programs will continue to fail until they get the same emphasis and support as technical controls. To address this, we have to better educate senior leadership that cyber security is far more than just bits and bytes; it also includes the human element.

2. **SOFT SKILLS ARE LACKING**: More than 75% of the awareness programs surveyed are run by people with highly technical backgrounds, such as IT admins or security analysts, but with little experience in softer skills, such as communications, change management, learning theory or human behavior. In addition, people limited to just technical backgrounds may be prone to view security strictly through a technical lens, while failing to account for the human factor. Organizations need to invest in and train their security awareness officers on the softer skills required for any security awareness program, or provide them access to the people who can deliver those diverse skills. In addition, we found that most security awareness programs lie somewhere in an information technology-centric chain. The question becomes, is this where security awareness programs should be?

3. **SECURITY AWARENESS IS STILL IN ITS INFANCY**: Using the Security Awareness Maturity Model, we found that half of the organizations surveyed currently do not have an awareness program or have an immature program that is solely focused on compliance. Only 5% of respondents felt that they had a highly mature awareness program that not only was actively changing behavior and culture, but also had the metrics to prove it. In addition, we found that one of the top challenges organizations face in 2015 is making people aware they are targets. This implies that we are still in the beginning stages of creating secure cultures. If we are going to effectively change behavior, employees must feel a sense of urgency and understand not only that they are targets, but that their actions play a key role in securing the organization.

While 225 people responded to the questionnaire, the results in this report are based, unless otherwise specified, on the responses of the 187 people who answered all the questions.

About This Survey

Welcome to the first SANS Securing The Human Security Awareness Report. The purpose of this report is to help people better understand how organizations are mitigating the information-related risks that arise from human behaviors and the challenges they face in accomplishing that. Ultimately, our goal is to enable security awareness officers to make more informed decisions and benchmark their programs to other organizations in their industry. To accomplish this, we conducted a survey in October 2014, which was National Cyber Security Awareness Month. This report is based on the findings from that survey.

Before we continue with the findings, we would like to take a moment to recognize the amazing efforts of some very smart and hard-working volunteers who made this possible. First, we would like to thank Lance Hayden of Cisco Systems for his help in creating the original survey. Second, we would like to give a big thanks to Bob Rudis and the Verizon DBIR team, who did the heavy lifting in analyzing the survey results and making this report possible. Finally, we would like to thank our community reviewers, including but not limited to the following people:

James Gannon – Cyber Invasion
Kevin Alston – Genworth
Stephen Burke – Cyber Risk Aware
Rhonda Kelly – Oshkosh
Tonia Dudley – Charles Schwab
Matt Beland – Davis Wright Tremaine LLP
Andrew Richter – Cisco Systems
Tim Harwood – HS and TC

We intend to create this report every year and develop it as a community resource. If you have any feedback, questions or suggestions on this report or on how to improve it for next year, please reach out to us at community@securingthehuman.org. We are especially interested in knowing what questions you want asked—what do you want to know that will help you?

With that said, let's get started.

Demographics

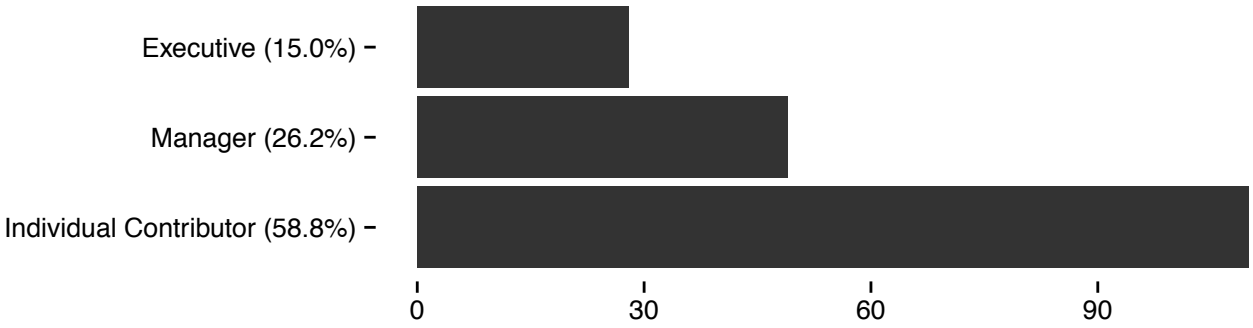
One of our initial goals was to establish demographics. We wanted to gain a better understanding of who is involved in running security awareness programs.

What Is Your Title?

To better understand who is running awareness programs, we asked for respondents' titles, to be provided in a free-form text field. Not surprisingly, the titles were very diverse. The word that appeared most often was security, followed by information. Responsibility for security awareness seems to be heavily rooted in information technology/information security roles, though there were a few compliance and project management roles in the mix, along with human resources and training roles. Surprisingly, in some cases, security awareness officers were system administrators, IT administrators and webmasters.

In addition, we mapped the titles to three levels, Individual Contributor, Manager and Executive, to make it easier to analyze the results. Those falling into the category of Individual Contributor were most often in IT and had titles such as “analyst,” “specialist,” “administrator” and “engineer,” with their level often indicated by such appendages as “senior” and “junior.” Those aligned to the Manager category were, for the most part, “managers,” but that category also included lower-level “directors.” There were, quite a few “training managers” and many “directors of information security” in that mix, too. Executives included “CISOs,” “CIOs” and anyone “VP” level or higher, but mainly consisted of “CISOs.” Interestingly, in the vast majority of cases, individual contributors are responsible for security awareness functions.

Who Is Responsible for Security Awareness?



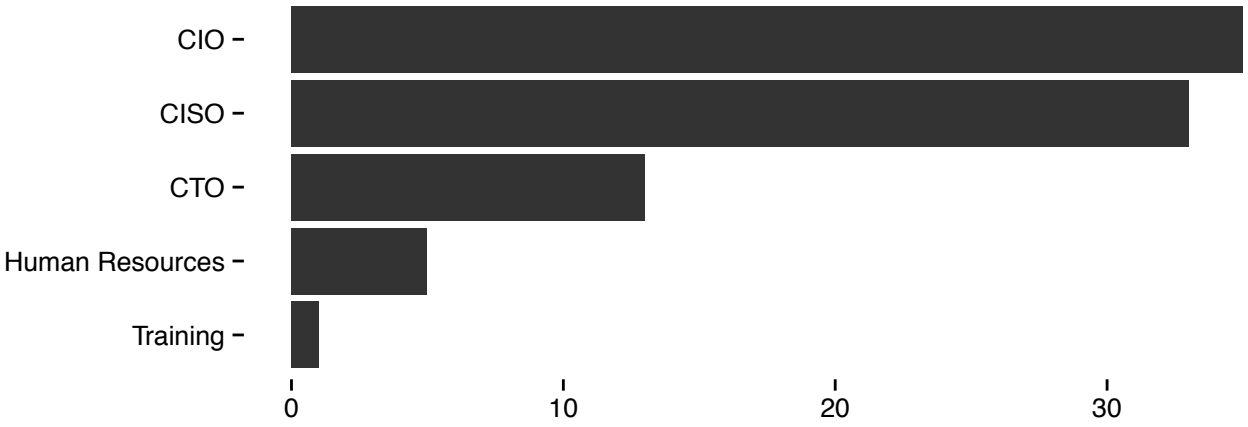
NOTE: Unless otherwise stated, for all graphs in this report, the numbers along the bottom (X) axis are the number of survey responses.

Who Is Your Boss?

Our second question was whom respondents report to. We offered six options, including "Other." Surprisingly, less than 5% reported to human resources or training. It is clear from both the titles of security awareness officers and their reporting structure that security awareness in most organizations falls within the purview of information technology.

But is this where a security awareness program belongs? Since security awareness is designed to address human issues, organizations may want to consider placing their program where the strongest human skills lie, such as change management or training. If you elect to keep your security awareness program under IT or security, ensure that your program maintains close working relationships with other departments, including communications, training, human resources and the project management office. Where we are seeing security awareness programs fail is not so much with the content, but how that content is being designed and communicated.

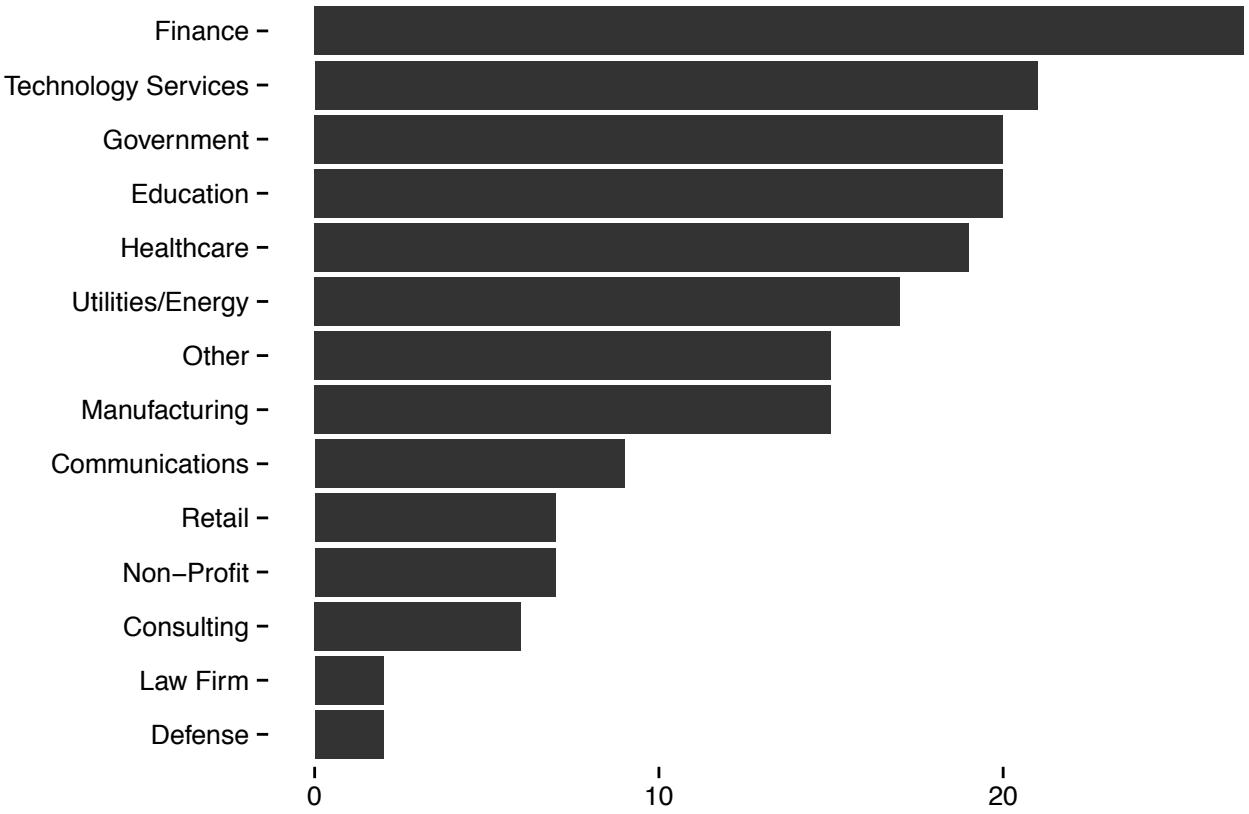
Whom Do You Report To?



Industry View

Finance, technology, government and education were the top industries represented in this survey.

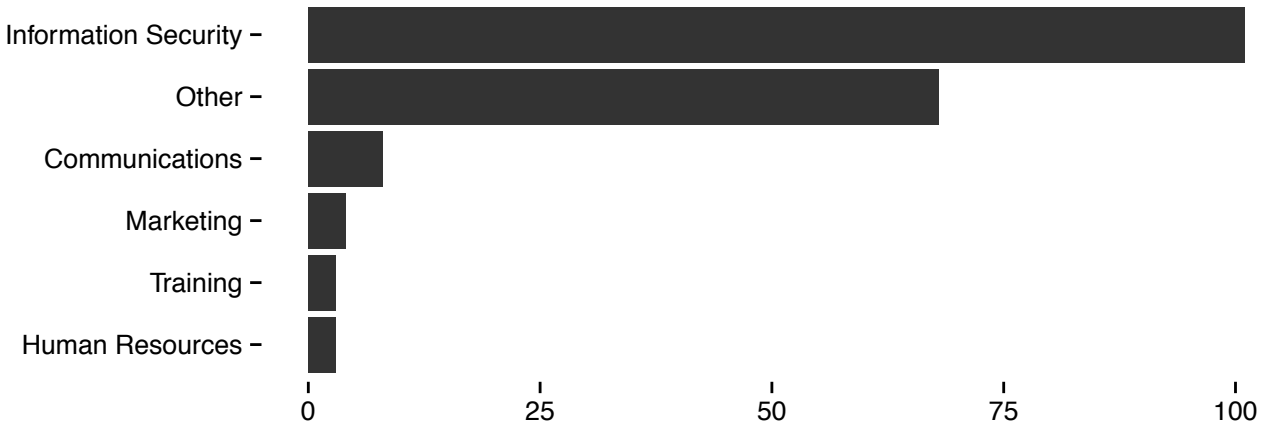
What Industry Is Your Organization In?



What Is Your Background?

We were especially interested in learning about the backgrounds of today's security awareness officers. What skills and experience do they bring to the organization, and what might they be lacking? In line with other findings, the vast majority of respondents had highly technical backgrounds in information technology or information security.

What Was Your Job Role Before You Became Involved in Security Awareness?



What's more, the "Other" category was dominated by information technology roles, such as IT admin. This preponderance of IT experience is a concern. As we discussed earlier, successful security awareness programs depend heavily on softer skills, such as communication, training theory, marketing, project management and an understanding of human behavior. People limited to technical backgrounds often lack these softer skills and are prone to view security strictly through a technical lens, while failing to account for the human factor. Organizations may be selecting the wrong people to run their programs, or not providing these people with the additional training they require.

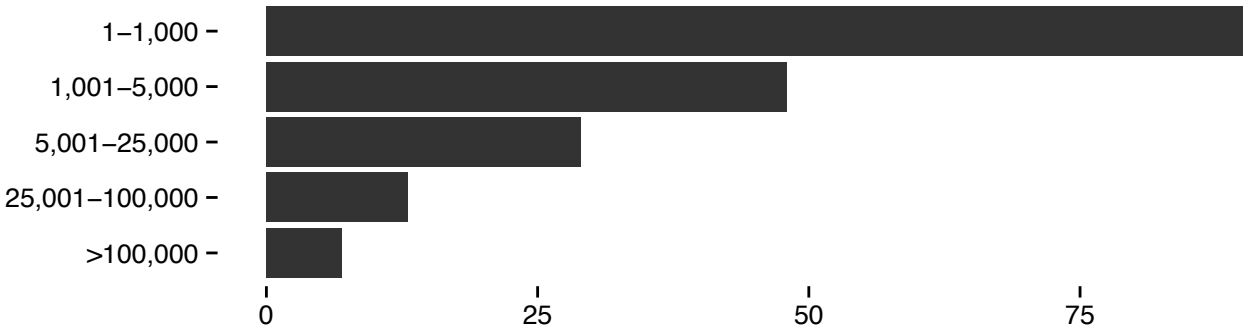
Organizations need to train their security awareness officers in all the skills that an effective security awareness program requires. If nothing else, the security awareness officer needs to identify who else within their organization has the required, softer skills and can help establish an effective security awareness program.

Scope & Resources

Call Out the Troops

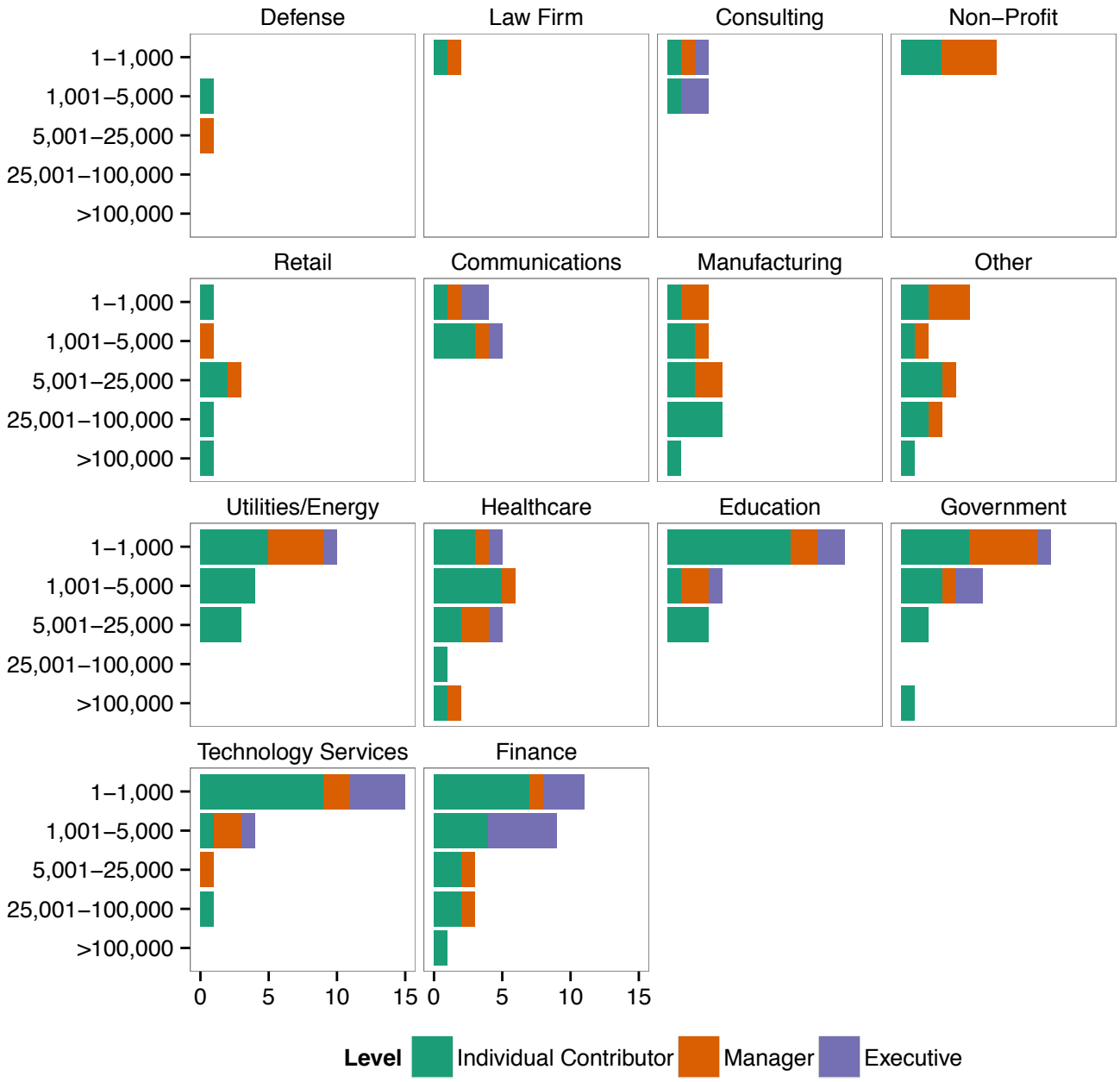
Next, we wanted to know the scope of respondents' programs. The job of presenting compelling awareness messages becomes more complex and demanding as the number of employees and contractors to be trained increases. By far, most of the respondents are responsible for training 5,000 or fewer people.

How Many People Are Responsible for Training in Your Security Awareness Program?



The next set of charts looks at organizations by size and industry and shows the level of management that is responsible for security. Interestingly, the more employees an organization has, the more likely it is that the person with responsibility for security awareness is at the lower level of Individual Contributor. While at first this may seem counterintuitive, there may be an explanation for this. In smaller organizations, managers often take on multiple roles. As a result, while smaller organizations may have more senior people running their awareness programs, these individuals are more likely to be multitasking and have less time to focus on awareness. In larger organizations, Individual Contributors may be dedicating a larger percentage of their time to their program, which can result in a more effective program.

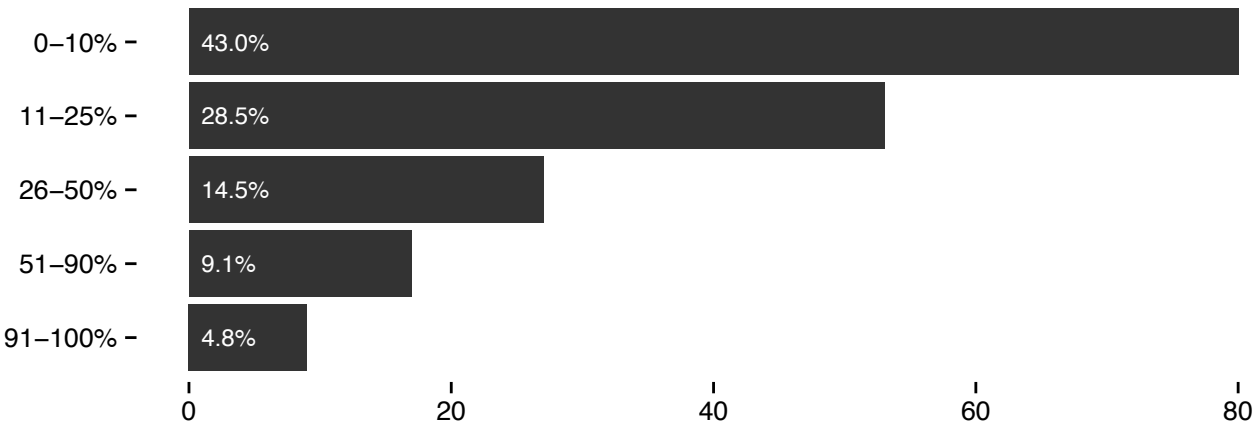
Worker Count by Industry and Officer Level



Time Spent on Security Awareness

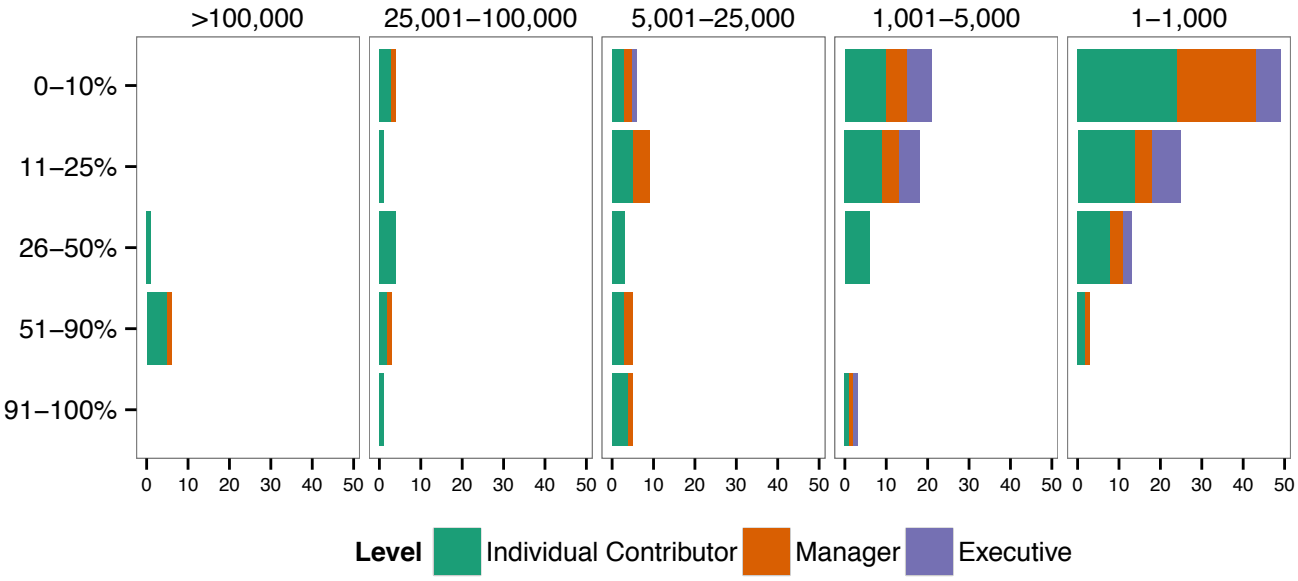
We feel that one of the strongest indicators of a mature security awareness program is how much of an individual's time is dedicated to running it. Unfortunately, only 4.8% of respondents seem to have security awareness as a full-time job.

What Percentage of Your Time Is Focused on Security Awareness?



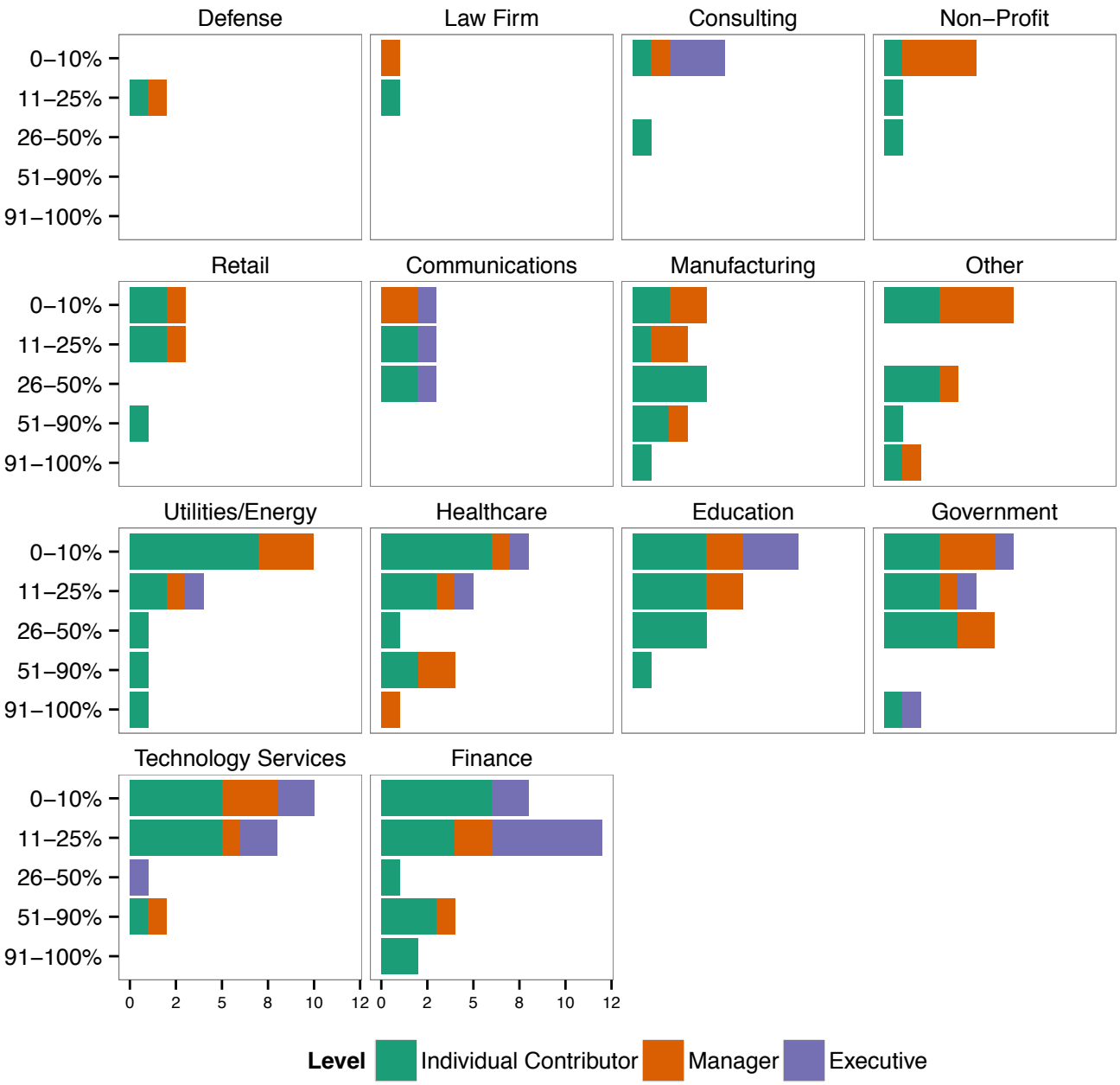
If we look at the time spent by both level and organization size, we see that respondents in mid-sized to larger organizations dedicate more time to their security awareness role than smaller organizations.

Time Spent by Level and Organization Size



And the industry they're in tends to influence how much time security awareness officers spend on awareness. Not surprisingly, those organizations that are the most risk-adverse or the most heavily regulated, such as finance, healthcare and government, had the most resources dedicated to their awareness programs.

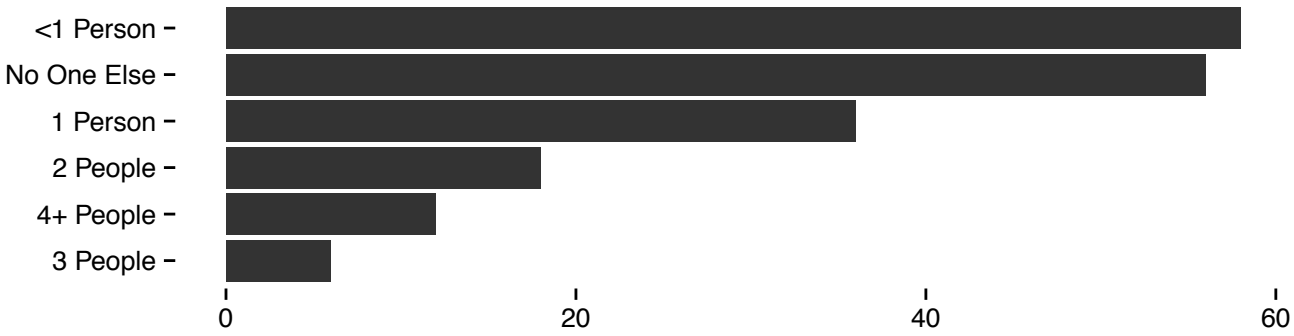
Time Spent by Level and Industry



Helping Hands

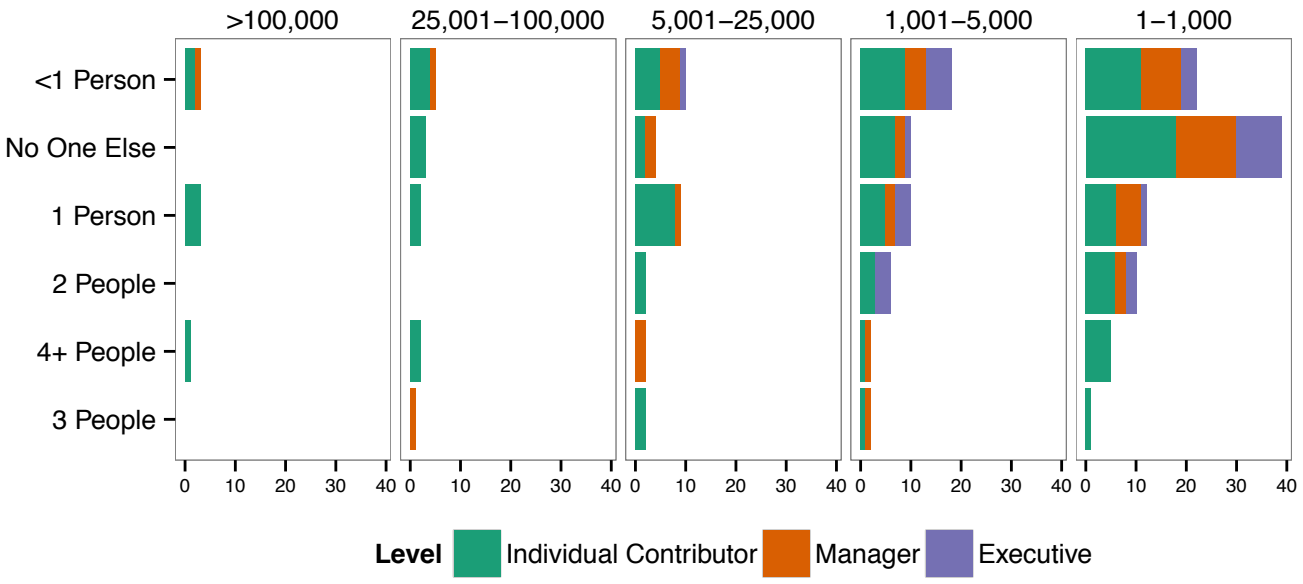
We also wanted to know whether security awareness officers had anyone helping them. Most had either no help at all or less than one full-time helper, which seems less than ideal. We would like to see awareness officers getting more support.

Do You Have Anyone Else Helping You Build and Maintain Your Security Awareness Program?



Looking at the helping hands by organization size, you can see that larger organizations (though more sparsely represented in the survey population) do not provide nearly as many human resources as the mid-tier organizations. The higher up on the food chain the awareness officer is does have some impact on the staffing support for the program. Finally, it's not too surprising that smaller organizations put the responsibility on one individual.

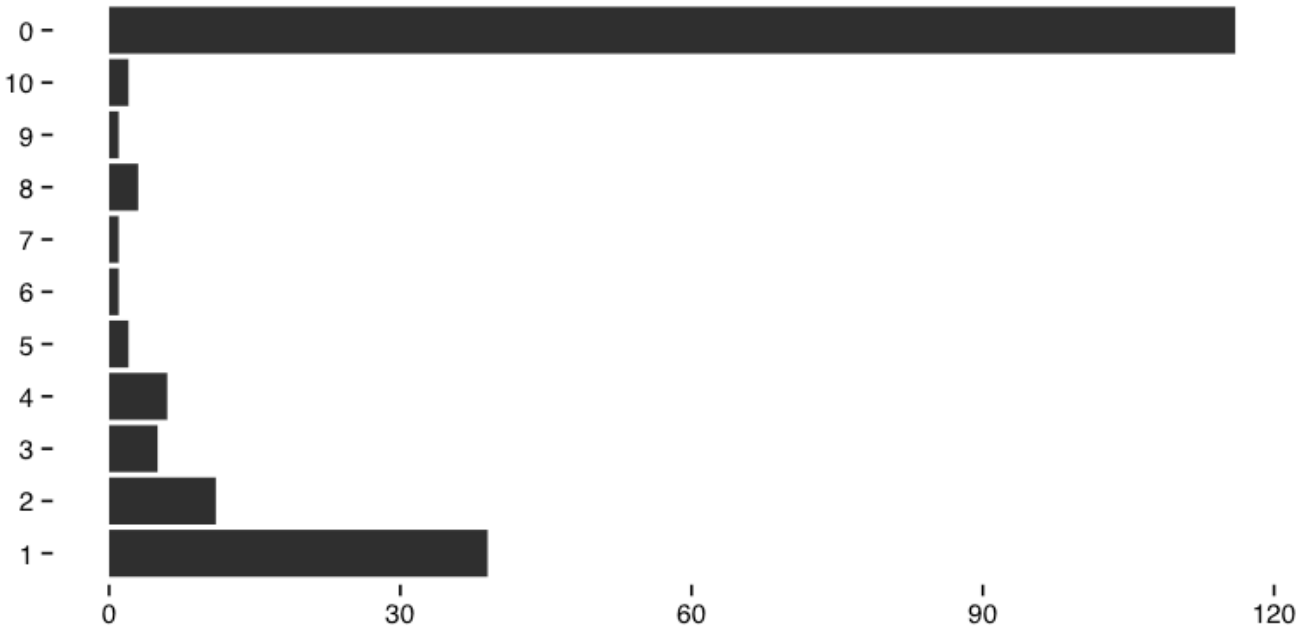
Helpers by Organization Size



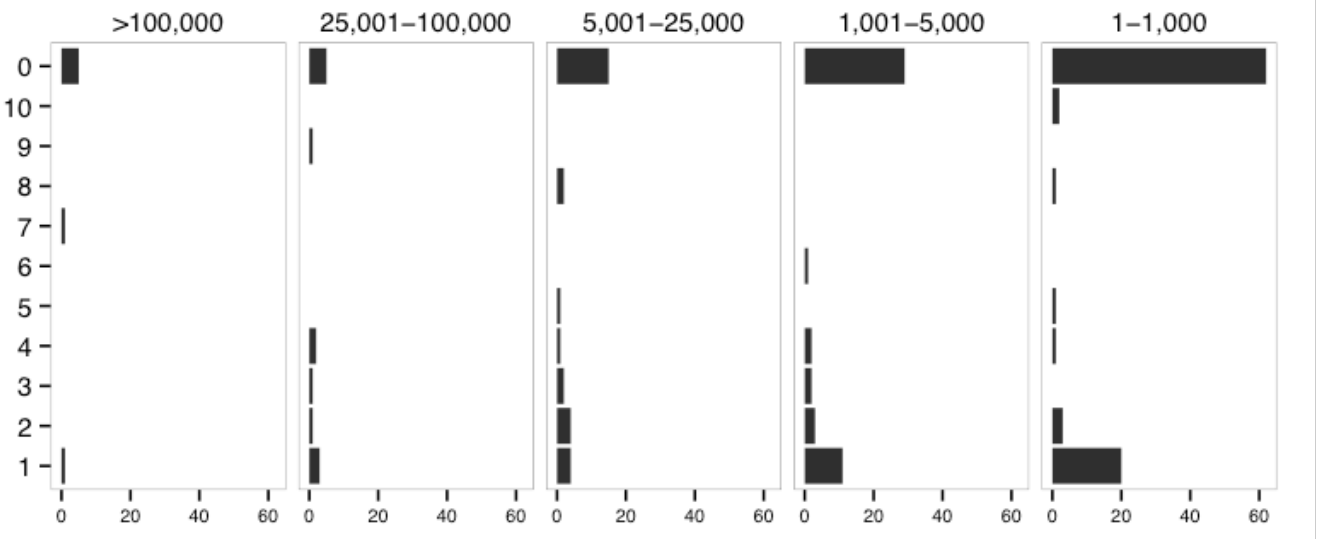
Lost in Translation

The vast majority of respondents did not translate their awareness materials into additional languages.

How Many Languages Do You Translate Your Security Awareness Program Into?



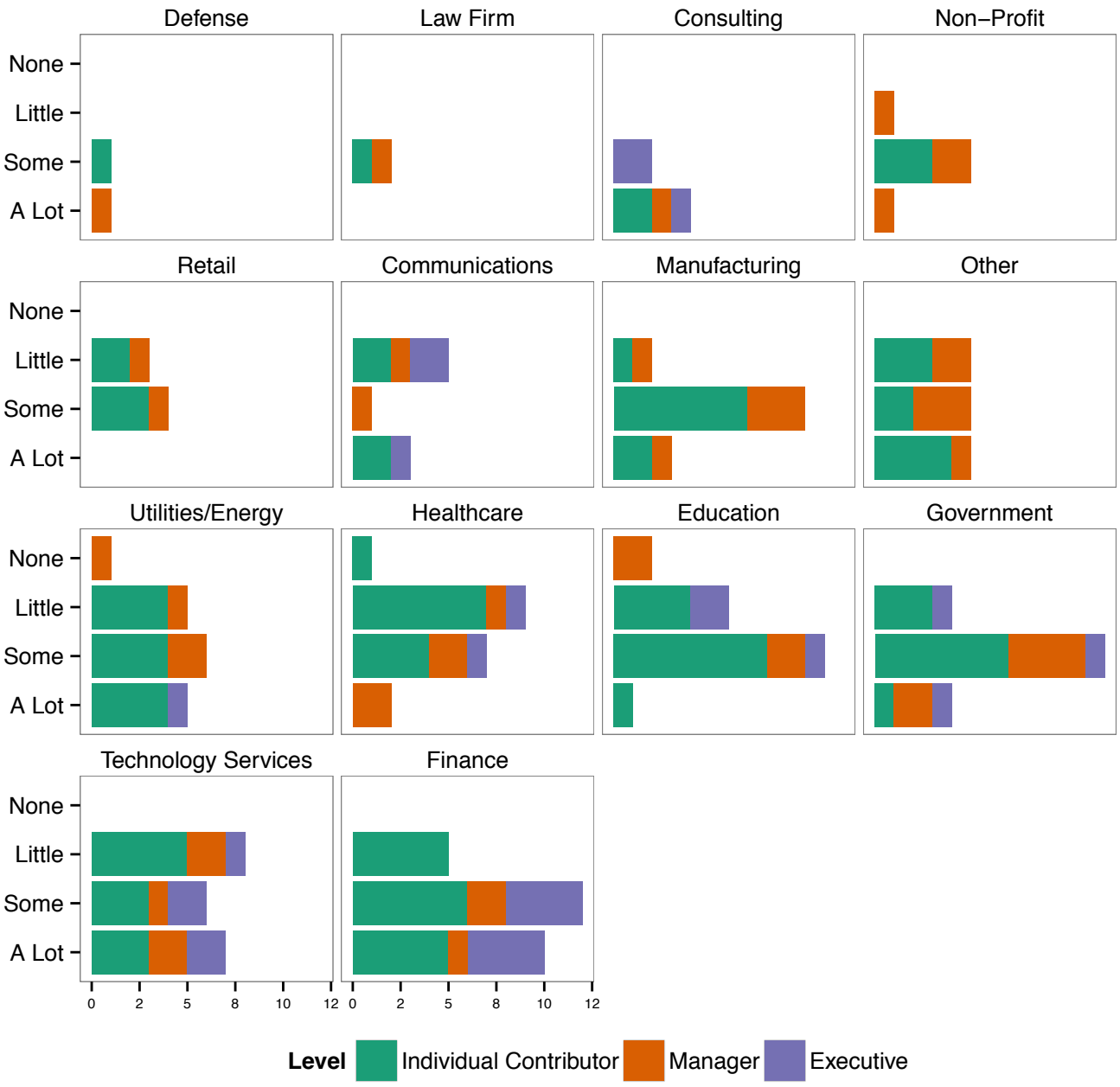
However, organization size does play a role in whether or not materials are translated, most likely due to the fact that larger companies tend to have a more diverse or global workforce.



Budgets and Executive Support

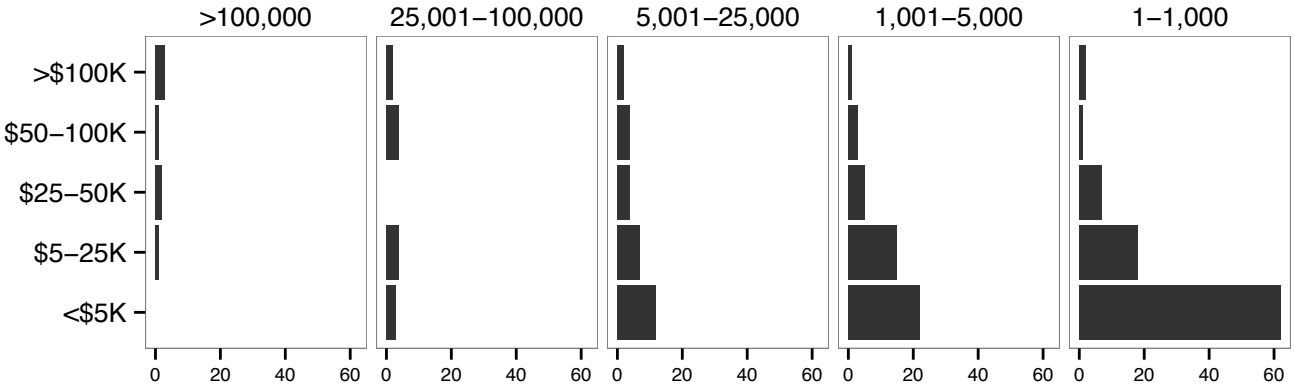
We are happy to say that 25% of respondents reported getting a lot of executive support for their security awareness programs. But that leaves over 75% of respondents potentially not getting the full support they need, with 5% saying they get no support at all. By industry sector, respondents in finance, government and education were more likely to say they enjoyed good support, while those in law firms and retail tended to be the weakest.

How Much Executive Support Do You Feel You Have (by Level and Industry)?



Support can also be measured in cold, hard cash. Overwhelmingly, the budgets for awareness are under $5,000. Some large organizations (5,000-100,000 staff) have budgets of under $10,000, which will most likely limit the effectiveness of their awareness programs.

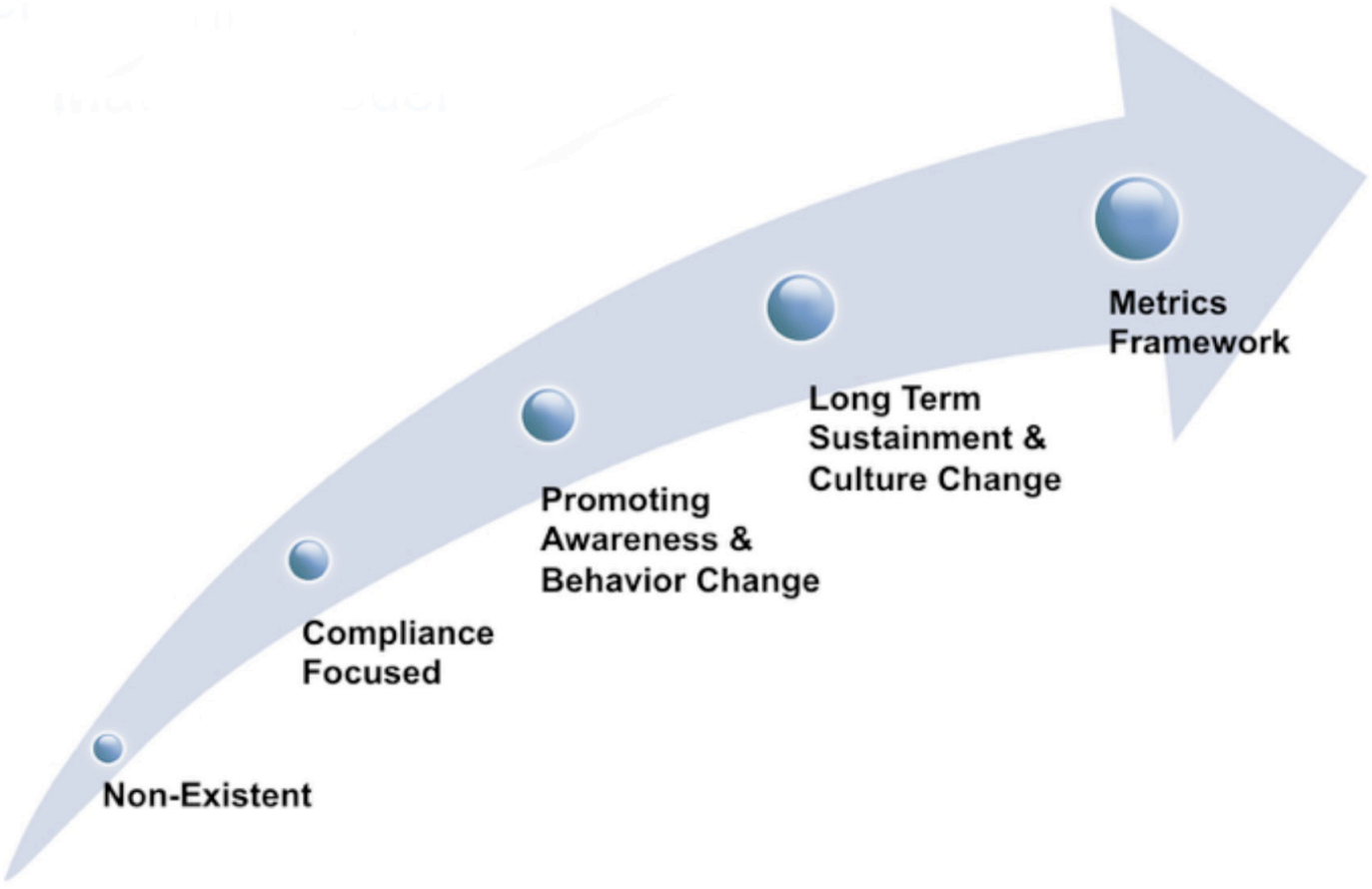
What Is Your 2015 Security Awareness Budget (by Organization Size)?



Results & Challenges

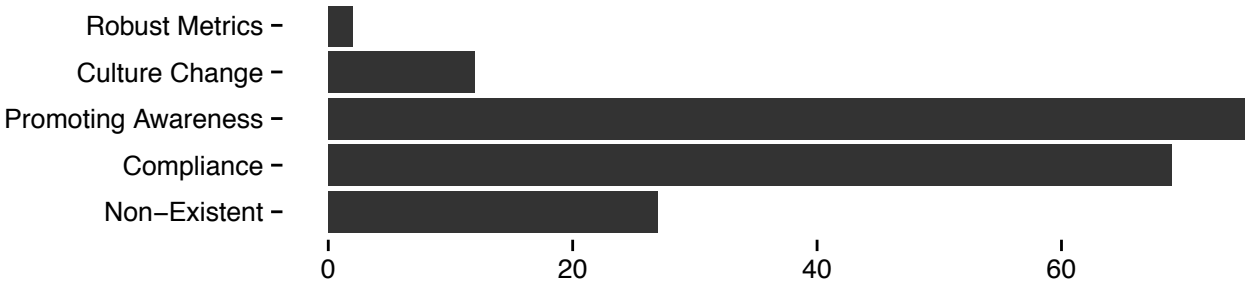
How Mature Is Your Awareness Program?

Awareness is still in its infancy. To define maturity, we used the Security Awareness Maturity Model, a model developed as a community effort by over 200 security awareness officers.

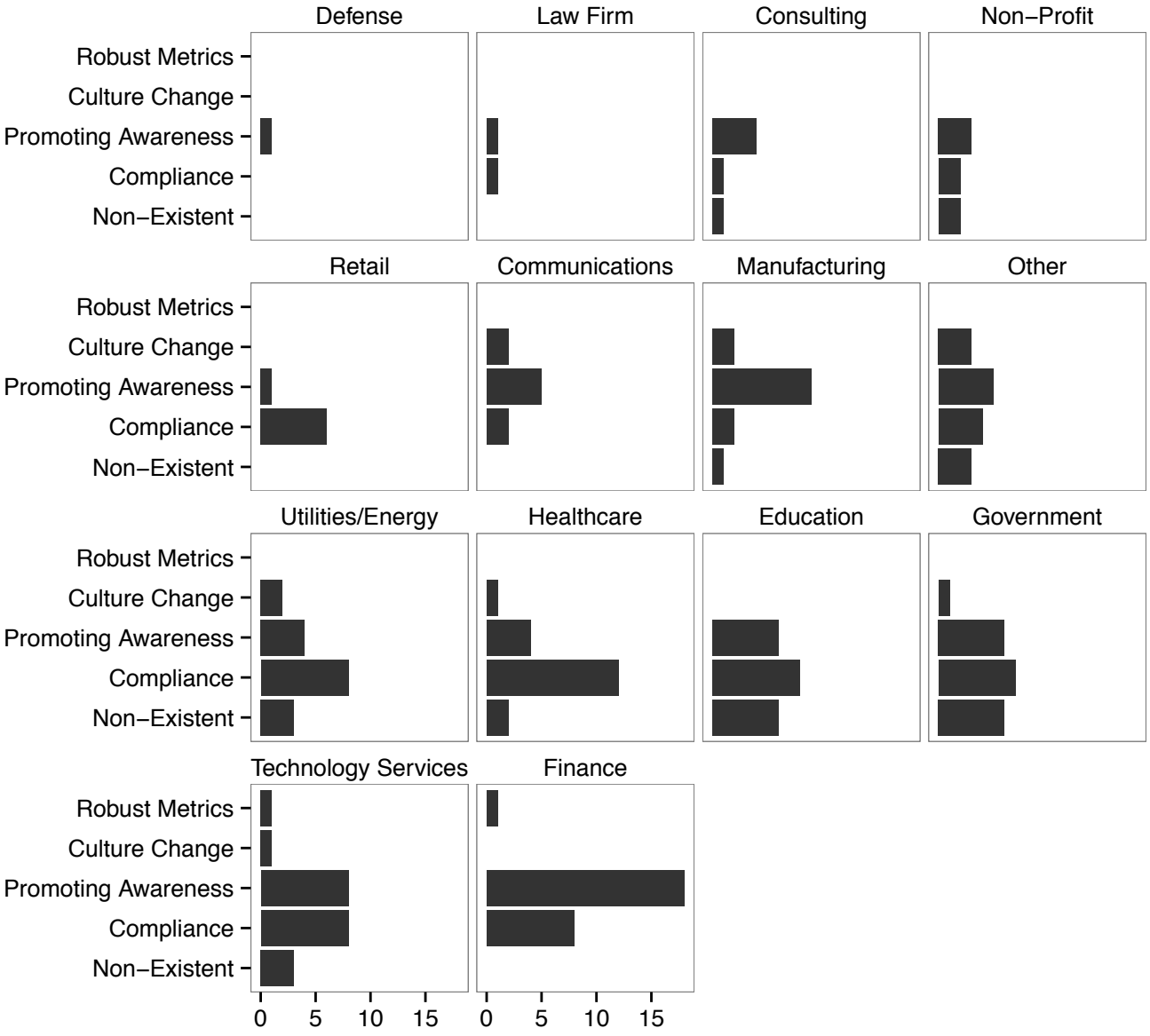


Half of the organizations surveyed either have no awareness program at all or one that is merely compliance-focused. Less than 5% said that they were at the most mature level, effectively changing behavior and culture, while also having the metrics to demonstrate that. Not surprisingly, for organizations with smaller budgets overall, half the awareness programs were very immature (compliance-focused) or did not even exist. Budgets aside, metrics-based programs are more common in mid-tier organizations than in larger or smaller organizations. This could be due to the fact that technology and financial service organizations have generally adopted metrics-based approaches more often than other organizations.

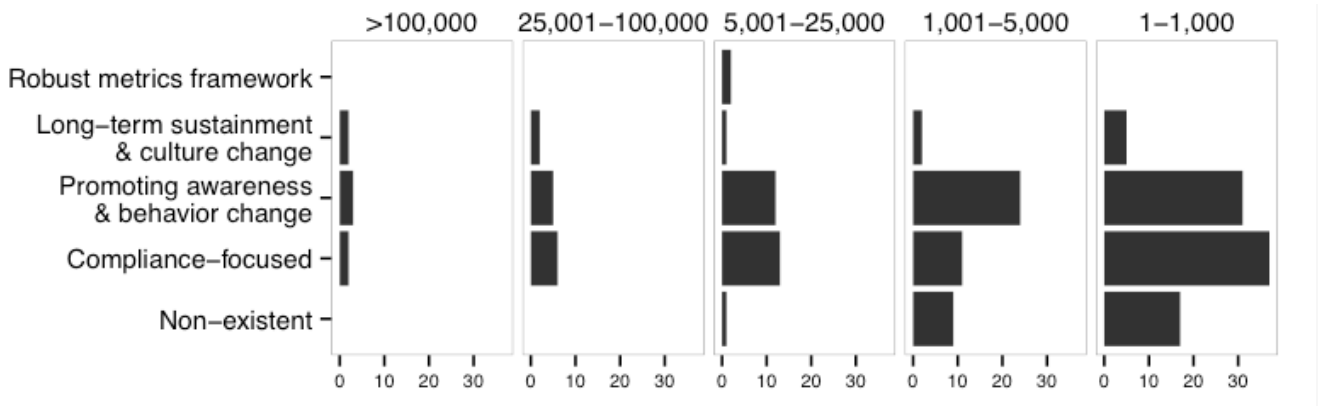
Awareness Program Maturity



How Would You Classify the Maturity of Your Organization's Security Awareness Program (by Industry)?

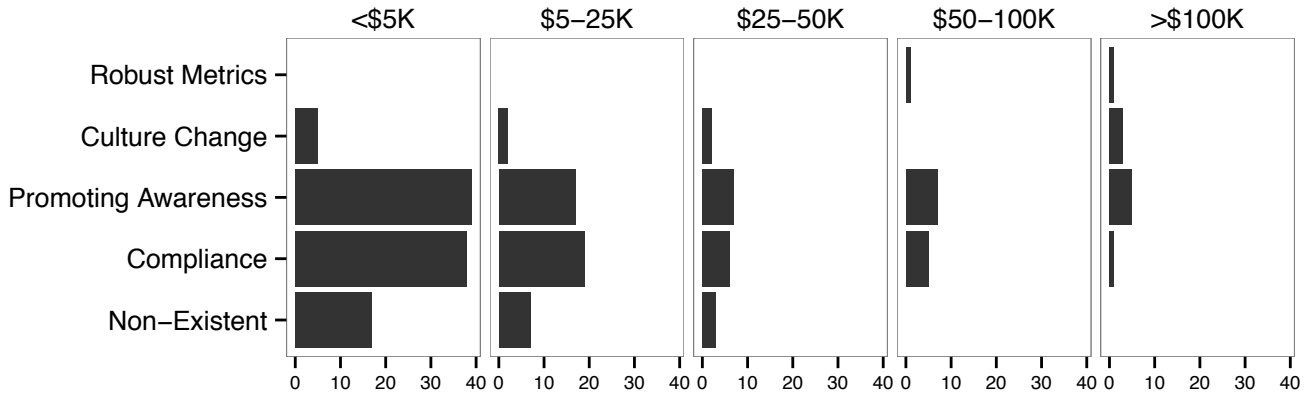


How Would You Classify the Maturity of Your Organization's Security Awareness Program (by Organization Size)?



This chart is key. It demonstrates that as budgets increase for your security awareness program, so does its maturity level.

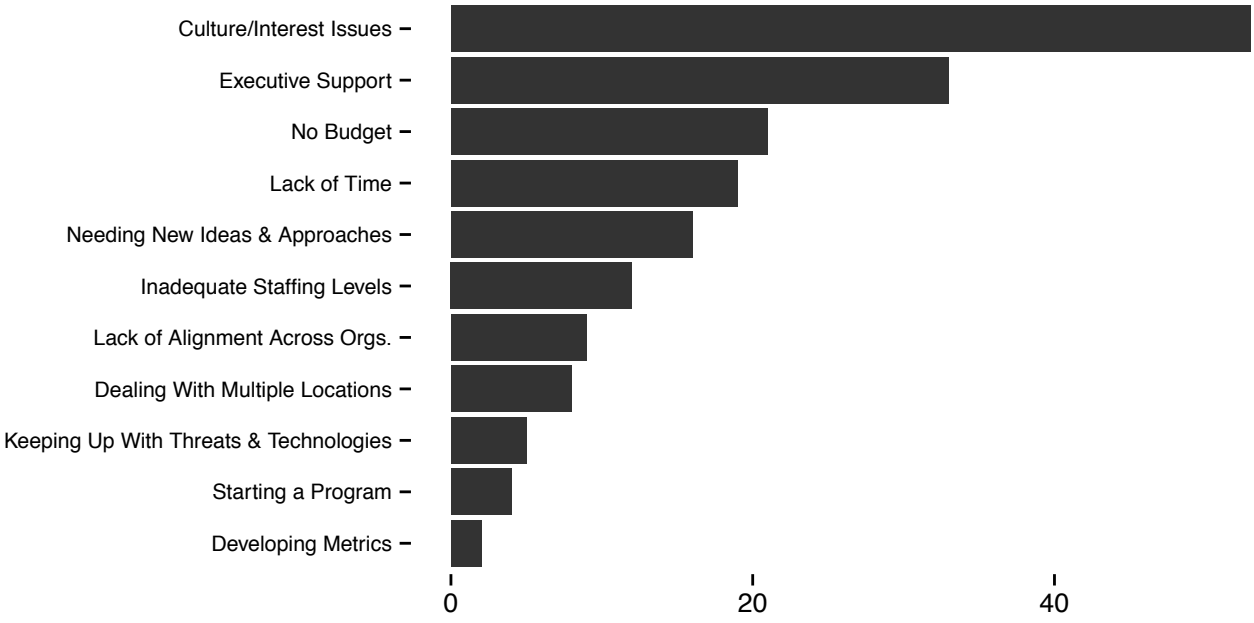
How Would You Classify the Maturity of Your Organization's Security Awareness Program (by Budget)?



Top Challenges for 2015

The top two challenges facing security awareness officers are employee engagement and lack of money and support from senior management. The two are related. We cannot engage employees if the security awareness officers lack the training, resources and support they need to create an engaging program. The way to turn such programs around is through the support of senior leadership. They need to understand that their organization cannot effectively mitigate risk if security is treated only as a technical issue; the human issue must be addressed also.

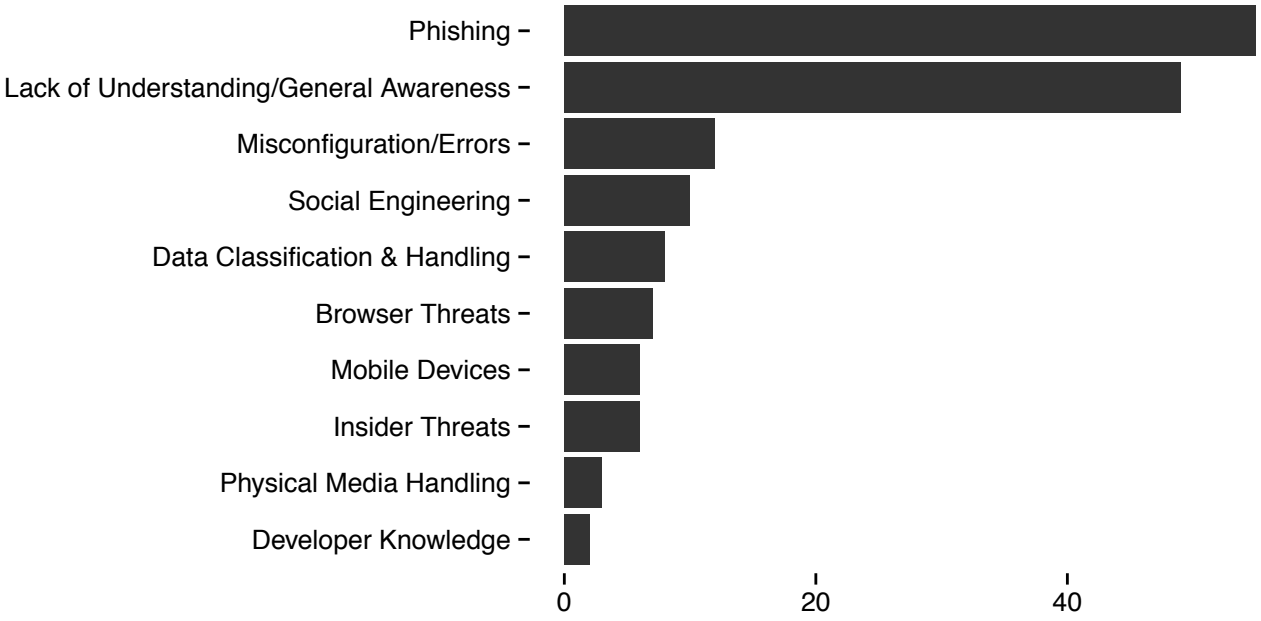
What Do You Feel Is the Biggest Challenge You Are Facing With Your Security Awareness Program?



Human Risks for 2015

Finally, we asked respondents what they expected the greatest human risk to be to their organizations in 2015. Phishing was unsurprisingly at the top of the list, but close behind was the fact that awareness officers feel employees do not realize they are targets or do not understand the need for security. This is troubling. It implies that our efforts to address human security are still very much in their infancy. We are not going to effectively change behavior until people have a sense of urgency, realize that they are targets and understand that their behaviors make a big difference. We as a community cannot hope to change behaviors without first making sure that people understand the problem and are engaged.

What Do You Feel Is the Greatest Human Risk Your Organization Must Mitigate for 2015?



Conclusion

Security awareness is still in its infancy. This isn't surprising, but it is good to have the numbers confirm it. What is surprising is how little support these programs continue to receive. Security awareness officers lack appropriate training and have minimal time, budgets and resources to accomplish their goals. In addition, because security awareness is more about the human element than technology, it requires extensive soft skills. Unless security awareness officers are trained in soft skills or able to tap people who already possess them, they will not be able to have an impact. Ultimately, for security awareness to grow and really make a difference, it needs the following:

1. **INCREASED SUPPORT**: Leadership needs to support security awareness programs. The need for cyber security has finally been recognized, but the focus on bits and bytes obscures the need to also address the human side.

2. **ACCESS TO SOFT SKILLS**: Organizations need to invest in and train their security awareness officers on the softer skills required for any security awareness program, or provide them access to the people who can deliver those diverse skills.

3. **MORE TIME**: Any organization with over 10,000 employees should have at least one person dedicated to running the security awareness program. Giving the person in charge of security awareness multiple responsibilities destroys his or her ability to focus.

4. **BIGGER BUDGETS**: Invest as much into securing your employees as you do in securing the devices they use.