SANS
SECURITY
AWARENESS

Creating Environments for Successful Awareness Programs:

Security Awareness for Executives

Table of Contents
Executive Security Awareness Report

Introduction

This first annual report on security awareness for executives is designed to answer the question, "What can executives do to create or enable their security awareness programs to succeed?" We dig into data from security awareness professionals around the globe to discover the common questions awareness leaders have:

- What resources, support, and inspiration can I add to address the growing area of human cyber risk?
- What individual or institutional blockers may be negatively impacting our awareness programs? What can I do to help?
- How does my organization's program compare to those of my peers?
- How do I evaluate the success of our security awareness program? What should I be looking for in terms of program goals?

This document serves as a companion guide to the 2018 Security Awareness Report, which was designed as a data-driven resource for security awareness professionals. Senior executives who support such awareness initiatives could benefit from this report.

Report Demographics

Figure 1: Reporting Industries

The 2018 Security Awareness Report aggregated responses from 1,718 awareness professionals across 65 countries. At a minimum, these professionals are either "responsible for" or "primary contributors to" their organization's awareness programs. Report respondents came from a wide variety of industries and organizational sizes, ranging from small numbers of trainees to programs reaching hundreds of thousands.

Security awareness leaders continue to show little consistency in their titles, which reflects the relative immaturity of the field. Organizational structures are more consistent with the majority of security awareness staff reporting to technical departments such as CIO, CISO, or IT Director.

Why is Managing Human Risk so Important?

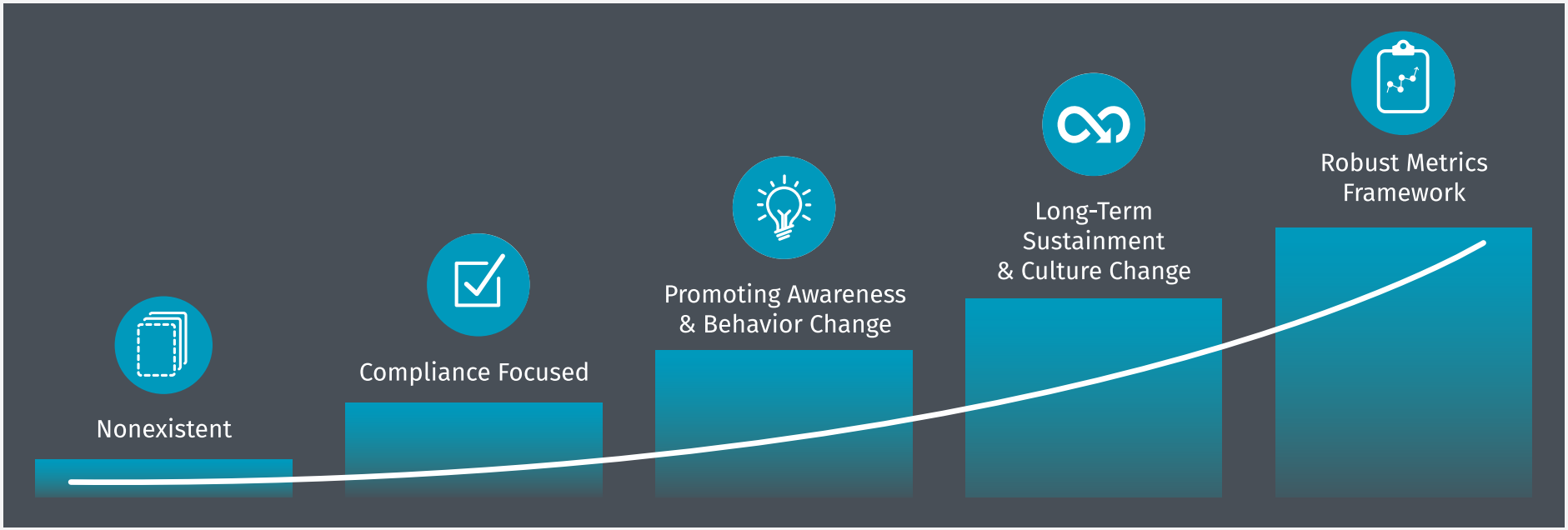
As technical solutions continue to evolve and play a key role in managing overall cyber risk to organizations, we are hitting the point of diminishing returns. Organizations continue to focus on and invest in technical solutions, but forget the importance of the human element. As a result, people are unprepared for the risks they face or how to secure themselves and the systems and data they work with. Therefore, people have become the primary attack vector for cyber attackers. In many ways, advancement in security technologies have made humans an easier target and a high percentage (https://enterprise.verizon.com/resources/reports/dbir/) of known information breaches have some human component.

Training security operations staff and funding of various technological efforts allow for the effort of a small number of people to have a large impact on security, but only a broad effort can result in a well-trained workforce. This not only dramatically reduces the number of incidents, but it can significantly increase your organization's ability to detect and respond to those incidents. Verizon's DBIR and SANS have found that people, not technology, were the most effective at discovering an internal incident. For this reason, cyber security awareness programs have become key components of the overall security risk management for a growing number of organizations today.

Use or disclosure of data contained herein is subject to the restriction on page 28.

The Evolution of the SANS Security Awareness Report

Figure 2: Maturity Model



In 2011, the SANS Institute, in conjunction with over 200 members of the security awareness community, developed the SANS Security Awareness Maturity Model©. The idea was to better define and describe the overall maturity of awareness programs. Findings in this report leverage the Maturity Model to both benchmark your program against others and to provide a roadmap on how to mature your own program. This report is designed to help professionals understand the current state of awareness programs in terms of:

- Program maturity and staffing
- The typical supporters and blockers of awareness programs
- The nature and reach of training initiatives

While both the scale and the scope of subsequent reports have grown substantially, the intent remains the same and serves to provide insight and guidance in reducing human risk in organizations. Further details about the Security Awareness Maturity Model can be found in the 2018 Security Awareness Report.

How to Measure Your Program from an Executive Leadership Standpoint

How to Measure Your Program from an Executive Leadership Standpoint

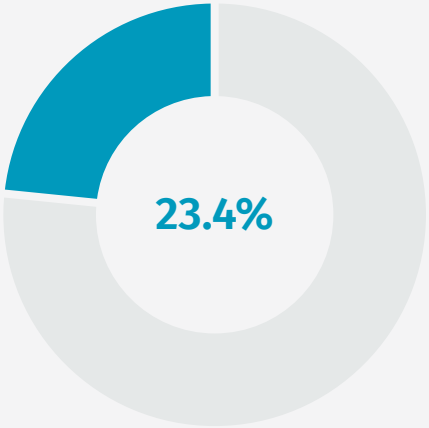
Program maturity provides context to help measure the success of your program. No program needs to be fully mature in order to see the results of a solid program plan. The goal of your awareness program is especially important, however, as it sets the tone for all future activities.

Your Primary Awareness Program Goal

Do you know your awareness program's current, primary goal? If your program is oriented around compliance, which represents 23.4% of the report's respondents in 2018, then the success of your program can be measured by the activities achieved at that level. Consider questions such as:

- Did all necessary training take place to achieve compliance?
- Did the assigned people complete the required training? Were records adequately kept?
- Were they trained on the correct content?
- Did new employees get required training within the appropriate timeline?

These questions are the basis for those needing to run and manage compliance-only, or basic security awareness programs. Less mature programs can still be "successful," provided they meet the requirements of the initial, outlined program goals. To develop a more mature program, review Establishing Program Goals within the Action Items below.



Awareness programs are focused on compliance as part of or the majority of their program.

Action Items
Establishing Program Goals

Identify the Current Goal for Your Program

Many program officers often speak in an aspirational manner when discussing program goals. Care should be taken to identify what the program seeks to achieve and how you define or measure success. What is your training program designed to do? Your goal should have a realistic, achievable statement, such as: "The goal of our program is to identify and manage our top five human risks, while ensuring our organization remains compliant with standards and regulations." Avoid writing a mission statement which is neither actionable or measurable in the near term.

Define Success in Terms of Your Immediate Program Goal

After establishing your program goal, identify what metrics you plan to use to measure your program. For example, a middle-maturity program may have this specific goal: "Identify the top five human risks to our organization, the key behaviors that manage those risks, and how we will measure those behaviors."

Whatever you decide success is, the program design should indicate some prescription for training based on roles and organizational memberships.

Remember to Evolve As Your Program Grows

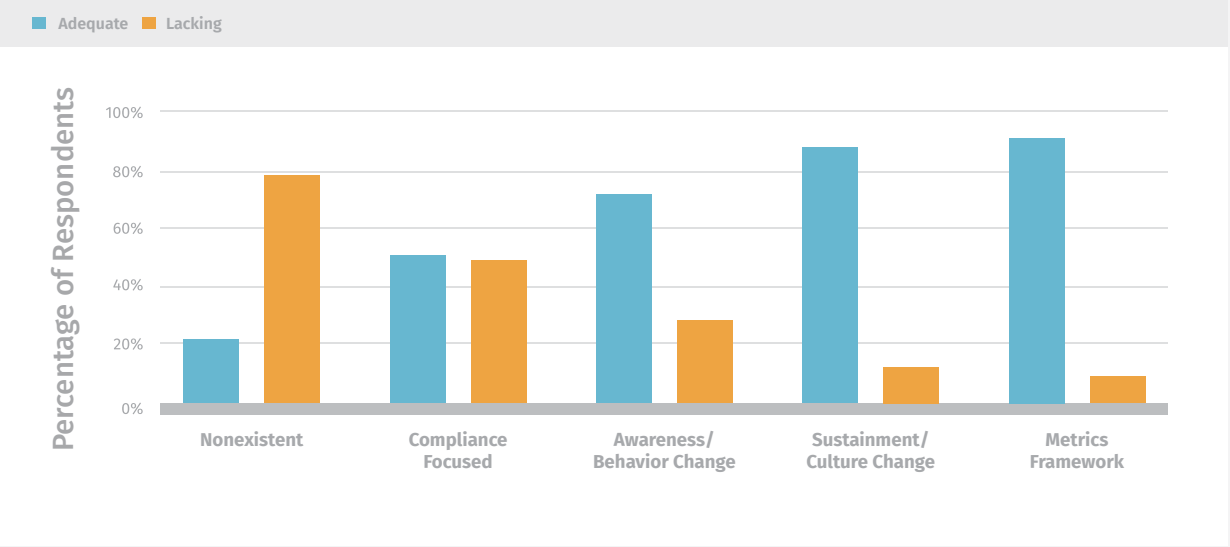
Successful security awareness training programs contain evolving program goals. Security Awareness staff should have an idea of the next generation of their programs. While successful training depends on near-term planning and measurement, long-term success of an awareness program requires evolution and redefinition of goals in order to increase maturity. Refer to the Security Awareness Maturity Model in the 2018 Security Awareness Report for further information on benchmarking your program.

Key Findings
Executive Leadership Support is Key

Executive leadership is a key element for a security awareness program to survive and thrive. The allocation of resources, enforceability of programs, identification of key program goals, along with the overall maturation of awareness programs, all depend on the support from key senior leadership.

Unsurprisingly, the data shows a clear correlation between support from executive leadership and program maturity. As depicted in the graph, the more support from the top down that an awareness program has, the better chance it has to grow into something that offers consistent culture change. [See fig. 3]

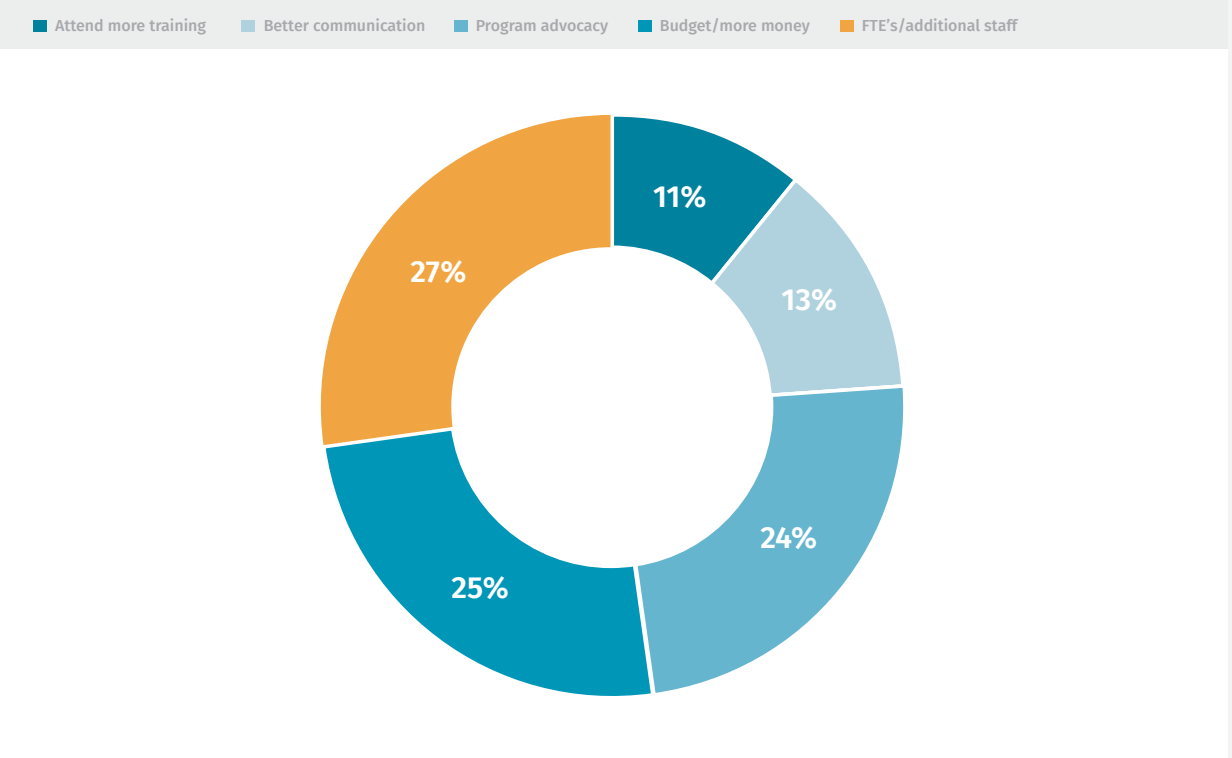
Figure 3: Program Maturity by Level of Executive Support



Key Findings
Executive Leadership Support is Key

A recent survey SANS conducted on 350 security awareness professionals in United States shows that other than having more FTEs, respondents revealed they wished their leadership played a much stronger role in advocating their awareness program. Other key asks were for better communication (both in quantity and variety, i.e., via email, face-to-face, corporate channels, etc.), and the opportunity for more training on building and enhancing a security awareness program. [See fig. 4]

Figure 4: Top 5 Requests from Security Awareness Professional to Leadership



Use or disclosure of data contained herein is subject to the restriction on page 28.

Action Items
Ways Leadership Can Voice Support

Participate Early, Often

In your team's program rollout, be first in line to take the training. Send out a supporting email emphasizing the necessity, value, and experience. A simple email describing, "I took the training, it was good, and it is very valuable to us as an organization" can provide a much-needed push in the initial adoption of a security awareness program. It sends a message that the leadership values this program and takes the time to do the training.

Communicate Out and Up

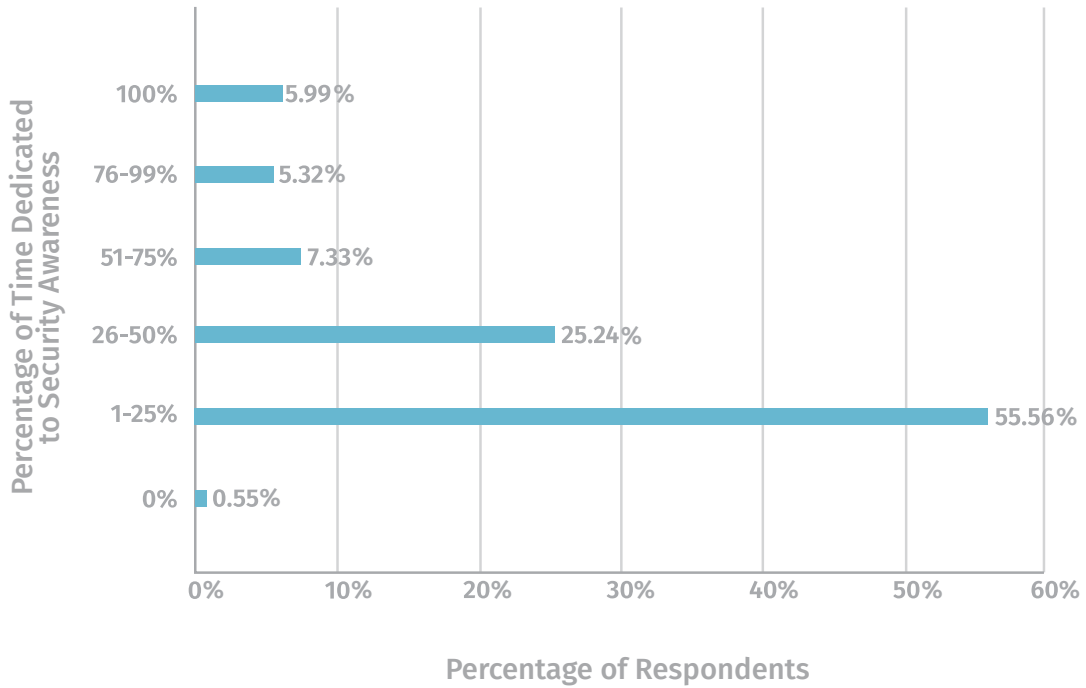
Security awareness programs rarely get, but do not depend on, total consensus of leadership to be successful. Communication isn't always about getting a total buy-in, but communicating a baseline understanding about the program will generate support. For example, if a CIO or CISO notifies the CFO in an open, casual manner, you could enable a positive environment for dialog. This could enable the opportunity to bring other executives into the fold of supporting the awareness program. Consider a message like, "Hey team, we are launching training next week to keep us safe and compliant. I wouldn't be surprised if you get some questions. Let me know if I can help answer them."

Invest in Alignment with Your Program Goals

The responses in this year's survey data shows a clear alignment between maturity and staffing. Successful programs also utilize a variety of training systems, training videos, phishing testing software, and so on. Realistically resourcing your program goals seems obvious, but the data shows staffing, staff resourcing, and training as key program blockers. As leadership, consider the investment you are allowing for and make sure that investment includes the right staff and training to make the program successful. When your security awareness professionals have the training they need, executing and maintaining a security awareness program becomes much easier to roll out.

Program Staffing

Figure 5: Time Dedicated to Security Awareness



Consistent with data received in 2017, respondents in this year's report clearly indicate that the **lack of staff-time is the number one challenge faced by security awareness organizations.** Over 80% of respondents reported **spending less than half of their time dedicated to awareness programs** and most organizations allocate security awareness program building as a part-time job. [See fig. 5]

Program Staffing

Figure 6: Combined FTE Program Staff vs Program Maturity

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

Executives involved in the resourcing, governance, and goal setting of awareness programs can aid these critical efforts greatly by evaluating the alignment between staffing and program goals. When assessing the needed program staff to maintain and mature programs, remember that while some aspects of program activity, such as in-person or live training increases with the number of trainees, many, such as material creation and CBT and phishing management don't. Consider if parts of your program can take advantage of contracted employees, services, or vendors to build up your program and to advance your training of key behaviors. Remember, the data clearly showed a correlation between programs with higher combined FTE counts and program maturity. Our data showed that organizations of 5,000 people should have at a minimum two FTEs dedicated to security awareness. [See fig. 6]

For those who want to go beyond changing culture and have a metrics framework, at least four FTEs are recommended. Ultimately securing organizations and keeping people safe, is a people problem, not a technology problem. Security awareness is a full-time job. It takes people to implement, maintain, and measure the solution. Whether you choose to do multiple in-person training sessions or implement computer-based training (CBT) for your awareness program, dedicated staff should be available to run the program full-time.

Action Items
Tips for Successful Staff Organization

Partnerships

Awareness is an organization-wide initiative. The most successful awareness programs have strong partnerships with different departments throughout the organization, to include Human Resources, Help Desk, Audit and Legal, Marketing and Communications, Security Operations Center, and other groups. Do everything possible to support and foster strong relationships between your security awareness team and the other departments.

Consider Staff Focus and Capability

Even programs with clear, measurable objectives often have varied approaches toward training. The path toward compliance programs, for example, still have specific training topics which need to be identified, training material that needs to be assigned, recorded, and reported, and so on. Consider asking your staff questions around the focus of the security awareness program:

- Do the skills of your team lean toward program execution or creation?
- Are staff members skilled in program design or do they need outside resources to help?
- Can staff create the appropriate training or should it be purchased?
- Does your organization have the proper delivery methods for offering phishing simulation and CBT?
- Do you own a LMS or need a vendor-hosted platform?

Organize your staff around it's competencies and fill in the gaps. Or, you may choose to outsource, purchase, and even seek community help. Whatever your program goals, consider the effect of misaligning outcomes and losing focus. Align your resources and staff carefully.

Use or disclosure of data contained herein is subject to the restriction on page 28.

Action Items
Tips for Successful Staff Organization

Soft Skills Equals Success

The most successful security awareness teams not only have strong technical skills, but also include members with strong soft skills. People with strong soft skills have the ability to communicate to, engage, and work with others. Security awareness professionals with highly technical backgrounds may suffer from what is called the "Curse of Knowledge". Because of their expertise, they find cyber security and awareness simple. As a result, they assume it is simple for others to comprehend, when in reality the principle can be confusing, even intimidating to others.

Don't look for computer science majors to lead your awareness efforts. Instead, look for those individuals who have backgrounds in communication, marketing or public relations. What security awareness professionals lack in technical understanding, they will quickly learn from your security team. Awareness programs fueled by personnel that have the ability to understand and communicate the way your organization expects will lead to greater success and adoption of the program.

Be Specific in Your Communication

Help your staff know and understand what you need. If you are looking for specific metrics or measurements, communicate that to your staff. If you are looking for specific wins or goals, once again communicate that.

Action Items

5 Questions to Ask When Evaluating a Security Awareness Training Vendor

1. What Kind of Security Awareness Training Do You Offer?

Your staff should request the type of awareness training offered from the vendor. What content is specifically included? Are there different types of training formats? What kind of supplemental materials are included with each training offering? A quality vendor should offer multiple options to help train a variety of people and meet optimal learning behavior.

2. What Are the Delivery Methods of the Training Materials?

There is more to a training program than the materials a vendor offers. It is especially important if your organization has international locations or if you have multiple departments in one location. Inquire if the vendor has more than one option for the delivery of training materials. Can you only deploy training on their platform or is content available to be hosted on your own? Are there options to do a hybrid approach?

3. What Level of Support is Available?

Any vendor you select should offer a solid support program. Maybe it's a customer success team, or dedicated account manager. They could have different levels of support available, or a blanket level support with options to add on specific managed services, but just be sure to have staff examine the quality support when purchasing training from a vendor.

Action Items

5 Questions to Ask When Evaluating a Security Awareness Training Vendor

4. How In-Depth is the Training Content?

The training content itself needs to offer a wide range of topics that cover the spectrum of relevant security threats, as well as a fairly deep level of information available on each topic. This allows the learner to fully comprehend the topic at hand. The goal of training is to change human behavior, but if the vendor you are considering only offers a limited selection for training, or the training isn't rich or engaging, it won't be useful for your organization. A great vendor should provide you with data from security experts on what topics are the "right" topics to train on. Your vendor should know and understand cyber security. What expertise does the vendor bring, what is their processes for the behaviors being taught and why? Ultimately, your training should focus on the fewest behaviors possible that have the greatest impact.

5. What Translations Are Available?

While this may not be a relevant question for every organization, many awareness programs have discovered the need for language translations in some capacity to help every learner grasp the concepts being taught. Ask about the types of languages, and the manner in which the content is prepared. How many languages are already translated? Does the content match the cultural requirements of that language?

What's in Your Program? Current Awareness Program Initiatives

The data we've gathered for this year's report revealed interesting insights around program initiatives that security awareness professionals commonly included in their programs. These insights reflect data reported from the top two maturity levels in the Maturity Model, which are Sustainment/Culture Change and Metrics Framework.

If you are looking toward more mature programs, expect to see:

- **Phishing Training Programs** – Specific phishing-oriented CBT, simulations, tests, and measurements.
- **Targeted Leadership Training/Briefings** – Training specifically designed for organizational leadership and management, report-out of awareness training activities, metrics, and resourcing.
- **Computer-Based Training (CBT)** – Broad usage of computer-based training addressing current essential awareness topics such as social engineering, privacy, and secure mobile device usage.
- **Ambassador Programs** – Leverage trained volunteers throughout the organization to accelerate change.
- **Support Materials** – Various forms of media (think newsletters, posters, games, mini videos, etc.) that allow awareness professionals to reinforce taught behaviors or concepts.
- **Events / Speakers** – Hosting speakers or events based on specific topics or relevant threats may boost awareness within your organization.

Consider incorporating these delivery methods within your training program.

Actions and Observations for Executives

Actions and Observations for Executives

Is there a culmination of what executives should be seeing, doing, or responding to in the development and maturation of a security awareness program? The data leads us to some actions that executives can take and use to create an environment for an effective and engaging awareness program. Of those successful programs, see figure 7 for top ten program success benchmarks, paired with top ways leadership can foster improvement.

Use or disclosure of data contained herein is subject to the restriction on page 28.

Actions and Observations for Executives

Figure 7: 10 Tactics for Rolling Out a Successful Awareness Program

Signs of a Successful, Mature Program	How Executives Can Help
1. Identified placement on the Maturity Model and goals for the future.	Work with staff to plan the awareness program
2. Defined the top human risks and the behaviors that manage those risks for your organization.	Offer partnerships with key security teams and work with security awareness professionals to identify ongoing risks.Offer partnerships with key security teams and work with security awareness professionals to identify ongoing risks.
3. Target audiences have been identified and assessed.	Resource staffing levels to attain program organization and goals (add FTE Staff).
4. Regular C-level briefings from program staff, including program reach, participation, and assessment data.	Task your awareness team to spend four hours a month on collecting metrics and measurements.
5. A strategic awareness program is planned that's friendly and valuable where people want to train.	Support your awareness team's effort to focus not just on work, but personal security. It is far more engaging.
6. A robust metrics program to measure key behaviors and strategic goals.	Be a mentor. Key security awareness staff need to learn how to deliver data and briefings in a way that resonates with executive leadership.
7. Training cycles that happen several times per year	Fund key program components such as CBT, phishing platforms, and training materials for long term efforts.
8. New staff training as part of onboarding	Encourage staff to connect with their peers. Join a cybersecurity awareness community online or network at a summit.
9. Secondary reinforcement training follow-ups	Be a program hero. Few programs need all executives on board to be successful, but all programs need a few to get anywhere.
10. Multiple methods of outreach, different people learn best with different modalities.	Offer budget support or ideas for easy resourcing of multiple learning outlets and modalities.

Conclusion

The data from the 2018 SANS Security Awareness Report indicates that although the security awareness industry is still in infancy, it promises encouraging progress and growth. While many organizations report a more entry-level program maturity, most reveal interest and understanding of the ultimate goals of behavioral and cultural change, and metrics. The data shows continued growth in support from executive leadership, although this does not always translate into more tangible backing with respect to budget and staff.

As a member of executive leadership, you have the ability to make a critical difference. Preventable incidents remain common and establishing a security awareness program can make a substantial difference. If you have a program, get involved and help. If you don't, work to establish one. Examples of initial and mature programs are plentiful, and the need to re-invent most program principals is minimal. Consider sending one of your staff members to the two-day SANS MGT433 course on Building, Maintaining and Measuring a Mature Awareness Program to kickstart the program.

A Big Thanks

We would like to take a moment and thank our contributors. Collecting data is easy. Sifting through all the data and creating a report that people can actually use is the real challenge. A big shout-out to the following who took the time to make this report happen:

The Kogod Cybersecurity Governance Center (KCGC)

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

KOGOD SCHOOL *of* BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC

A Big Thanks

Dan DeBeaubien
Author

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

Lance Spitzner
Author

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

Alyssa Ideboen
Editor

Alyssa Ideboen has over a decade of experience in writing and communications for organizations in the tech industry. She has authored works on the growth and management of SaaS platforms and software, the rise of OTT technologies, adaptive software development, the use and implementation of Electronic Medical Record (EMR) platforms, as well as security awareness. She currently writes, edits, and manages content and communications for SANS. Alyssa has a degree in Communications and Business, and a passion for advancing the education of information security.

About SANS Security Awareness

SANS Institute is by far the most trusted and the largest source for information security training in the world. With over 25 years of experience, SANS information security courses are developed by industry leaders in numerous fields, including cyber security training, network security, forensics, audit, security leadership, and application security.

SANS Security Awareness, a division of the SANS Institute, provides organizations with a complete and comprehensive security awareness solution, enabling them to easily and effectively manage their 'human' cyber security risk. SANS Security Awareness has worked with over 1,300 organizations and trained over 6.5 million people around the world. Security awareness training content is translated into over 20 languages and built by a global network of the world's most knowledgeable cyber security experts. Organizations trust that SANS Security Awareness content and training is world-class and ready for a global audience. The SANS Security Awareness program includes everything security awareness officers need to simply and effectively build a best-in-class security awareness program:

- Expert-authored training, tools, and content for easy compliance, better behavior change, and a more secure culture.
- Managed services support security awareness officers from program startup to measuring success.
- The world's largest and most engaged community of cyber security professionals, so you benefit from quick access to relevant and actionable information.

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

Use or disclosure of data contained herein is subject to the restriction on page 28.

SANS SECURITY AWARENESS