Welcome to Your New Job in Security Awareness – A Playbook

Version 0.2

SANS
SECURITY
AWARENESS

Table of Contents

Welcome to Your New Role

Welcome to your new role in Security Awareness, this is a challenging and yet rewarding field and we are excited to have you join us! This simple document will introduce you to expectations, goals and ultimately how to succeed and grow in this field. If you are a bit confused on what is expected of you, you are not alone. Security Awareness is a relatively new field in cybersecurity and quickly evolving and maturing. In addition, this field can have many different names, to include Security Culture, Security Engagement, Security Training and Education or Security Influence. Your role may be a full-time position dedicated to security awareness, or you may be part time with other responsibilities. Regardless of your title, industry, location and time-dedicated, your job is to help your organization's security team manage risk by focusing on the human side of cybersecurity. In many ways, your job is to make security simple for your workforce.

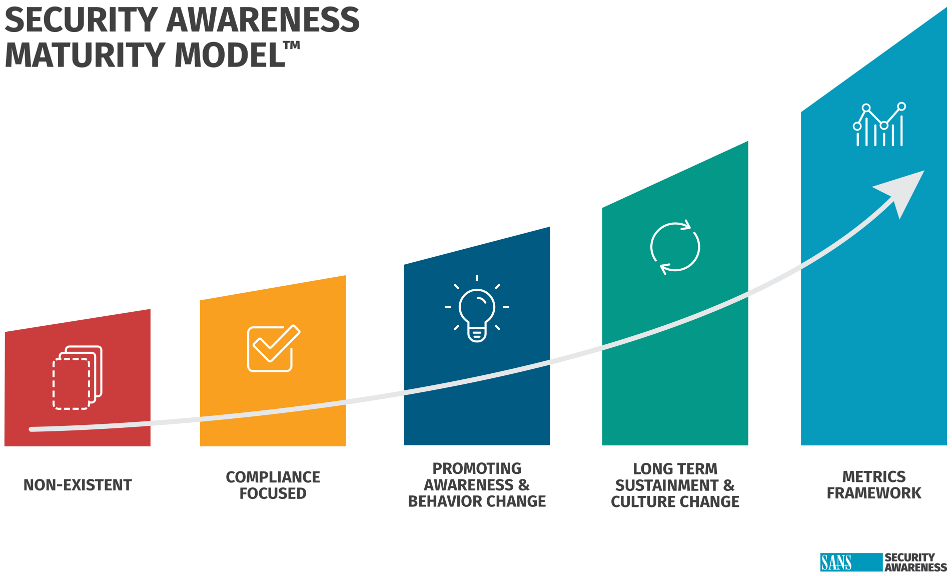
Resources

First, you are not alone, SANS has a tremendous number of resources to not only help you build a highly successful awareness program but grow your career and ensure you succeed.

1. **Community Forum**: SANS maintains a private, invite-only Community Forum just for security awareness and culture professionals. This is a very friendly, trusted and supportive group of over 2,000 awareness professionals from around the world. To learn more about this resource reach out to Lance Spitzner lspitzner@sans.org.
2. **MGT433 Human Risk Course**: This two-day SANS course walks you through step-by-step how to build, manage and measure a mature security awareness program, to include how to implement all the key steps covered in Security Awareness Maturity Model. New to security awareness or security in general, or looking to mature your existing program? This class is where you want to start. In addition, achieve the SSAP Credential (SANS Security Awareness Professional) demonstrating your expertise in this field.
3. **MGT521 Security Culture Course**: This five-day SANS class is designed for more senior or experienced leaders who want to focus on and develop their understanding of creating a strong security culture. It is highly recommended that people who take this class have extensive experience in cybersecurity and / or have completed the MGT433 course first.
4. **Security Awareness Summit**: This annual two-day event brings together awareness professionals from around the world to share their lessons learned, tips and resources on managing and measuring mature awareness program. Not only is this a fantastic opportunity to learn from your peers, but to network with others from around the world.

Security Awareness Maturity Model

Your goal is to help your security team reduce your organization’s human risk. Human risk involves the day-to-day behaviors people engage in that could expose your organization to harm. For example, employees falling victim to email phishing attacks or phone call scams, using weak passwords that are easy to hack or failing to update their devices or computers leaving them vulnerable to attacks. To manage these human risks and change peoples behavior you need to build, manage and measure a mature security awareness program. But what exactly does that mean, what are the different stages of a mature program, how do you know which stage you are in, and how do you grow and mature? SANS has developed the Security Awareness Maturity Model to enable you to answer these questions.



Established in 2011 through a coordinated effort by over 200 security awareness officers, the Security Awareness Maturity Model™ has become the industry standard model which organizations use to not only benchmark the maturity of their program, but to leverage as a strategic roadmap to both plan and communicate the impact of their program. What makes this model so powerful is that organizations can quickly determine why their program may not be having the impact they want, identify proven steps they can take to mature their program, and how to communicate program value to their leadership / stakeholders.

As you begin your role in Security Awareness, you must first determine where your organization’s program currently falls on the Security Awareness Maturity Model.

Nonexistent

A security awareness program does not exist in any capacity. Employees have no idea that they are a target, that their actions have a direct impact on the security of the organization, do not know or follow 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 being offered on an 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

The program identifies the target groups and training topics that have the greatest impact in managing human risk and ultimately supporting the organization's mission. The 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. As a result, people understand and follow organization policies and actively recognize, prevent, and report incidents.

Long-Term Sustainment & Culture Change

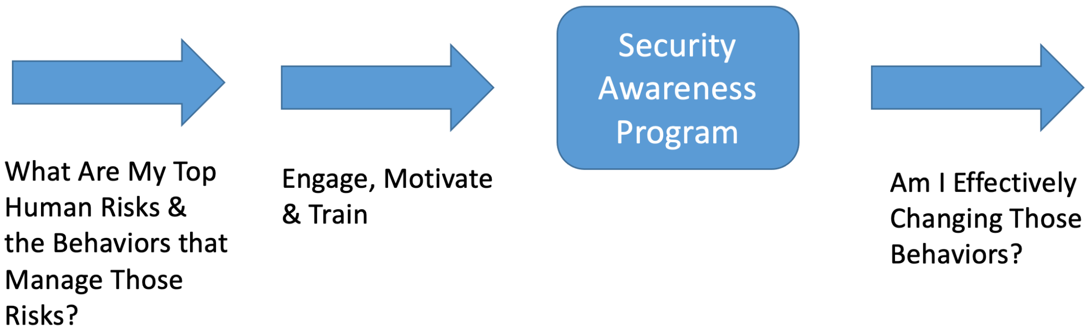
The program has the processes, resources, and leadership support in place for a long-term life cycle, including (at a minimum) an annual review and update of the program. As a result, the program is an established part of the organization's culture and is current and engaging. The program has gone beyond changing behavior and is changing people's beliefs, attitudes, and perceptions of security.

Metrics Framework

The program has a robust metrics framework aligned with the organization's mission to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment. Metrics are an important part of every stage, and this level simply reinforces that to truly have a mature program, you must be able to demonstrate value to the organization.

Building Your Strategy

So how do you go about building a mature program? There are three strategic priorities to building your awareness program. Remember, your goal is to effectively manage (reduce) your organization’s human risk by changing peoples behaviors.


What Are My Top Human Risks & the Behaviors that Manage Those Risks?
Engage, Motivate & Train
Security Awareness Program
Am I Effectively Changing Those Behaviors?

1. **Risks**: What are the top human risks to your organization and the key behaviors that reduce those risks? For example, do we people need to change behavior so they can easily identify the indicators of a phishing attack, use stronger passwords, or enable automatic updating on their devices? To effectively manage human risk you need to first identify and prioritize your human risks. This often requires not only reviewing data from past incidents or audits, but can also include assessing your workforce’s knowledge, behaviors and security culture.

2. **Engage and Train**: How do you most effectively engage, train and enable your workforce to exhibit those behaviors? The key here is to make security simple for your workforce. It’s not just about training, but about simplifying policies, providing people tools, and communicating in a simple manner anyone can understand.

3. **Measure**: Ask yourself - *How do I measure the impact I’m having? Are we changing key behaviors, are we reducing risk*? If you completed step #1, measurements can be easy than you think.

You should try to plan your security awareness program from this perspective and in this order. You begin by understanding what your top human risks are, then the behaviors that manage those risks, then determine how will you change peoples behaviors? If you already have an awareness program you are attempting to mature, start with step #1, review what you are teaching and why.

So Where do I Start? Partnerships

So where do you start, how do you achieve all of this? The first thing is, you DON"T do it all alone. The key to your success is partnering and working with other teams throughout your organization. You are attempting to solve a human problem, that requires a human solution. You can use technologies to help save you time (such as Computer Based Training) but that is a small part of a much bigger challenge. These are the groups you should be partnering with, listed in order of whom we feel you should start with first.

1. **Senior Leadership**: For your program to succeed you need to ensure you have senior leadership support. Depending on the size, industry and your structure of your organization, this may mean just keeping your Chief Information Security Officer (CISO) updated to perhaps communicating to your entire executive board. To accomplish this you need to communicate in business terms how you are helping support your organization's mission. Don't communicate in terms of what you are doing (CBT, lunch-n-learns, guest speakers) but instead focusing on why you are doing it – reducing human risk. This is why the "*Building Your Strategy*" section we just covered is so important, by following those three strategic steps you can demonstrate you are managing human risk, and not just in the entertainment business.
2. **Cybersecurity Team**: A big part of your job is helping your security team identify and manage your organization's human risk. Remember, by human risk we mean the behaviors that people exhibit that expose your company to potential harm. For example, are people vulnerable to phishing attacks or texting scams, are they using weak passwords or sharing their passwords with others, are they using outdated, easy to hack devices? By changing your workforce's behavior, you create a more secure workforce. This starts with partnering with key people in your security team who understand your organization's top risk, such as those involved in the Security Operations Center (SOC), Incident Response team or the Cyberthreat Intelligence (CTI) team. Reach out to them, introduce yourself and partner with them. In many ways your job is to help them. Most security professionals are highly passionate and very skilled but work primarily with technology. They have little experience or training in helping secure people and often struggle communicating security in simple terms to the workforce. They may not know how to priority top human risks or the key behaviors that manage those risks. Work with them to identify what are your top human risks, and determine most common behaviors that are causing breaches? What is your security team's top concerns when it comes to employees? Far too often security teams focus on just the technical side of cybersecurity. Part of your job is helping them understand that security is also a human challenge and helping them address that challenge.

3. **Communications**: Once your security team has helped you identify your top human risks, your communications team can help you engage your workforce and provide strategies on how to enable people to exhibit secure behaviors. Often this not only includes cybersecurity training but creatively communicating about new or updated security policies, supporting new security tool roll-outs, or communicating in a crises or about latest events in the news. Work with your communications team ahead of time. Partner with them to not only help you craft simple messages everyone will understand, but take the time to better understand their processes, challenges and how they operate. Don't make them change their processes to support you, instead work with their processes to make it easy for them to support you.
4. **Human Resources**: HR can help you in numerous ways. First, they may be responsible for training new hires or training for your entire organization. As such, they can help ensure all new hires receives initial security training. In addition, they often understand culture, so they can help you build a stronger security culture.
5. **Legal / Compliance /Audit / Privacy**: You may have certain legal or privacy issues you need to align with in managing your awareness program. Legal or compliance can also help you better understand key standards and regulations you need to adhere to. Additionally, legal, compliance or privacy programs may have information security value and benefits, and it may be possible to create awareness programs that covers multiple objectives
6. **Learning Management System (LMS) / Training**: If you are providing any type of Computer Based or Online Training, you are most likely providing it via a LMS platform. This technology is what hosts and provides online training. If you are hosting your training internally (as opposed to a vendor) you will need to partner with your department that hosts and manages your organizations LMS. Be sure you reach out to them six months before you want to deploy any online security training, it can take that long to coordinate their support. Far too often LMS or Training teams are understaffed and under resourced, having to work with outdated tools and technology.
7. **Help or Support Desk**: As you begin to roll-out your awareness program people will have questions about cybersecurity policies, tools, expectations and behaviors. Train and prepare your Help Desk to best support your workforce.

Summary

This is a very exciting time to be involved in security awareness, as not only can you have a tremendous impact for your organization, but you have just joined an extremely friendly and supportive community. Welcome aboard, as there are many opportunities grow your career in this developing field!

Appendix – Common Security Terms

Here are the definitions of some of the most common security terms used in our field. Please keep in mind that there are no internationally recognized definitions for security terms. Every organization, and quite often every individual has their own perspective on what each term means. Never feel afraid asking someone what they mean when they are using security terms. For example, you can ask "What do you mean by *Insider Threat*" or "What is your definition of *Vulnerability Management*?". If your organization uses a different definition of any of the terms below that is fine, what is important is ensuring everyone in your organization is using the same definition.

- **Awareness**: Awareness focuses on changing behaviors; it does not teach new skills. Think of email. Our goal is not to teach people how to use email; they already know that. Our goal is to teach them new behaviors, specifically how to use email safely and securely. People already know how to click a link in an email; however, we show them how to spot indicators of a phish and when not to click that link.
- **Culture**: People's shared attitudes perceptions and beliefs. Your security culture is peoples attitudes, perceptions and beliefs towards cybersecurity. Some of the biggest drivers of your security culture are your security policies, your security team and the interactions your security team has with your workforce.
- **Education**: Education is not just learning skills, but the theory and knowledge that go behind those skills. Education may be beyond the scope of your security awareness program as most awareness programs focus primarily on *awareness* and *training*.
- **Impact**: The damage or harm caused by an incident. Impact is one of the three variables that make up the equation of risk (the other two are *Vulnerabilities* and *Impact*).
- **Insider Threat**: This is one of the most commonly confused terms in our field as so many people have different definitions. At the simplest level, the term means a trusted individual (usually employee or contractor) that causes harm. Some organizations define Insider Threat as only trusted individuals who cause harm with malicious intent, some define Insider threat as only trusted individuals who cause harm with malicious intent or through negligence, while others use the term very broadly meaning anyone who causes harm, including employees who fell victim to an attack. Always ask individuals to clarify what they mean when using this term.

- **Risk**: The probability of something bad happening (called an incident) and the impact if something bad does happen. For example, what is the probably of you being in a car accident in the next 12 months, and if you are in a car accident what is the harm to you. Human risk is the risk caused by peoples actions, such as them using weak passwords, falling victim to phishing attacks or using unpatched, vulnerable devices. Security awareness is all about changing peoples behaviors so they are less likely to cause harm, and if they do cause harm we minimize the impact.
- **Security**: Security are the technologies, processes and people used to reduce risk. We either reduce the risk of an incident happening, and / or reduce the impact if the incident does happen.
- **Training**: Training teaches new skills and tends to be role specific. For example, an organization may add additional security training for its IT staff, developers, or Help Desk. The IT staff training could include new skills such as command-line tools they can use to find an indication of whether a system has been compromised.
- **Threats**: Entities that cause harm by exploiting vulnerabilities in your organization. Ultimately a threat always comes back to people. Malware is not a threat it is simply a tool a threat uses to achieve their goals.
- **Vulnerabilities**: Weaknesses in your organization’s technology, processes or people. The more vulnerabilities your organization has, the more likely it will experience an incident.