Cybersecurity is no longer just a technical challenge but also a human one. People and their actions represent one of the top risks organizations around the world face, but few organizations have a mature program to manage their human risk. Security Awareness Programs identify the top human risks to your organization, the key behaviors that manage those risks and then enable and change those key behaviors organization wide.

The most effective programs go beyond just changing workforce behavior but ultimately embed a strong security culture. The Security Awareness Maturity Model enables you to benchmark where your program is, define where you want to take it and provides a detailed roadmap and the resources to get there. Also, the model is a powerful tool to communicate to leadership your strategy and sustain their support.

Security Awareness Roadmap

Managing Your Human Risk

SANS CYBERSECURITY LEADERSHIP

sans.org/cybersecurity-leadership

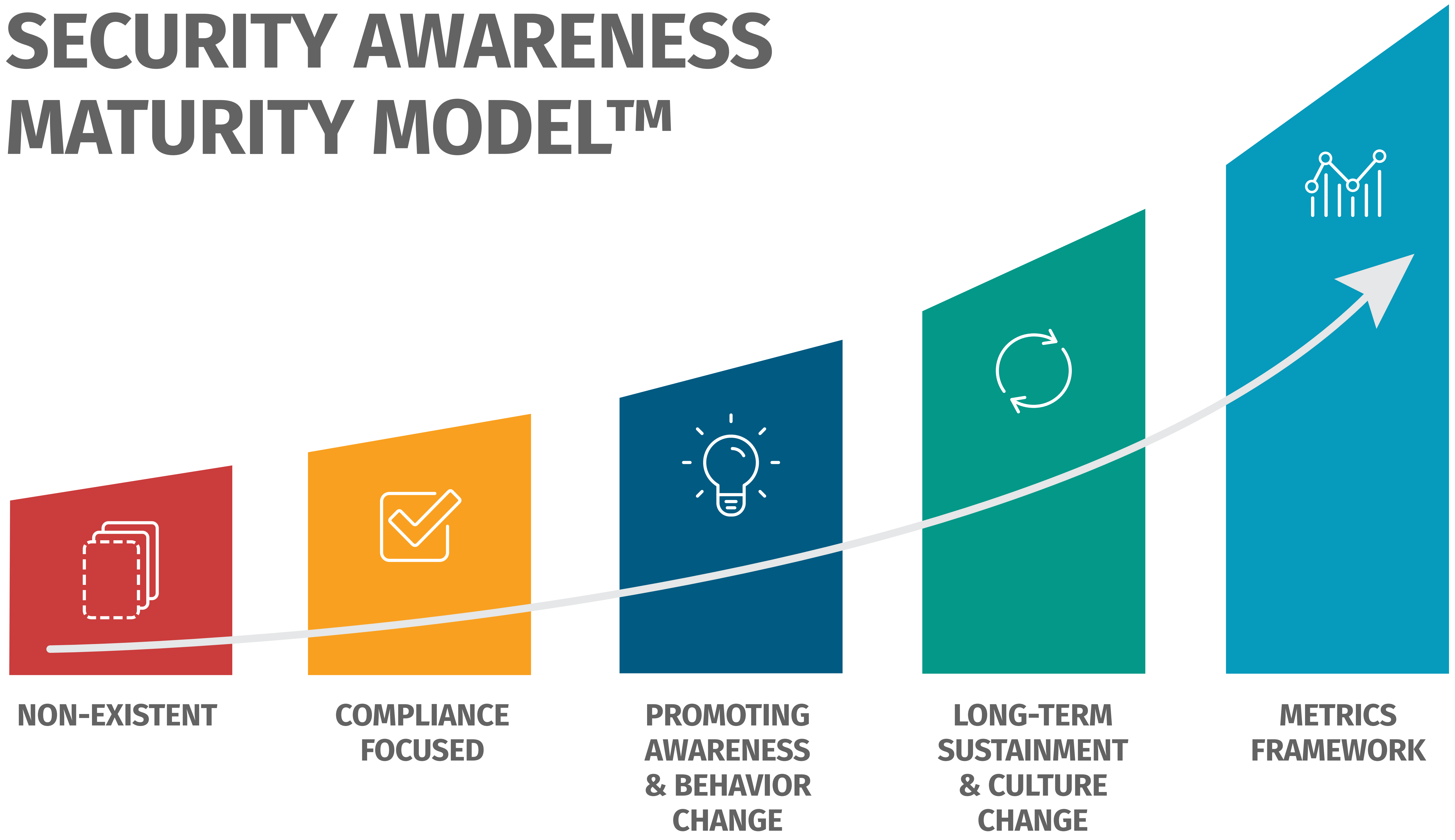
@secleadership

SANS Security Leadership

SSA_Roadmap-v1.1_05-21

This poster was created by Lance Spitzner with support of the SANS Faculty. ©2021 Lance Spitzner. All Rights Reserved.

SECURITY AWARENESS MATURITY MODEL™



NON-EXISTENT

COMPLIANCE FOCUSED

PROMOTING AWARENESS & BEHAVIOR CHANGE

LONG-TERM SUSTAINMENT & CULTURE CHANGE

METRICS FRAMEWORK

Key Elements to a Successful Program

Managing human risk is a people problem, as such it requires people as the solution.

- Your Security Awareness Program should report to and be an extension of the Security Team. Awareness is nothing more than another security control, one to manage human risk.
- The individual in charge of the Awareness Program should be dedicated full time to managing it.
- Running an awareness program requires strong people skills, including effective communication and partnering but also understanding the fundamental concepts of cybersecurity and risk management.
- The key to managing human risk is both motivating and enabling change. The most common mistake organizations make is making security hard, confusing and overwhelming for their workforce (Curse of Knowledge).
- The key to maintaining leadership support is do not communicate in terms of what you are doing (such as gamification) but in terms of how you are helping the organization manage its human risk. Demonstrate how your program supports leadership's strategic security priorities.

Developing Your Career

SANS MGT433: Managing Human Risk: Mature Security Awareness Programs

This intense two-day course will enable you to build a mature awareness program that proactively engages your workforce and has an impact you can measure.

sans.org/mgt433

SANS MGT521: Leading Cybersecurity Change: Building a Security-Based Culture

This advanced five-day course is designed for senior security leaders and highly experienced awareness officers. The course provides the skills, models and frameworks to build, manage and measure a strong security culture.

sans.org/mgt521

Trust SANS to Bring Security Awareness to Your Workforce

Leverage our best-in-class Security Awareness solutions to transform your organization's ability to measure and manage human risk. Expertly created, comprehensive training builds a powerful program that embodies organizational needs and learning levels.

SANS SECURITY AWARENESS

sans.org/security-awareness-training

@SANSAwareness

linkedin.com/showcase/sans-awareness

Security Awareness Maturity Model Indicators Matrix

This matrix details each of the stages of the maturity model, identifies which stage your organization is in, the value of the stage, and how to achieve the next stage. Leverage this matrix as a strategic planning guide for your approach to managing and measuring your organization's human risk. For more information and free resources, visit **sans.org/security-awareness-training**.

Maturity Level	Description	Program Indicators	People Indicators	Time to Achieve	Metrics	Steps to Next Level
STAGE 1 No Security Awareness Program	Program does not exist. 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 understand organization policies, and easily fall victim to attacks. **VALUE: None – your organization is at high risk to both failing to meeting any compliance requirements and highly vulnerable to human-driven incidents.**	• There is no security awareness program. • Leadership does not discuss or care about security awareness.	• Employees never discuss security or exhibit secure behaviors.	N/A	None	• Identify the regulations or standards that you must adhere to • Identify security awareness requirements for those standard • Identify someone to roll out the required security awareness training • Develop or purchase training that meets those requirements • Deploy security awareness training • Track and document who completes the training"
STAGE 2 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. **VALUE: Your security awareness program meets the legal requirements your organization is required to adhere to. However your organization is not effectively managing it's human risk.**	• There is no strategic plan – training topics are ad hoc and deployed at random times. • Program has limited leadership support – leadership's goal is to maintain compliance at minimum costs. • Security awareness is only considered during audits. • Program lead is a part-time job for one single person, often someone reporting to the compliance, audit or governance teams. • There is little coordination or partnership with other departments, such as communications and human resources. • Leadership perceives security is purely a technical issue. • Training is primarily once a year. • There is little to no communication to the workforce about security beyond the annual training.	• People have a "Let's get this over with" attitude. • People feel security is something that IT takes care of, it's not their problem. • People feel security is something they have to do. • People have a negative perception of security and/or the security team.	Depends on the standards, regulations or legal requirements you are attempting to adhere to. However the overall effort is usually minimal, requiring nothing more than annual training.	• Number/% of people that have completed training • Number/% of people that have signed Acceptable Use Policy • Number of on-site training sessions in one year • Number/frequency of awareness materials distributed (newsletters, posters, etc.)	• Identify and gain support of stakeholders • Create Project Charter, identifying things such as scope, goals, objectives, assumptions, and constraints • Identify who will be responsible for the awareness program. To ensure greatest success that person should be dedicated full time, have soft skills and report to and be a part of the security team. • Create Advisory Board • Identify the top human risks you will need to manage, this may require a human risk assessment • Identify the key behaviors that will mitigate those risks • Identify how you will communicate to, engage and train your workforce, to include cultural analysis, primary training and reinforcement training • Develop or purchase your materials • Create execution plan with milestones, to include metrics • Have senior leadership announce plan, execute
STAGE 3 Promoting Awareness and Behavior Change	Program identifies the target groups and training topics that have the greatest impact in supporting the organization's mission and focuses on those key elements. 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 and at home. As a result, people understand and follow organization policies and actively recognize, prevent, and report incidents. **VALUE: Your organization is not only meeting its compliance requirements, but is able to effectively manage and measure it's human risk.**	• Leadership understands and commits to the need for managing human risk. • There is a strategic plan that has identified the scope of the project, goals, objectives and justification for the program. • Security team has identified and can explain their top human risks and the behaviors that most effectively manage those risks. • Program has sufficient leadership support to provide resources necessary and has an executive champion. • Security awareness is considered part of the organization's overall security effort. • Program lead is dedicated full time to the effort, has a strong communication skills and is a part of the security team. • Program coordinates and collaborates with various departments within organization, including Communications, Human Resources, and Help Desk. Often this coordination is done through an Advisory Board. • Program has gone beyond just annual training and includes continuous reinforcement throughout the year. Usually also includes a phishing program. • Program works to postively engage the workforce.	• Employees understand that security technology alone cannot protect them and they have a responsibility to protect themselves and the organization's assets. • People are reporting incidents or suspected attacks. • When security team pushes out information, people are asking them questions. • Employees are exhibiting the behaviors they are being trained on. • Employees bring strong security behaviors home.	Depending on the behaviors you are attempting to change, you can begin impacting behaviors organization wide within 3-6 months. For example, you can begin to see a dramatic drop in phishing click rates organization wide if you do extensive phishing training and simulations. However, the more behaviors you are attempting to change, the longer it can take to change those behaviors organization side. This is one of the reasons it is so important to priotize your top human risks, and the behaviors that manage those risks. The fewer behaviors you focus on the more likely you can change those behaviors.	• Phishing simulation click and report rates • Number of infected computers/devices each month • Number of lost or stolen computers/devices each month • Number of security policy violations • NOTE: See the interactive metrics matrix for more examples. These metrics are ultimately driven by what behaviors are the most important to managing your human risk.	• Establish a process to give leadership regular updates on awareness program • Identify new or changing technologies, threats, business requirements, or standards that should be included in annual update • Conduct surveys and assessments to determine current state of awareness and associated behaviors • Schedule a specific date when the security program is reviewed every year and updated by the Advisory Board • Expand modalities to scale and engage workforce. Examples include ambassador program, gamification, and OSINT briefs for senior executives • Build outreach, communication and engagement efforts into as many security initiatives as possible.
STAGE 4 Long-Term Sustainment and 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. Program has gone beyond changing behavior and is changing people's beliefs, attitudes, and perceptions of security. At a minimum, it takes 3–10 years to achieve this level. **VALUE: Your organization is not only meeting compliance requirements and managing it's human risk, but a strong culture enables and promotes the success of other security initiatives and efforts, and helps ensure security is built into almost all operational aspects of the organization, expotentially increasing the overall security of organization.**	• Program is actively reviewed and updated on an annual basis. • Program has identified multiple different target groups that have unique training requirements, including skills-based training for IT and Developer groups. • Leadership believes in and has invested in long-term support of the program. Program lead is actively updating leadership on a monthly basis. • Security team believes in investing in human controls just as much as technical controls. Strong integration between awareness and technical. • Multiple FTEs are dedicated to the program. • Program has developed training modalities that engage organization-wide, such as a security ambassador/champion program or gamification.	• Good security practices are "baked in" to who we are and what we do. • Employees educate others on good security behaviors. • Employees start providing ideas or suggestions on how to improve security in the organization. • Employees or departments request security briefings/updates; they are actively seeking more information. • Department leads and teams request security reviews/audits. • Departments beg to compete/compare who has the best security. • The security team and their security efforts are perceived as a positive thing by the workforce.	Impacting your organizational culture takes much longer than impacting behavior. Impacting culture can take 3-10 years depending on the size, complexity and age of your organization and it's culture (John Kotter, Leading Change). For this stage we recommend not focusing on changing your organization's culture, but embedding security into and aligning with your organization's existing culture."	• Survey measuring people's attitudes, perceptions, and beliefs towards information security • Number of people/departments requesting security briefings or updates • Number of people submitting ideas on how to improve security • Number of people attending optional events * Number of requests on how family can take the training	• Creating a metrics dashboard that combines all the information/measurements from the different maturity levels. • Tie in metrics to technical security metrics and ultimately organization's overall mission.
STAGE 5 Metrics Framework	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. 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 impact.	• Metrics are collected on a regular basis, often automated. • Metrics are integrated into security frameworks, such as the NIST Cybersecurity Framework or 20 Critical Controls. • Different metrics are delivered to different target audiences.	• Leadership actively requests and uses security awareness metrics to measure their organizational progress/compare departments across organization.		All the above combined into a single dashboard interface or some type of centralizing capability that can be visualized and easily reported to business partners. Metrics are measured over time demonstrating long term impact. Strategic metrics include • Number of incidents • Time to detect an incident • Time to recover from an incident	

SANS SECURITY AWARENESS

SANS CYBERSECURITY LEADERSHIP