Organizations and security leaders are coming to terms with the fact that cybersecurity is no longer just a technical challenge but also a human one. In fact, people are now the biggest contributors to breaches, with employees involved in 68% of all breaches globally.* In many ways security teams have become so effective at using technology to secure systems that they are driving threat actors to target people.

The key to managing human risk is establishing a mature security awareness program. These programs take a structured approach to change and secure your workforce's behaviors. The most mature programs go beyond behavior modification and ultimately cultivate a strong security culture. A successful awareness program follows a proven roadmap that enables you to plan, communicate, and measure your efforts. The SANS Security Awareness Maturity Model® enables you to do exactly that.

*Verizon 2024 Data Breach Investigations Report

Security Awareness Roadmap

Managing Your Human Risk

SANS CYBERSECURITY LEADERSHIP

sans.org/cybersecurity-leadership

@secleadership

SANS Security Leadership

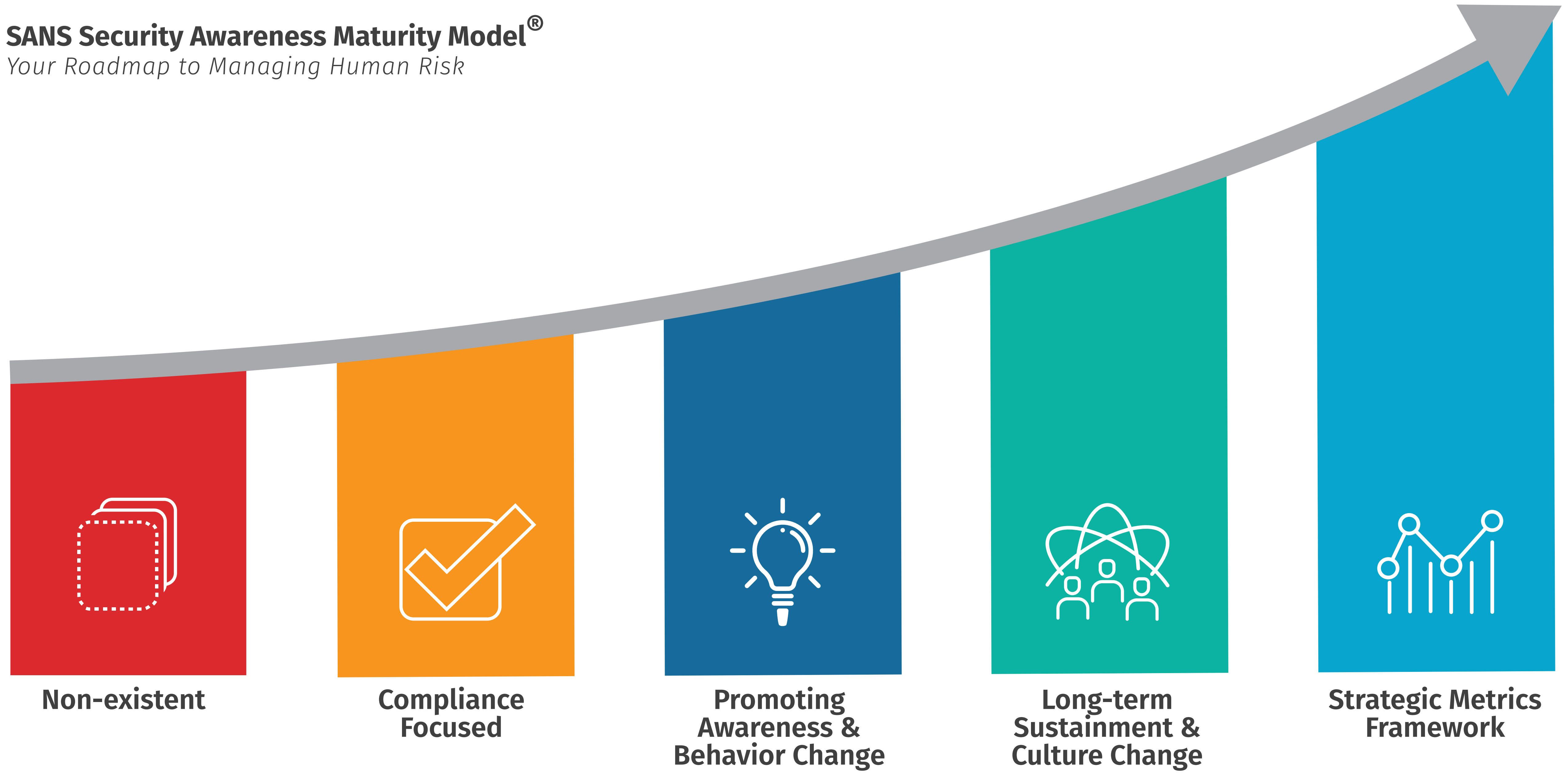
sansurl.com/leadership-youtube

sansurl.com/leadership-discord

SSA_Roadmap-v1.5_01-25
This poster was created by Lance Spitzner with support of the SANS Faculty.

SANS SECURITY AWARENESS

SANS Security Awareness Maturity Model®
Your Roadmap to Managing Human Risk


Non-existent
Compliance Focused
Promoting Awareness & Behavior Change
Long-term Sustainment & Culture Change
Strategic Metrics Framework

Key Elements to a Mature Program

Managing human risk is a people problem, requiring people for the solution.

- **Effective Engagement—**Great programs start with making security personal. Show your workforce why security matters and how it safeguards them and their work. Simplify behaviors so they feel easy and natural to adopt—small steps can create big changes.
- **Empowered Teams with Leadership Support—**Success grows from strong leadership support. When leaders champion security awareness and back it with resources, programs thrive. With a dedicated team leading the charge, security awareness becomes a shared goal everyone can rally behind.
- **Integrated Awareness—**Security awareness is more than compliance—it's a proactive foundation for protecting your people and your organization. Aligning awareness with the security team makes it a powerful part of your overall strategy.
- **Continuous Improvement—**Building a security-aware culture is an exciting journey. Through consistent communication, training, and reinforcement, your workforce becomes more resilient and ready for what's ahead.

Developing Your Career

SANS LDR433: Managing Human Risk™

This three-day class lays the foundation of risk management, changing organization behavior and ultimately managing and measuring human risk. Course content is based on lessons learned from hundreds of security awareness programs from around the world. **sans.org/ldr433**

SANS LDR521: Security Culture for Leaders™

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/ldr521**

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 of failing to meet 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 standards. • 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 its human risk. In some circumstances this stage can be the most dangerous, as leadership perceives the organization is effectively managing its human risk, but it is not.**	• Program is led by someone who is only dedicated part-time to the security awareness efforts. • Security awareness reports to GRC, compliance, audit, legal or human resources. • 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. • There is little coordination or partnership with other departments, such as communications and human resources. • Leadership perceives security as purely a technical issue. • Training is primarily once a year, often mandatory. • 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 perceive security as something that the IT or security team takes care of—it's not their problem. • People feel security is something they have to do. • People have a negative perception of the security team, which is perceived as arrogant, too technical or perhaps even blockers. • People perceive security policies as confusing, difficult and as a blocker to their daily work responsibilities. • People often ignore policies and use their own solutions to get work done.	It depends on the standards, regulations or legal requirements you are attempting to adhere to. However, the overall effort is usually minimal, often requiring nothing more than annual training.	• Number/percentage of people that have completed training • Number/percentage 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, webcasts, etc.)	• Identify and gain support of key leaders and stakeholders • Create Project Charter, identifying things such as scope, leadership, goals, objectives, assumptions, and constraints for the awareness program. • Identify who will be responsible for the awareness program. To ensure greatest success, that person should be dedicated full-time, have strong people skills, and report to and be part of the security team and report to the CISO. • Identify the top human risks you will need to manage. Coordinate with Incident Response team, Security Operations Center, and/or Cyber Threat Intelligence team to assist with this. This may also require some type of human risk assessment. • Identify the key behaviors that will mitigate and manage the top human risks. • Plan how you will communicate to, engage, and train your workforce on these key behaviors. • Develop, resource and/or purchase your training materials and platform to include Learning Management System or a Human Risk Management platform. • Create execution plan with milestones to include metrics.
STAGE 3 Promoting Awareness and Behavior Change	The program identifies the the top human risks to the organization and the behaviors that manage those risks. The program goes beyond just annual training and includes continual reinforcement throughout the year. More mature programs in this stage identify additional roles, departments, or regions that represent unique risks that require additional or specialized role-based training. Content is communicated in an engaging and positive manner that encourages behavior change. As a result, people understand their role in cybersecurity, follow organizational policies and exhibit key behaviors to secure the organization. **VALUE: Your organization is not only meeting its compliance requirements but is able to effectively identify, manage, and measure its human risk.**	• The program is led by someoned dedicated full-time to managing the security awareness program. In addition, this individual often has strong communication/people skills. • Security awareness reports to and is an integrated part of the security team. • Leadership understands and commits to the need for managing human risk. • There is a strategic plan that has identified the scope, goals, objectives, and justification for the program. • Through a risk assessment and in partnership with different security team members (DFIR, SOC, CTI), the security team has identified and can explain the organization's top human risks and the behaviors that most effectively manage those risks. • The program has sufficient leadership support to provide resources necessary and has an executive champion. • The Security Awareness team actively partners and collaborates with various departments within the organization, including communications, human resources, and help desk. • The program goes beyond just annual training and includes continuous reinforcement throughout the year. • More mature programs have identified different departments, roles, or regions that represent increased or unique risks to the organization and require specialized or additional training (role-based training). • The program works to positively engage the workforce. Engagement is not based on mandatory training but creating training that people want to consume.	• Employees understand that technology alone cannot protect them and they have a responsibility to protect themselves and the organization. • People are reporting incidents or suspected attacks. • When the security team pushes out information, people are asking them questions. • Employees are exhibiting the behaviors they are being trained on. • Employees begin to exhibit the same strong security behaviors at home and in their pesonal lives. • Employees are asking how their family can take the training.	Depending on the behaviors you are attempting to change, you can begin impacting behaviors organization-wide within 3–6 months. However, the more behaviors you are attempting to change, the longer it can take to change those behaviors organization-wide. This is one of the reasons it is so important to prioritize 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.	This stage is all about measuring the behaviors you care about and which behaviors are the most important to managing your risk. Some examples include: • Phishing simulation click rates, number of repeat clickers and report rates • Number of lost or stolen laptops or mobile devices • Adoption rate of Password Managers or MFA • Percentage of employee passwords that could be cracked • Percentage of workstations that are securely locked down at night • Percentage of mobile devices that are current and/or screenlocks enabled • Number of accidental data loss events, such as data loss due to auto-complete in email or insecure cloud accounts. **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 the awareness program. • Identify a specific date when the security awareness program is reviewed and updated every year. • During annual review and update, identify any new risks or behaviors required to manage human risk and new ways to communicate to, engage, and train your workforce. • The security awareness team should partner with audit, compliance, or GRC and actively assist with policy development to help ensure they are as simple as possible for the workforce. • The Security Awareness team should be actively assisting the Security team in any outreach, communication and engagement efforts to include any new tool rollouts. • Establish some type of formal incentive program to recognize individuals, groups, or departments excelling in cybersecurity and/or exhibiting key behaviors.
STAGE 4 Long-Term Sustainment and Culture Change	The program has the processes, resources, and leadership support in place for a long-term sustainment, including (at a minimum) an annual review and an 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 the workforce's shared attitudes, perceptions, and beliefs about cybersecurity. **VALUE: Your program has gone beyond impacting behavior and has started building a strong security culture. By security culture, we mean your workforce's shared attitudes, perceptions, and beliefs about cybersecurity. A strong security culture not only creates an environment where people are far more likely to exhibit secure behaviors, but promotes and helps ensure security is built into almost all operational aspects of the organization, exponentially increasing the overall security of the organization.**	• The program is led by someone dedicated full-time to managing the security awareness program and has a team of multiple full-time employees focusing on managing human risk. • Security awareness reports directly to the Chief Information Security Officer (CISO). • Program is actively reviewed and updated on an annual basis. • Leadership believes in and has invested in long-term support of the program. The program lead is regularly updating leadership on a monthly or quarterly basis. • Security team believes in investing in human controls equally as much as technical controls. There is a strong partnership between the security awareness team and different elements of the security team (SOC, DFIR, CTI, etc.). • The security ambassador champions the program and is run by a dedicated program manager. • The Security Awareness team is assisting in the development of security policies, processes, and procedures to ensure they are easier to understand and comply with. • The Security Awareness team is assisting the Security team with all organization-wide security communications or security tool roll-outs ensuring that expectations are simple to understand and easy to use.	• Good security practices are baked into 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 actively reach out to and request assistance or briefings by the Security team. • Department leads and teams request security reviews/audits. • The Security team and their security efforts are perceived as approachable, collaborative, and helpful by the workforce. (e.g., people feel safe reporting an incident, even when they know they caused it).	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 its 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 people's attitudes, perceptions, and beliefs towards information security (this can be broken down by what people think about your security policies, your Security team and your security training). • Conduct focus groups or interviews for deep dives into people's attitudes, perceptions, and beliefs • A number of people/departments are requesting security briefings or updates. • A number of people engaging the security team with questions or submitting ideas on how to improve security.	• Create a metrics dashboard that combines all the information/measurements from the different maturity levels. • Identify and align with leadership's strategic priorities. • Identify and align with any key strategic security frameworks or models.
STAGE 5 Strategic Metrics Framework	The program has a robust metrics framework aligned with and supporting the organization's mission and business goals. The program is no longer just measuring and reporting on changes in behavior and culture, but ultimately how these changes are reducing risk and enabling leadership to achieve their strategic priorities. As a result, the program is continuously improving and able to demonstrate return on investment. **VALUE: Your program is aligned with and actively supporting your leadership's strategic priorities and your organization's business goals/mission.**	• The Security Awareness team works with business leaders to identify and align with their strategic business priorities. • Metrics are collected on a regular basis, often automated. • Metrics are provided to senior leadership demonstrating value at a business level and showing alignment with strategic business priorities. • Metrics are aligned with the security framework(s) that your leadership has committed to, such as NIST Cybersecurity Framework or CIS Critical Controls. • Different types of metrics are delivered to different target audiences. • You have the ability to benchmark your program's maturity against peer organizations in your industry.	Leadership actively requests and uses security awareness metrics to measure their organizational progress and/or compare departments across the organization.	This is a long-term effort aligned with your overall program, as you are continually updating and improving your ability to collect useful metrics that you can both act on and provide to leadership.	• A metrics dashboard that tracks the key metrics covered in the previous stages. In some cases, a Human Risk Management platform may be used to automate the collection and display of these metrics. • How these changes are impacting and reducing overall risk to the organization, which can be measured in strategic metrics such as: - Overall number of security incidents - Average time to detect an incident (attacker dwell time) - Average time to recover from an incident - Number of policy, audit, or compliance violations In addition, show leadership how the awareness program is aligned with and enabling strategic goals in any strategic security frameworks, like the NIST CSF.	

SANS SECURITY AWARENESS

SANS CYBERSECURITY LEADERSHIP