Leveraging the **SANS Security Awareness Maturity Model®** to Effectively Manage Human Risk

SANS SECURITY AWARENESS

Introduction

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.

1 Verizon 2024 Data Breach Investigations Report

The Key to Successful Awareness Programs

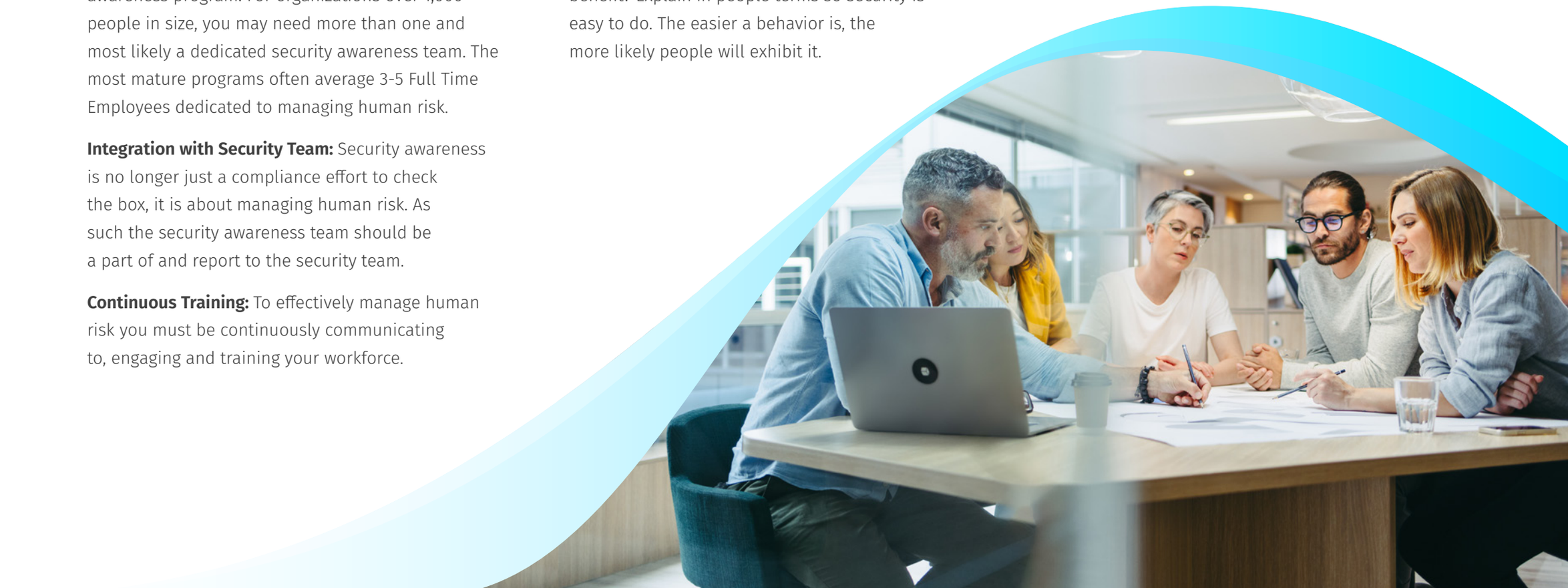
The definition of a mature security awareness program is its ability to effectively manage and measure your human risk. Working with hundreds of organizations at a global level these are key elements to building a strong program.

Team Size: Securing people is a human problem that requires people as the solution. You need to have a person dedicated full-time to leading your security awareness program. For organizations over 1,000 people in size, you may need more than one and most likely a dedicated security awareness team. The most mature programs often average 3-5 Full Time Employees dedicated to managing human risk.

Integration with Security Team: Security awareness is no longer just a compliance effort to check the box, it is about managing human risk. As such the security awareness team should be a part of and report to the security team.

Continuous Training: To effectively manage human risk you must be continuously communicating to, engaging and training your workforce.

Effective Engagement: To effectively engage you must explain to people why they should care, why is security their responsibility and how do they benefit? Explain in people terms so security is easy to do. The easier a behavior is, the more likely people will exhibit it.

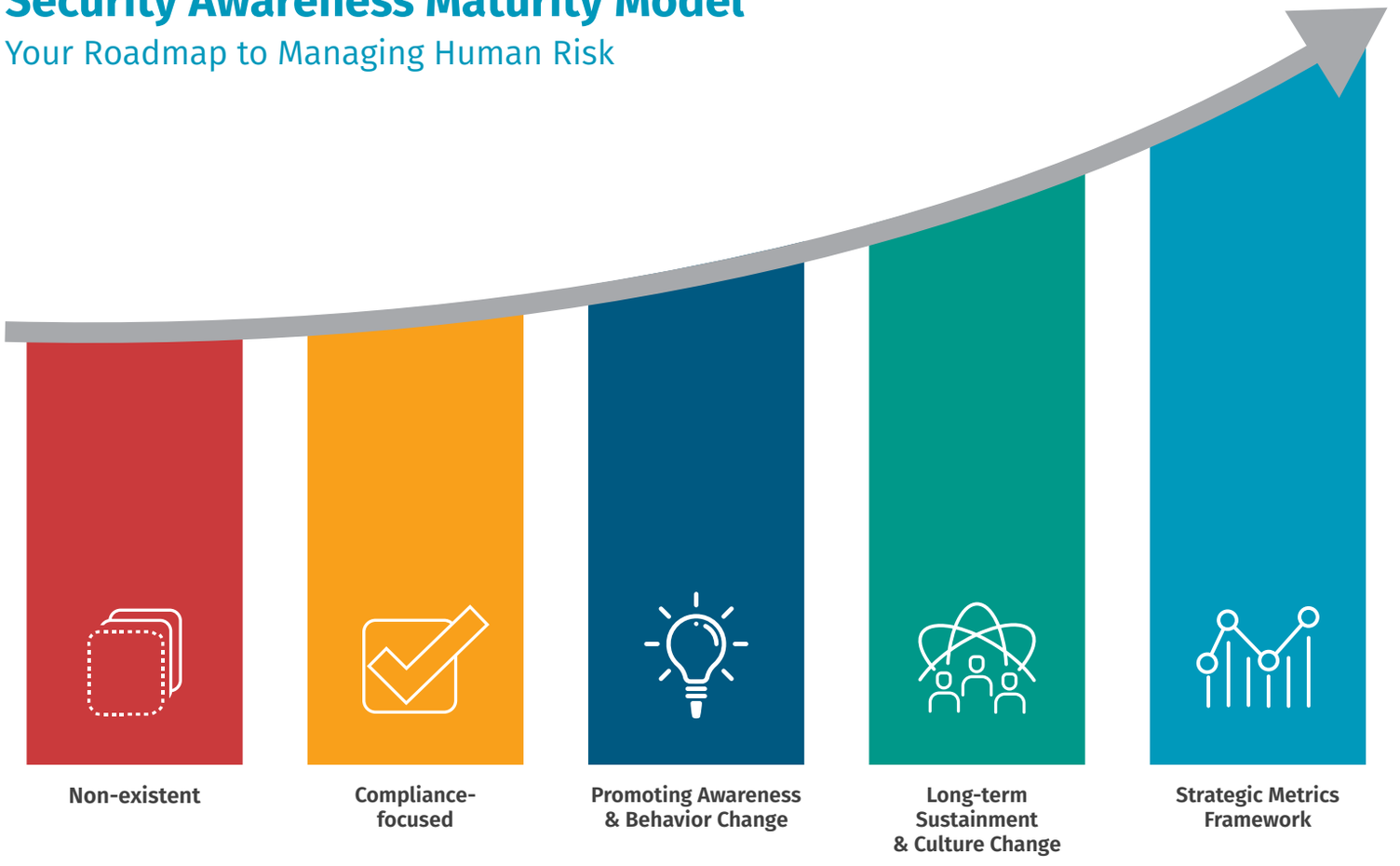


The SANS Security Awareness Maturity Model®

The SANS Security Awareness Maturity Model® is a powerful tool and detailed roadmap for building your security awareness program, no matter what stage your organization is at in your development.

The model helps organizations self-evaluate their current place on the cybersecurity evolutionary scale, learn to develop security operations further, and determine how to communicate strategy and results to leadership and sustain their support.

The following pages not only describe each stage of the model, but also the value of each stage, the indicators to determine which stage you are in, and metrics to use for each stage and steps to achieve the next level. The model is not only a way to benchmark your current program, but a roadmap on how to grow and mature your program.



SANS SECURITY AWARENESS

Stage 1

No Security Awareness

Description

Stage 1 is the most basic level of security awareness. In Stage 1, your security awareness program does not exist. Employees have little knowledge that they could be a target, or what to do if they are, and don't understand that their actions directly impact the organization's security. There are no tracking metrics and no thought given to how the organization can evolve its security awareness.

Value

Unsurprisingly, employees at Stage 1 companies don't know or understand security policies and best practices and are easy victims of cyberattacks. Stage 1 organizations are at an incredibly high risk of failing to meet compliance requirements and being compromised by human-driven security incidents.

Program Indicators

There is no security awareness program and leadership does not discuss security awareness.

People Indicators

Employees discuss security and exhibit secure behaviors extremely rarely or never at all.

Steps to the Next Level

To advance beyond this stage, it's essential to lay the groundwork for a formal security awareness program by identifying the organization's specific needs and gaining leadership support.

- Identify the regulations or standards your organization must comply with.
- Secure the support of key leadership to champion the security awareness initiative.
- Assess current security gaps and potential human risk factors within the organization.
- Develop a basic framework for an awareness program that addresses these risks.
- Begin allocating resources (time, personnel, and budget) to build the program.

Stage 2

Compliance Focused

Description

A security program exists, but is designed to meet specific compliance or audit requirements and nothing more. Training is limited to an annual or ad hoc basis.

Value

Most employees remain unclear about organizational security policies and their role in protecting information assets. Although the program meets legal requirements, the organization remains highly vulnerable to breaches because it is not effectively addressing human risk.

Program indicators

No strategic plan: Training topics are ad hoc and random. Training frequency is usually annual or sporadic.

Limited leadership support: Leadership aims to maintain compliance at minimum costs, with security awareness only considered during audits. Leadership perceives security as purely a technical issue.

Limited resources: The program lead is typically one person with additional (usually primary) responsibilities. Program leadership is a part-time job that often reports to compliance, audit, or governance teams.

Limited coordination: There is minimal coordination with other departments, such as communications or human resources, which limits the reach of security initiatives. Communication to employees is restricted to annual training, with no ongoing engagement.

People Indicators

Because leadership doesn't prioritize security, employees often see security training as just another task to check off their to-do list, viewing it as an IT issue that doesn't directly affect them. Security policies may seem confusing and disruptive to their daily work, leading to frustration. As a result, employees may become disengaged and look for ways to bypass these security rules when possible.

Time to Achieve: Within a Month

Time to achieve depends on the standards, regulations, or legal requirements to which the organization must adhere, but typically is relatively short and the overall effort minimal.

Potential Metrics

The metrics at this stage are basic and typically focus on process rather than effectiveness, including:

- Percentage of employees who have completed training
- Percentage of employees who have signed the acceptable use policy
- Number of on-site training sessions conducted annually
- Number and frequency of security awareness materials distributed (such as newsletters, webcasts, or lunchroom posters)

Steps to the Next Level

Because a strong security-driven culture must start at the top, it isn't easy to evolve your organization past Stage 2 without leadership buy-in.

1. That means your first and most important step is identifying and gaining the support of the right C-suite and management stakeholders.
2. Next, create a project charter identifying essential elements such as scope, goals, objectives, assumptions, and constraints.
3. Identify who is responsible for the awareness program – this person should have a mix of soft and hard skills and be part of the security team – and dedicate them to the job full-time.
4. Create an advisory board, a team of people that can help security awareness professionals plan and maintain the program. Ideally your advisory board has individuals from various departments, including HR, marketing, and the C-suite.
5. Identify the top human risks to address. This may require coordination with Incident Response, the Security Operations Center, or Cyber Threat Intelligence teams, and possibly conducting a human risk assessment.
6. Identify critical behaviors to mitigate these risks and how you'll communicate to, engage, and train your workforce in these behaviors.
7. Create an execution plan that includes milestones and the metrics you'll use to gauge effectiveness (not just process).
8. Develop or purchase your training materials.
9. Have senior leadership announce your security awareness program, ideally at an all-hands meeting.

Stage 3

Promoting Awareness and Behavior Change

Description

Your program identifies and focuses on the target groups and training topics that have the most significant impact on keeping the organization safe. The program goes beyond sporadic or annual training in favor of regular and ongoing engagement, with content encouraging behavior change at work and home communicated effectively.

Value

Employees understand and follow organizational policies and actively recognize, prevent, and report incidents. Your organization meets its compliance requirements and can effectively manage and measure its human risk.

Program indicators

Leadership support and active planning: Leadership understands and has committed to the need for managing human risk, and the program has an executive champion. A strategic plan identifies the project scope, goals, objectives, and reason for being.

Enhanced situational awareness: The security team knows the organization's top human risks and any desired behaviors to manage those risks.

Baked-in security awareness: Security awareness is considered part of the organization's overall security effort. The program lead works full-time on the project, has strong communication skills, and is part of the security team.

Cross-organizational effort: The program lead collaborates with various departments within the organization, including communications, HR, and the IT help desk, typically via the advisory board.

Ongoing engagement: The program works to positively engage the workforce, going beyond annual training in favor of continuous reinforcement throughout the year. Companies at Stage 3 also often conduct phishing and social engineering awareness training.

People Indicators

Employees understand that security isn't just a problem to be left to technology and the IT team and that everyone has a responsibility to protect themselves and the organization's assets.

Employees proactively report any suspected attacks and incidents, and employees are engaged and ask meaningful questions after consuming security awareness information. Employees exhibit the behaviors learned in training during their day-to-day jobs and bring these behaviors home with them.

Time to Achieve: 3-6 months

Most organizations will see organization-wide behavior change within three to six months. For example, focused phishing training and simulations will likely result in a dramatic drop in phishing click-through rates within that period.

However, keep in mind that it's vital to be selective in the number of behaviors you're trying to change. Not only does changing more behaviors take more time, but it can also become a change management issue if not handled properly.

That's why it's important to prioritize your top human risks and the behaviors that help manage those risks. The fewer behaviors on which you focus, the more likely you'll be able to change those behaviors.

Potential Metrics

Stage 3 metrics focus primarily on program effectiveness and ultimately depend on the behaviors you identify as being most important for managing human risk. Keep in mind that at every stage of the maturity model, it's important to add new metrics while continuing to track the metrics implemented in previous stages.

New metrics in Stage 3 include:

- Phishing simulation click and report rates
- Number of infected computers and devices each month
- Number of lost or stolen computers and devices each month
- Number of security policy violations

Steps to the Next Level

Because leadership is already engaged and the program can at least partially demonstrate its effectiveness through meaningful metrics, moving to the next level isn't as complex as the previous stage.

1. Establish regular and engaging leadership updates on the program, its metrics, and effectiveness.
2. Constantly evaluate emerging and changing technologies, threats, business requirements, or standards to include in your program.
3. Conduct regular surveys and assessments to determine the current state of awareness and associated behaviors in the organization.
4. Schedule a comprehensive program review date, where the advisory board can closely examine the program and update elements as necessary.
5. Expand your modalities to scale and even better engage the workforce through initiatives such as ambassador programs, gamification, and open-source intelligence (OSINT) briefs for senior executives.
6. Build outreach and communication efforts into as many security initiatives as possible to build engagement and momentum.

Stage 4

Long-term Sustainment and Culture Change

Description

At Stage 4, your program has become an integral part of your organization's culture. It has the processes, resources, and leadership support necessary to sustain itself indefinitely. The program is dynamic, continuously evolving, and goes beyond simply changing behaviors – it influences employee beliefs, attitudes, and perceptions about security. Security awareness is no longer just a part of operations but is woven into the fabric of your organizational culture.

Value

Your organization easily meets compliance requirements, manages its human risk, and has developed a strong security-driven culture that enables and promotes the success of all other security initiatives in a virtuous cycle. Security is built into almost all operational aspects of the organization.

Program indicators

Strong leadership support: Leadership believes in and has invested in the program for the long term. The program lead actively updates leadership every month, and multiple FTEs work on the program.

Regular reviews and engagement: The program is actively reviewed and updated annually and engages with multiple target groups with unique training requirements (including skills-based training for IT and developers).

A symbiotic relationship: The security team believes in investing in human awareness as much as technical controls, and employees view the security team as a trusted partner in their day-to-day jobs.

Organization-wide engagement: Training modalities, such as security ambassador or gamification programs, engage employees from every department and business unit across the organization.

People Indicators

Good security practices are part of every employee's day-to-day operations and attitudes, with many employees taking the initiative to educate their peers on good security practices. Employees often suggest new ways the organization can improve security.

Departments and business units ask for security briefings and updates, with department leads requesting security reviews and audits and a spirit of competition emerging between departments over who has the best security practices and discipline. The security team and their efforts are perceived positively by the rest of the workforce.

Time to Achieve: 3-10 years

Reaching this level typically takes between three to 10 years of development, depending on your organization's size, complexity, age, and culture. Achieving this requires sustained effort and consistent leadership support to deeply embed security into the organizational fabric. During this stage, we recommend not focusing on changing your organization's culture directly.

Potential Metrics

At Stage 4 of the Security Awareness Maturity Model, security is already a significant cultural driver in your organization. At this point, we recommend aligning any further changes within your organization's existing culture.

New metrics in Stage 4 include:

- Periodic surveys measuring employees' attitudes, perceptions, and beliefs about information security.
- The number of employees or departments actively requesting security briefings or updates.
- The number of employees submitting suggestions for improving security within the organization.
- Attendance rates at optional security events or training sessions.

Steps to the Next Level

Set up a comprehensive metrics dashboard combining all information and measurements from the various maturity levels, combined with technical security metrics, and aligned with the organization's overall mission of tracking progress, measuring impact, and continuous improvement.

Stage 5

Metrics Framework

Description

Stage 5 is the final evolutionary benchmark in the SANS Security Awareness Maturity Model®. At this stage, your program's robust metrics framework is fully aligned with the organization's mission, tracking progress and measuring impact for continuous improvement. Beyond measuring behavior and culture, Stage 5 focuses on how these changes reduce risk and support leadership in achieving strategic priorities. The program can easily demonstrate ROI.

While metrics are important at every stage, Stage 5 emphasizes that a mature program must demonstrate a tangible, measurable impact.

Program indicators

Strong partnership: The security awareness officer, or team, works with business leaders to identify and align with their strategic business priorities

Ongoing analysis with intelligent automation: Metrics are collected on an ongoing basis and consistently scrutinized to reveal patterns and insights. Most organizations automate the data collection function because of the frequency and amount of data collected

Framework integration: Metrics are integrated into reputable, third-party security frameworks such as the NIST Cybersecurity Framework or the latest version of CIS Controls (formerly known as Critical Security Controls).

Refined audience: Different target audiences receive different metrics, depending on relevancy.

People Indicators

Leadership actively requests, uses, and analyzes security awareness metrics to measure organizational progress and compare the effectiveness of individual departments or business units.

Potential Metrics

Metrics include data points from all stages of the maturity model, and should be combined into a single dashboard or user-friendly interface that can provide data visualizations for analysis and stakeholder reporting. Metrics must be measured over time to demonstrate long-term impact and uncover trends that may not be noticeable within time-limited datasets.

Additional Stage-5 metrics can include:

- Number of incidents
- Time to detect an incident
- Time to recover from an incident
- Number of policy, audit, or compliance violations

Mature Your Program With SANS Security Awareness

SANS is the most trusted and largest source for information security training and security certification in the world. Our Security Awareness solutions have been built using SANS expertise to help transform your organization's ability to measure and manage human risk.

End User Training

Results-focused Cybersecurity training to manage human risk

Authored by SANS experts and designed by adult learning specialists, our engaging, modular, and multilingual content reduces training fatigue and increases comprehension by tailoring your security awareness training program to the issues relevant to your organization.

SANS Phishing

Reduce Human Risk with real-world phishing simulation programs

Keep employees at the highest level of security awareness through continuous training and testing. The SANS phishing platform allows you to control every aspect of your phishing awareness program, with pre-configured or customizable phishing tests, just-in-time training, and automated remedial courses.

Specialized Training

Support targeted instruction for focused responsibilities

Cybersecurity training is essential for all. Some sectors require even greater specialized training, such as developing secure web apps, understanding NERC CIP policy requirements, or handling Industrial Control System (ICS) incidents.

Improve Your Organization's Security Awareness with SANS

This guide provides an industry proven benchmark of your organization's current level of security awareness, along with guidelines and roadmap for developing an ever-more sophisticated approach to managing your organization's human risk.

Indeed, any organization – no matter where it currently lives on the maturity scale – can leverage the SANS Security Awareness Maturity Model® to manage, measure, and improve its level of human risk.

You can also leverage SANS' best-in-class security awareness training solutions to accelerate your organization's transformation to a security-driven culture. Expertly created, timely, and comprehensive training is a strong foundation for building a powerful program that embodies all organizational needs and individual learning levels.

SANS Security Awareness: Managing Human Risk Summit

The Managing Human Risk Summit is an annual event hosted by SANS Institute, dedicated to the human element of cybersecurity. It brings together professionals, leaders, and experts in security awareness, human risk management, and behavioral science to explore strategies for reducing cyber risk through human-centered initiatives.

Find SANS training and certifications
Learn more about SANS security awareness training

SANS Cybersecurity Courses & Certifications

SANS LDR433

Managing Human Risk
This intense three-day course equips participants with the tools needed to build a mature awareness program that proactively engages the workforce and delivers measurable results.

The SANS Security Awareness Professional (SSAP)

The SANS Security Awareness Professional (SSAP) credential is designed for individuals responsible for managing or supporting security awareness programs. It provides the foundational knowledge and skills required to create, implement, and assess the effectiveness of such programs within an organization. The first step toward achieving your SSAP credential is completing the three-day SANS LDR433 course on building mature awareness programs.

SANS LDR521

Security Culture for Leaders
Designed for senior security leaders and experienced awareness officers, this advanced five-day course provides the skills, models, and frameworks necessary to build, manage, and measure a strong security culture at your organization.

View the complete list of cybersecurity courses and certifications here.

About SANS

Launched in 1989 as a cooperative for information security thought leadership, SANS' ongoing mission is to empower cybersecurity professionals with the practical skills and knowledge they need to make our world a safer place.

We fuel this effort with high quality training, certifications, scholarship academies, degree programs, cyber ranges, and resources to meet the needs of every cyber professional. Our data, research, and the top minds in cybersecurity collectively ensure that individuals and organizations have the actionable education and support they need.

SANS SECURITY AWARENESS