SANS SECURITY AWARENESS

2021 SECURITY AWARENESS REPORT™

MANAGING HUMAN CYBER RISK

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Security awareness programs have evolved from having a limited compliance focus to becoming a key part of an organization's ability to manage its human cyber risk. The SANS 2021 Security Awareness Report™ analyzes the data of over 1,500 security awareness professionals from around the world to identify and benchmark how organizations are managing its human risk. The goal of this report is to offer analysis and insights as to what makes great programs successful, as well as to provide actionable data to improve your own program. Key findings from this year's report are listed below.

1. Time, not budget, continues to be the top challenge awareness programs face.

According to the data, over 75% of security awareness professionals spend less than half their time on security awareness, implying awareness is too often less than a full-fledged effort.

> **Organizations reporting program success by changing user behavior had on average 2.5 full-time-equivalent (FTE) employees dedicated to awareness.**

Organizations reporting success going beyond behavior change and impacting culture report that they have at least 3 FTEs dedicated to security awareness. To effectively manage human risk, leaders must make long-term, strategic investments in people, just as they would for other security efforts like Vulnerability Management, Incident Response or Security Operations Centers. People, not budget, are key to managing human risk.

2. Majority of program leads are technical in nature, lacking soft skills, such as communications and marketing, continues to limit organizations' ability to effectively engage their workforce.

The data show that security awareness responsibilities are very commonly assigned to staff with highly technical backgrounds who may lack the skills needed to effectively engage their workforce in simple-to-understand terms.

3. Strategic alignment is important.

> **Awareness programs manage human risk; as such, security awareness should be an extension of the security team, as opposed to being a part of and reporting to legal, audit or human resources.**

A new recommendation added this year is that most organizations' security awareness teams should report to and be the responsibility of the security team, reporting directly to the CISO if possible.

To make the most use of this report, you can read it through in its entirety or skip to the sections that are most valuable to you. We have strived to provide not only the data and what the data mean, but also actionable steps you can take to better manage your human risk. In addition, we have added a new section on how security awareness professionals can grow and develop their career, including detailed salary information (a first for our field) and a career development path.

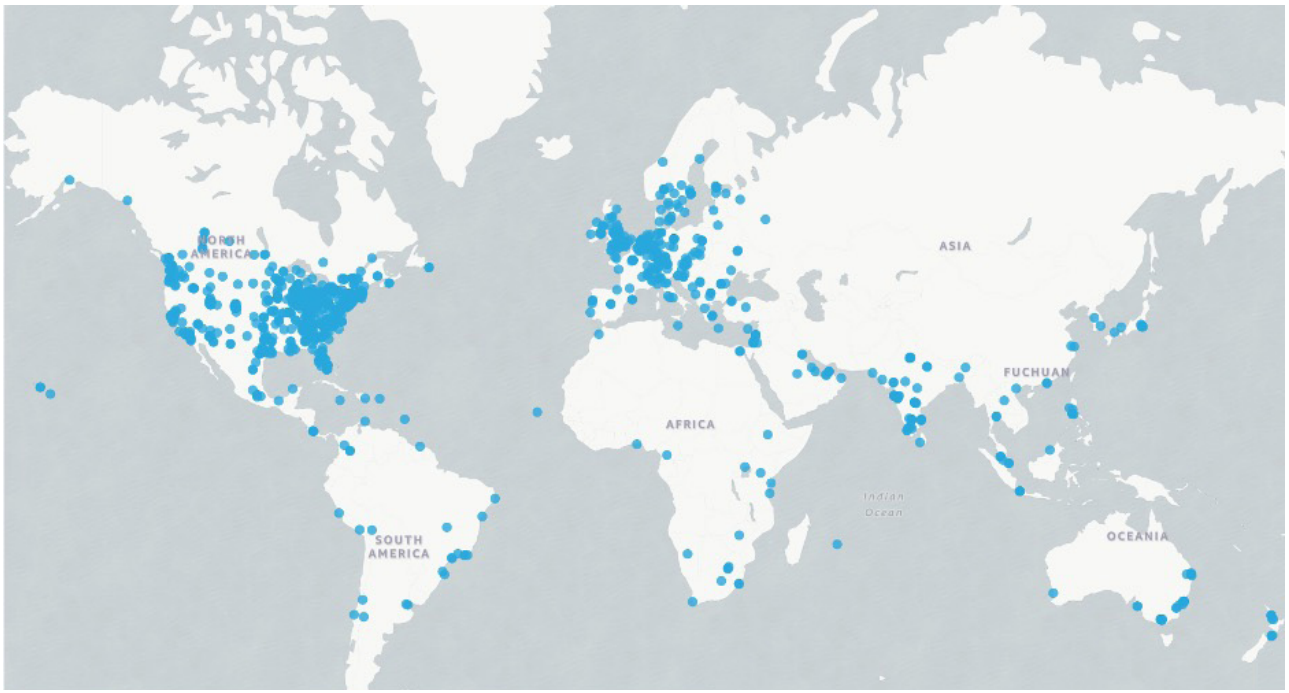
ABOUT THIS REPORT

INTRODUCTION

2021 marks the sixth release of the SANS Security Awareness Report, and through 2020-2021 we have witnessed deep and rapid changes in how and where we work. These changes have caused an unprecedented evolution not only in the technology we use, but in how we use it, especially with so many people now working from home. Simply stated, it has never been more important to effectively create and maintain a cybersecure workforce and a vibrant security culture.

The 2021 annual SANS Security Awareness Report enables organizations to understand their program maturity, improve their security awareness programs and benchmark those programs against others. It includes data-driven analysis of how mature programs are succeeding and identifies opportunities for improvement. For the 2021 report, the SANS Institute conducted a global survey of over 1,500 qualified security awareness professionals from 91 countries.

Global Map of Respondents



CONTRIBUTORS

We would like to recognize the organizations and people who made this report happen, including our partnership with the Kogod Cybersecurity Governance Center at American University. You can find the full biographies of all the authors and contributors at the end of this report. Ultimately this report was developed *by* the community *for* the community.

INFORMATION REQUESTS

If you have any questions or suggestions about this report, we want to hear from you! Drop us an email at SAReport@sans.org or reach us on Twitter at @SANSAwareness using #SecAwareReport.

DEMOGRAPHICS OF SECURITY AWARENESS PROFESSIONALS

Overwhelmingly, respondents reported having been in an information technology or information security role prior to working in security awareness.

Fewer than 20% of this year's respondents have a non-technical background such as communications, marketing, legal, or human resources.

DIGESTING THE DATA

Having a strong technical or security background can be beneficial because it provides familiarity with the common technologies and behaviors that pose a risk to the organization, as well as with threat actors and tactics, techniques and procedures (TTPs). However, being "too technical" can mean that individuals lack the skills to effectively communicate those risks or meaningfully engage employees.

Being overly technical is often referred to as the "curse of knowledge," a type of cognitive bias. The more expertise a person has on a subject, the more difficult it can be for them to teach or communicate it. Security professionals often perceive security as being "simple" because it, and the related technology, is a part of their daily life. Experts can further make assumptions that security and technology are "common knowledge" for everyone else and then build their awareness program based on these misconceptions. As a result, what experts tend to communicate is often confusing, intimidating, overwhelming and difficult for non-experts.

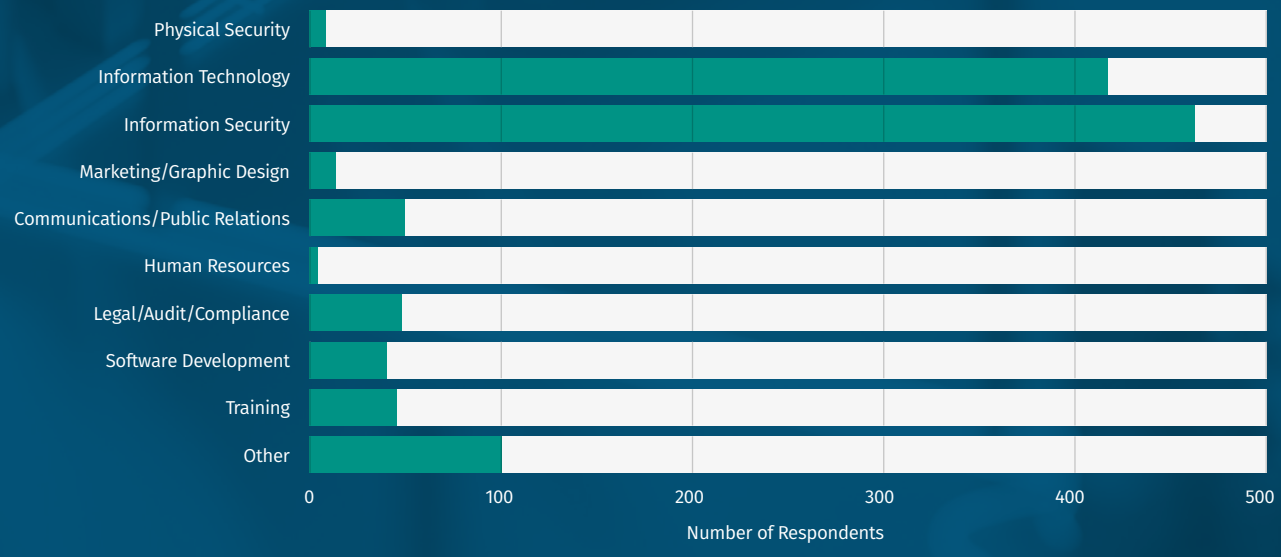
This not only creates less effective training materials, but also impacts communication with peers and leadership and ultimately can create a negative security culture. Thus, technical and security experts should take care to be aware of their "curse of knowledge".

ACTION ITEMS

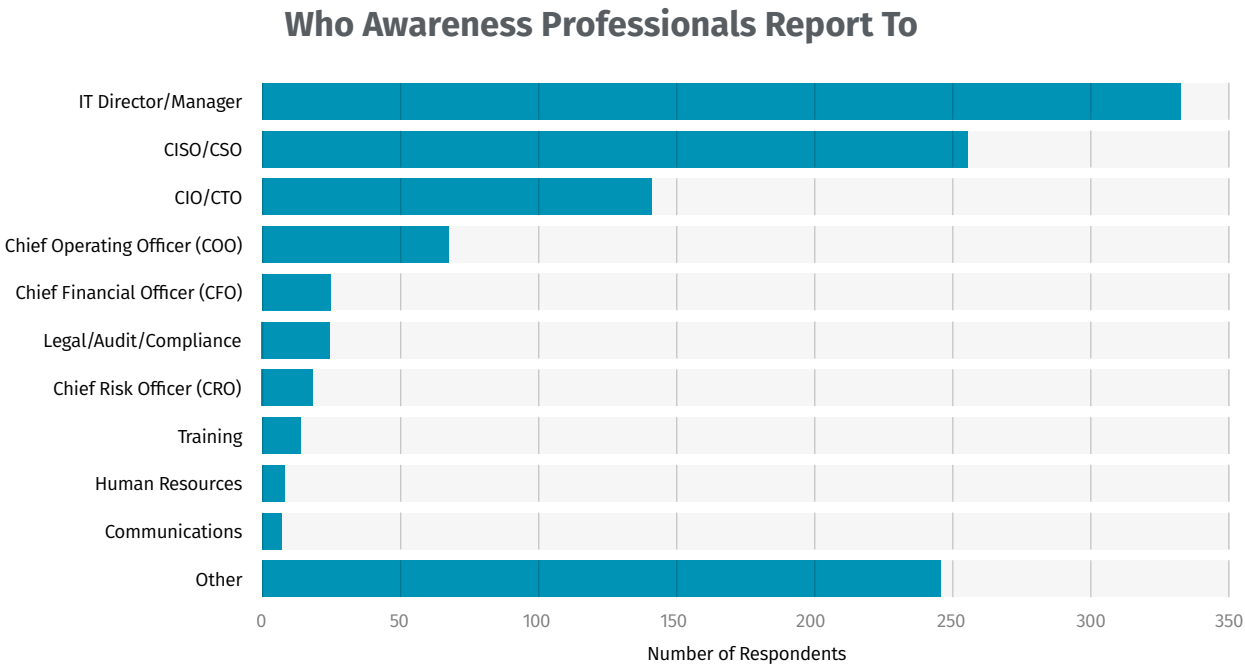
- **Know Your Bias:** If you are highly technical or have a strong security background, make sure you work with others to help craft your messaging. Your expertise is a plus, but security concepts and technologies that are easy for you are most likely difficult, confusing and intimidating for most others. One of the biggest challenges security professionals often face is making security simple for their workforce.

- **Communication and Engagement Skills:** Be sure you have someone on your awareness team who has the skills required for effective communication and engagement. This might mean training someone on your security team, partnering with your communications or marketing department, or even having one of their members embedded into your security awareness team. Or, consider acquiring the appropriate skills yourself to help more effectively engage your workforce. Review Appendix B: Career Development for Security Awareness, Engagement, and Culture Professionals.

Backgrounds of Security Awareness Professionals



THE ORGANIZATIONAL STRUCTURE OF MANAGING HUMAN RISK



Similar to past years, this year's survey found that most security awareness professionals report to the technical side of their organization.

DIGESTING THE DATA

We recommend that an awareness program be managed by a full-time dedicated individual who is part of the security team and reports directly to the CISO. This does not mean that the individual necessarily has maximum technical skills, but it does mean that they are involved in security. This individual would be responsible for helping identify, manage and measure all of the organization's human risk. This individual (or team) would have direct access to the rest of the security team, enabling them to identify and stay current with the organization's top human risks and the behaviors that most effectively manage those risks. In addition, the awareness team can work with the rest of the security team to simplify and communicate policies, processes, procedures and workforce-wide security announcements. Security awareness should be a part of and an extension of the security team, not disconnected from other security efforts.

ACTION ITEMS

- **Maintain Partnerships:** While there are benefits to ensuring that security and technology teams are directly involved with security awareness, it is also essential to develop cross-functional partnerships with other teams, such as Human Resources, in order to successfully deploy training.

- **Properly Define the Role:**

> **A commitment to managing human risks needs to be demonstrated by assigning the overall person in charge a title that aligns with their mission and by ensuring that the individual is part of the security team.**

In other words, a title is needed that focuses on managing human risk. Examples of titles used in organizations include:

- Human Risk Officer
- Security Awareness and Education Manager
- Director of Security Out-Reach and Engagement
- Security Communications and Training Leader
- Security Awareness and Culture Lead

COMPENSATION AND CAREER

For the first time, the Security Awareness Report Survey asked respondents about their compensation[1].

The average annual salary reported was US$103,000.

> **Salaries trended higher for those who were involved in security awareness during only a portion of their work time ($106,000) versus those who were dedicated to security awareness full-time ($96,000).**

A similar relationship was indicated for those who had a technical or security background (higher salary) compared to those without such a background (lower salary).

DIGESTING THE DATA

As this is the first year this question has been posed, a trend analysis cannot be conducted. However, the data suggests that those who work only part of their time on security awareness are often already part of the security or information technology team and often are involved in security awareness in addition to all of their other responsibilities. Their higher salary could be a reflection of their technical skills and/or their primary other roles. Those who are dedicated full-time to awareness may not have such technical backgrounds, or the role of awareness may not be prioritized and therefore be compensated less.

[1] Respondents, and thus salaries reported, are global and encompass a wide array of different industries and countries.

ACTION ITEMS

- **Training:** Review Appendix B: Career Development for Security Awareness, Engagement, and Culture Professionals. Those without a security or technical background may want to train in security fields in order to have a better understanding of the terms, technologies and challenges involved.

  > **Not only will this enable you to better understand your organization's risks and communicate with others about those risks, but you may be perceived as more valuable by your more technical team members.**

- **Reframe the Perception:** Organizations, leaders, and security teams may not perceive security awareness as part of security, or they may perceive security as a purely technical problem requiring a technical solution. To help change these perceptions, focus and speak in terms of managing human risk. Human risk is far more aligned with most organization's strategic security priorities, far more likely to gain leadership buy-in, and far more likely to resonate with a security team. Identify top human risks and the key behaviors that manage those risks. Demonstrate how you can better support the security team with security policies, processes, and priorities. Measure key strategic security metrics that leadership cares about.

MEASURING PROGRAM MATURITY

SECURITY AWARENESS MATURITY MODEL™

Established in 2011 through a coordinated effort by over 200 awareness officers, the Security Awareness Maturity Model™ enables organizations to identify and benchmark the current maturity level of their security awareness program and determine a path to improvement. The most successful and mature security awareness programs not only change behavior and culture but can also measure and demonstrate their value via a metrics framework. The model describes the following security awareness program levels:

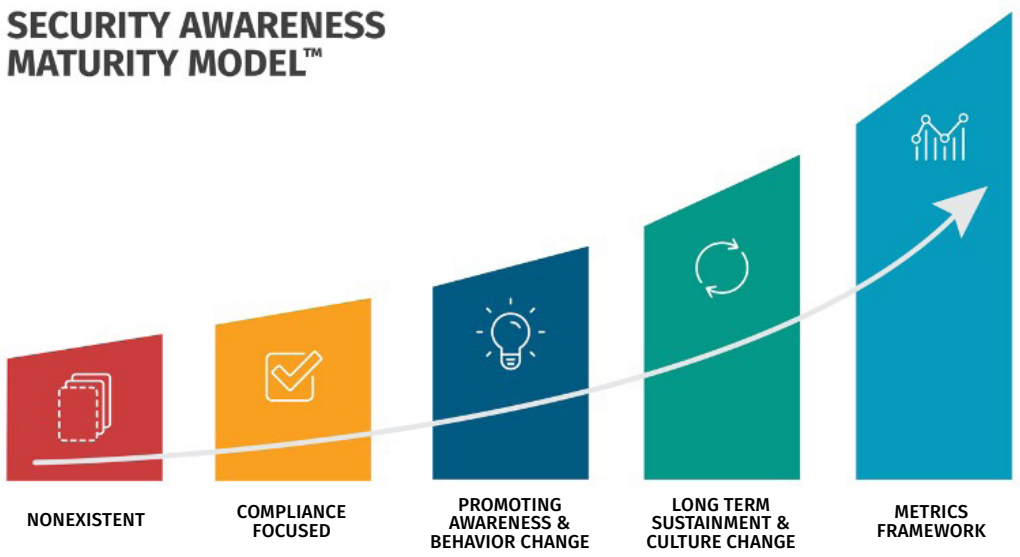
- **Nonexistent:** A security awareness program does not exist in any capacity. Employees have no idea that they are a target, that their actions have a direct impact on the security of the organization, do not know or follow organization policies, and easily fall victim to attacks.

- **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.

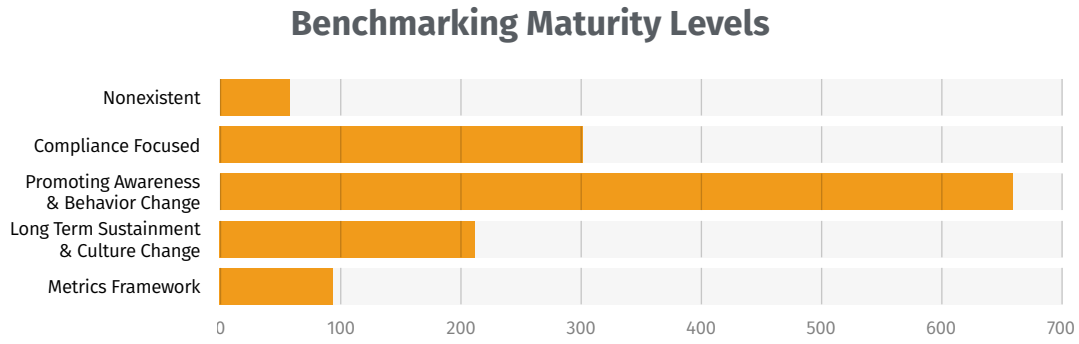
- **Promoting Awareness & Behavior Change:** The program identifies the target groups and training topics that have the greatest impact in managing human risk and ultimately supporting the organization's mission. The program goes beyond just annual training and includes continual reinforcement throughout 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.



While there are multiple ways to leverage the SANS Security Awareness Maturity Model, one of the most common is to benchmark the maturity of your program against others. The majority of respondents (53%) reported that their programs fall squarely in the middle of the Security Awareness Maturity Model that is in the Promoting Awareness & Behavior Change stage.



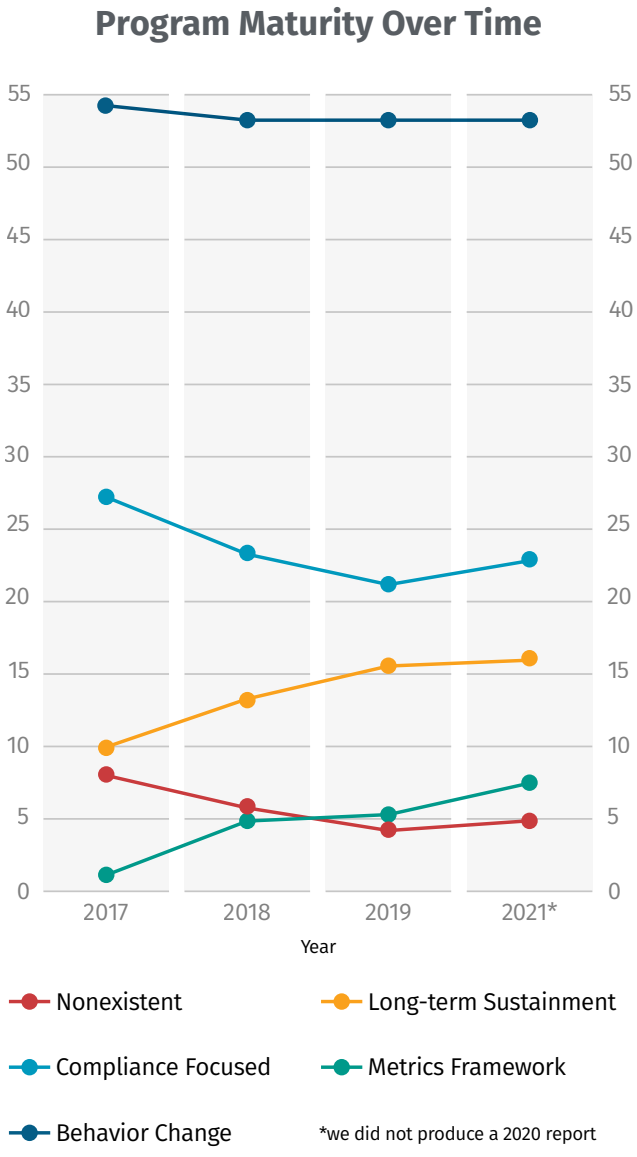
Additional approaches include using the Maturity Model to effectively communicate strategic goals to leadership and as a roadmap outlining the ideal progression of a program. As program maturity reflects multiple aspects of your program, such as frequency, engagement, and measurement, more mature programs are considered much more effective at managing the human risks to cybersecurity.

DIGESTING THE DATA

Over the past four years respondents report that program maturity is increasing. Those stating that their security awareness program is immature – defined as a Nonexistent or Compliance-Focused programs – have decreased by approximately 4%. Concurrently, there's been a consistent year-over-year increase in respondents identifying their program to be at a level of increasing maturity – defined as Long-Term Sustainment & Culture Change (from 9.8% to 15.71%) or Metrics Framework (.08% to 7.26%).

ACTION ITEM

Use the Security Awareness Maturity Model Indicators Matrix included in Appendix A to determine your program maturity level. Look to the rest of this report to help identify the steps to help mature your program.



PREDICTING SUCCESS

ADDRESSING PROGRAM SUPPORTERS AND BLOCKERS

A key component of a mature awareness program's success is a strong partnership and working relationship with key departments within the organization. Awareness programs typically receive strong support from departments such as Security, Information Technology, Human Resources, and Audit, and from senior leadership. These supporters often provide assistance, approval, or resources to enable the program's execution.

DIGESTING THE DATA

In contrast, awareness programs also must work with departments that restrict their ability to execute, which we'll call "blockers." Many programs reported that Operations and Finance departments are common blockers.

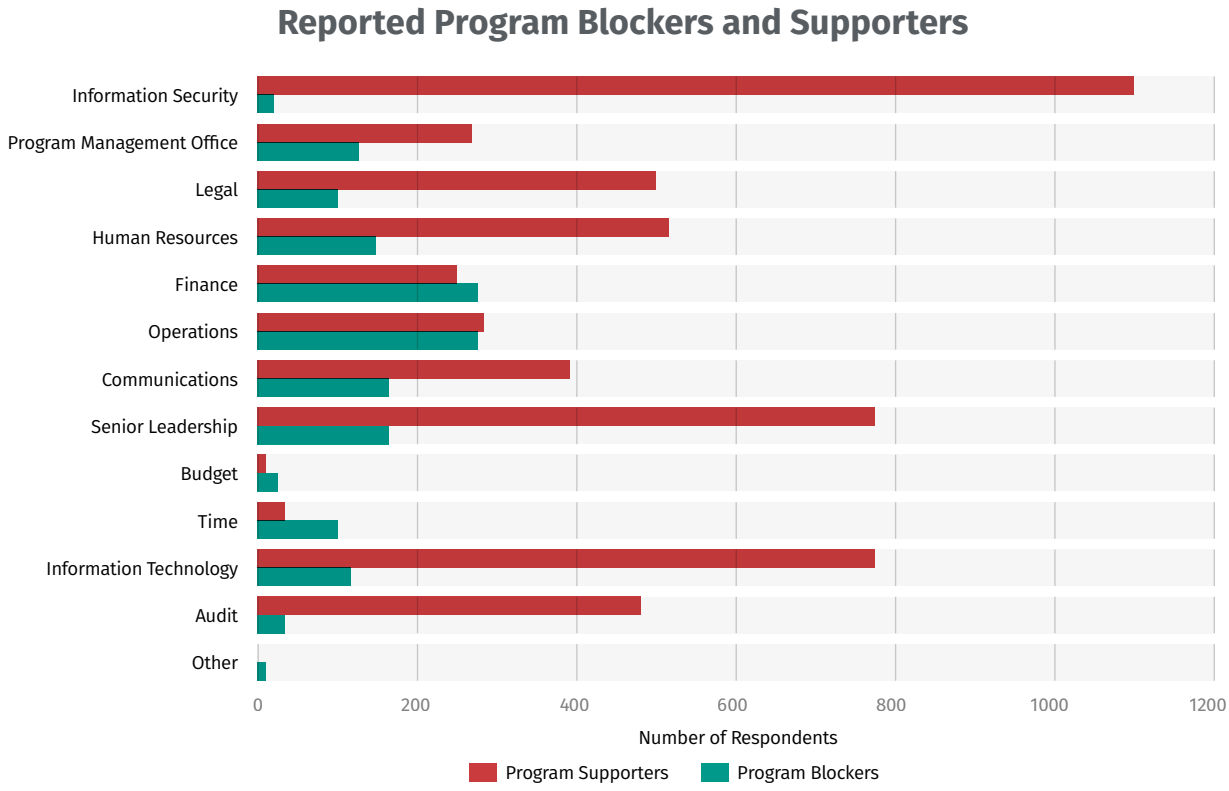
Because most awareness programs have significant budget and operational impact, it is not surprising that these are the top reported blockers.

ACTION ITEMS

Here are some steps you can take to deal with blockers. Remember, you may not always have to convert a blocker into a supporter. In some cases, simply converting a blocker to "neutral" status is enough to clear the path for your program to succeed.

- **Finance:** Justify associated training costs by not only demonstrating the impact of a training program, but also the value of that impact on the overall organization and the program's mission. Consider analyzing costs due to past breaches, compliance failure, or to meet partner or vendor security requirements. Compare this to the cost of the security awareness program you intend to roll out, demonstrating that by investing in security awareness you can dramatically reduce those other costs.

- **Operations:** Simplify awareness programs wherever possible to minimize the operational impacts, including lost work hours due to training, the politics of mandatory training, and the complexity of program operations. This can be done by reducing the topics you focus on to those that are of great concern to your organization. Also involve the Operations team in your planning process and consider adding them to your Security Awareness Advisory Board. Make sure your Operations team has an active voice in how and when your program is rolled out.

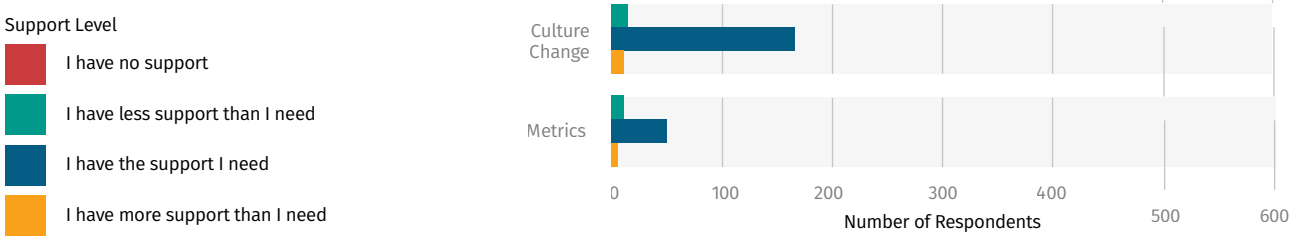


- **Executive Level:** Ask a senior leadership champion who is a proponent of the security awareness program for guidance on how to best engage or handle specific blockers. They can often provide a different perspective on how to handle your challenges or can approach the blocker on your behalf.

- **Develop Metrics:** Program metrics related to human risk can help promote a common understanding that awareness training programs are necessary and allow program costs to be balanced against risk.

GAINING LEADERSHIP SUPPORT

Respondent data shows a correlation between executive support and program maturity. As organizational leaders often decide on critical program resourcing, identification of program goals, training time allocation, and program enforceability, executive support is a key ingredient in program success.



DIGESTING THE DATA

Consistent with five years of data collection and research, leadership support is a key variable in predicting a security awareness program's success.

ACTION ITEMS

- **Talk in Terms of Risk:** Far too often, security awareness is perceived as a compliance effort. Use terms that resonate with your leadership and demonstrate support for their strategic priorities. Instead of talking about engagement and awareness, use terms such as managing human risk.

- **Quantify the Risk:** Security reports, meaningful data and statistics help demonstrate to leadership the need to address human risk and how other organizations are actively leveraging awareness programs to effectively manage their human risk. One such report is the annual Verizon DBIR, which identified the human element as the top driver for both incidents and breaches at a global level. Another option is joining and working with industry security groups, such as your industry's ISAC (Information Sharing and Analysis Center).

- **Make the Most of a Breach:** Never let a breach go to waste – they are powerful motivators and teaching tools. If your organization had a recent incident that was human-related, use that to help drive the justification for your program. Another option is work with your Security Operations Center (SOC) or Incident Response (IR) team and document all human-related incidents over the past six months and the related costs. Don't have any breaches? Use breaches that have occurred within your industry or at other similar organizations.

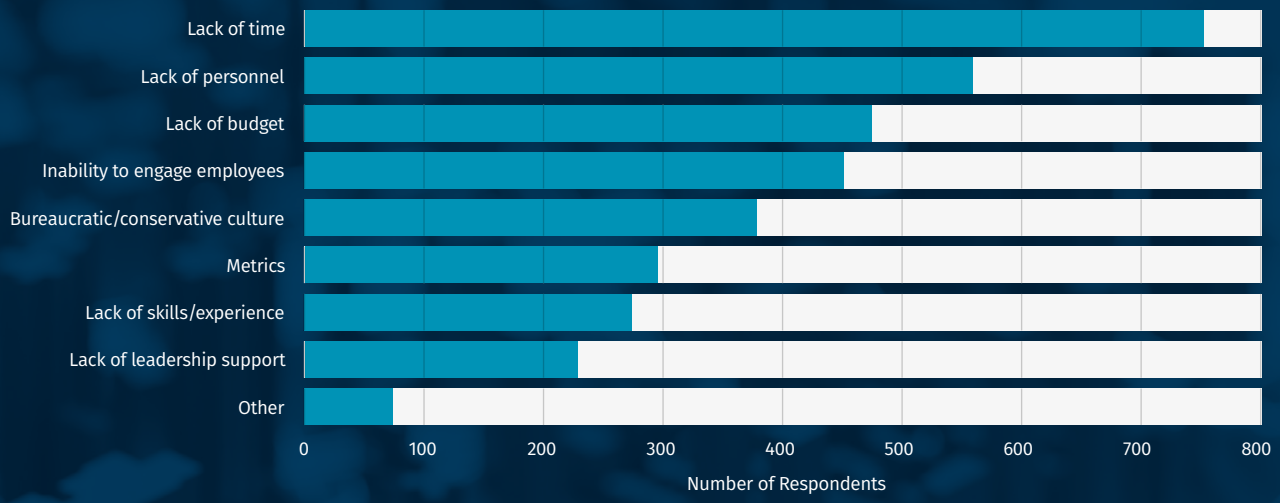
- **Communicate the Benefits:** Dedicate at least four hours a month to collecting and communicating the impact of your awareness program to your leadership. Enable them to better understand and regularly see the value your program is providing. Not sure what metrics to collect? Download the **SANS Security Awareness Metrics Matrix.**

- **Make a Business Case:** Present all these concepts to management as a business case. Download and use the **SANS Security Awareness Leadership Presentation** to explain to leadership what human risk is, how awareness programs effectively manage human risk and support your organization's security priorities, and how these programs align with the overall strategy of the organization.

MAXIMIZING MINIMAL TIME

The two top reported challenges for building a mature awareness program were the lack of time to manage the program and a lack of personnel to work on and implement the program.

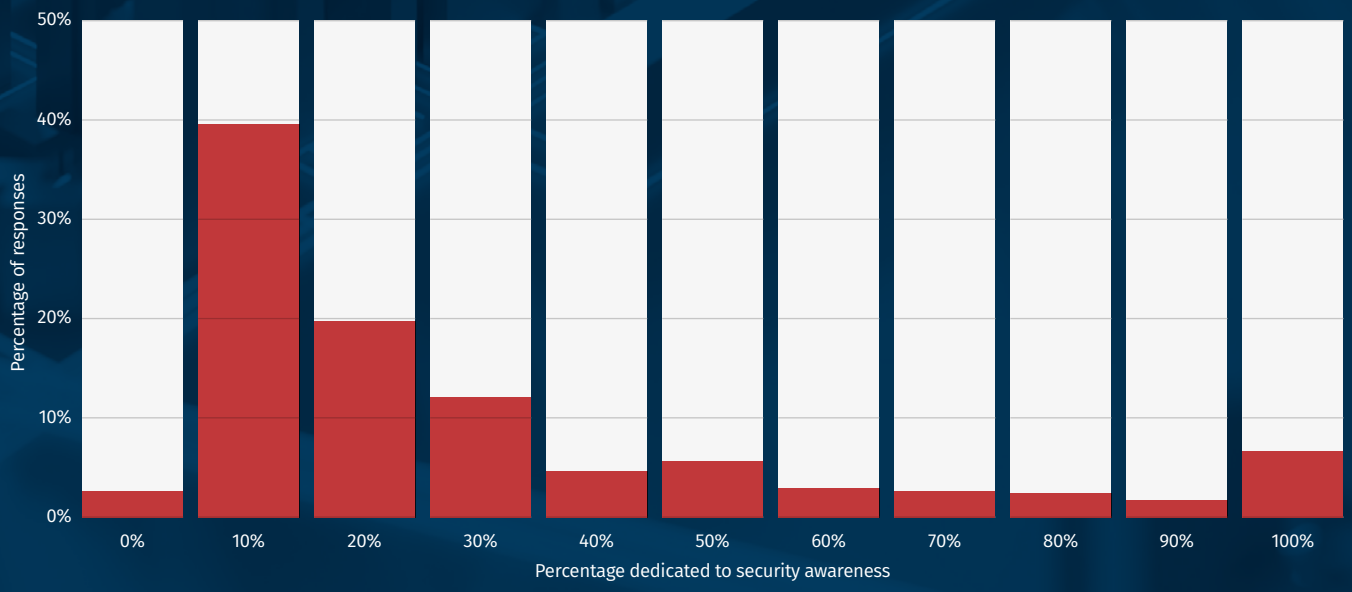
Top Reported Program Challenges



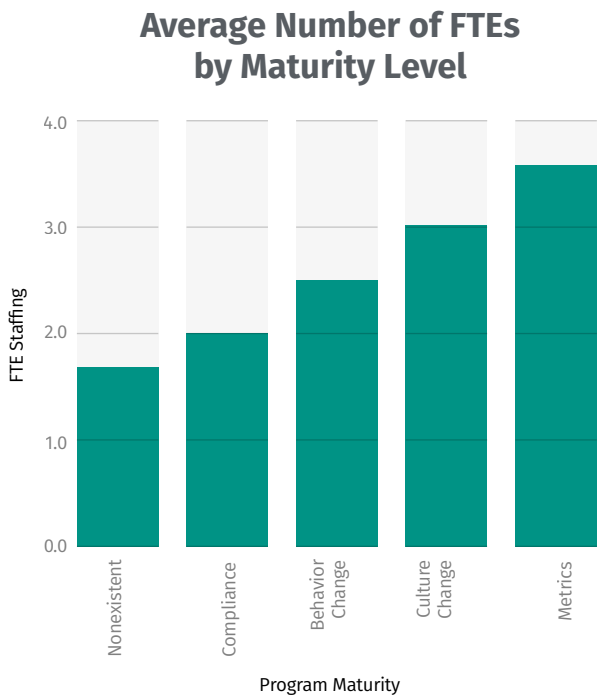
This challenge was further demonstrated when we asked people on average how much time they spend on security awareness.

Over 80% of security awareness professionals reported that they spend half or less of their time on awareness, indicating far too often that security awareness is a part-time effort.

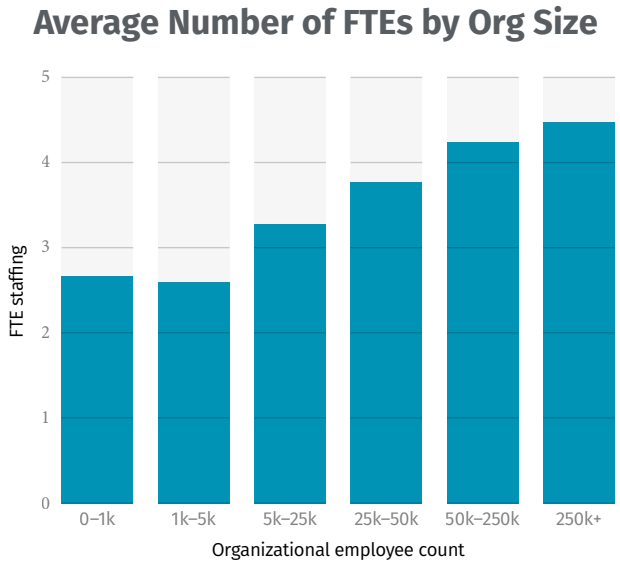
Percentage of Time Spent on Security Awareness



We then wanted a better understanding of just how many people it takes to build and maintain a mature awareness program, using full-time equivalents (FTEs) as a measure. For example, if you have three people each dedicating half (50%) of their time to your awareness program, that will total 1.5 FTEs dedicated to your awareness program. The survey data revealed a strong correlation to the amount of people dedicated to running an awareness program to the maturity of an awareness program and indicated a nearly linear relation between the two.



Below is the same breakdown, but by organization size. Here again, there is a nearly linear relationship between the number of staff working on security awareness programs and the employee count.



DIGESTING THE DATA

It appears difficult to grow a mature program beyond compliance without some number of full-time staff, so you should consider aligning staffing with your maturity goals.

The number of FTEs required will vary, not only with workforce size, but with the complexity and diversity of an awareness program as well. While a basic awareness program covering essential training for a large company may require more staff as the company size grows, companies with diverse training needs, regional awareness programs involving multiple business units, languages, etc., will involve many more staff. The data indicates that larger organizations have more FTEs not just because of the larger workforce, but because they are often doing more within their program, such as more diverse engagement efforts, advanced metrics reporting, host multiple security awareness events, and ambassador programs.

ACTION ITEMS

- **Increase Staffing:** Consistent with initiatives like Incident Response, Vulnerability Management or Security Operations Center activities, managing human risk requires strategic, long-term investments in people. Program sponsors should consider further investments in security awareness staffing.

- **Buy Time:** Use your budget to buy yourself time. Don't create a monthly newsletter yourself, contract someone to do it for you or license materials from a vendor. Instead of creating a survey, hire a contractor that specializes in social science. Don't build the solution yourself; rather, see if there is a solution you can buy or license. The more you are able to delegate, the more time you have to create partnerships within your organization, engage with others and ultimately drive change with your program.

- **Build Partnerships:** Reach out to other teams/departments such as Marketing, Graphic Design, Communications or Security Operations. Partnering with other teams will amplify your reach and allow you to drive adoption of the behaviors you wish to promote.

- **Define Resources:** Identify the roles or specialties you need to execute your program plan. For example, will you need someone with a communications background, a graphic designer or an expert in developing surveys? Once you define their roles and estimated the time involved, conduct a cost-benefit analysis demonstrating why leadership should invest in these people and doing so will ultimately enable you to better manage your organization's human risk.

- **Train:** Train the people you do have to be more effective. Refer to Appendix B: Career Development Path for Security Awareness, Engagement, and Culture Professionals.

SUMMARY OF KEY ACTION ITEMS

- **Have the Right People:** You need 2.5 FTEs to begin changing behavior at an organizational level.

  > **To achieve a truly mature program, including a strong metrics framework, you will need at least 3.5 FTEs.**

  FTE numbers may vary depending on organizational size, structure, and requirements.

- **Provide the Right Title:** Demonstrate organizational commitment to the program, not only by having someone dedicated full-time but also by ensuring they have a title that aligns with the program's goals. In other words, have a title that is focused on managing human risk.

- **Ensure Leadership Support:** Pressure is one of the most effective means to obtain leadership support. Demonstrate to your leadership how other organizations in your industry have mature awareness programs and continue to invest in them.

- **Encourage Partnerships:** Build partnerships and collaborate with others in your organization. This is especially important for any key departments that are blockers, such as Finance or Operations. Get key stakeholders involved in the planning process from the beginning.

- **Buy Time:** If you have the budget, use it to buy yourself time. For example, buy or license materials rather than create your own.

- **Know Your Bias:**

  > **If you are a technical or security expert, make sure you work with others to create clear messaging.**

  Your expertise is a plus as long as you pay careful attention to how it contributes to your program.

- **Improve Communication and Engagement Skills:** Be sure you have someone on your awareness team who has the skills required for effective communication and engagement.

- **Seek out a Champion:** Find a strong champion within leadership. Have that leader help you better understand certain blockers, communicate the value of your program to other leaders, or help you craft your message in the language that business leaders understand and act on.

- **Take Security Training:** Review Appendix B: Career Development for Security Awareness, Engagement, and Culture Professionals.

  > **Security training will provide you a better understanding of risks and the different technologies, frameworks and approaches to managing them, helping build both your credibility and value.**

- **Improve Perception:** Focus and speak in terms of managing human risk. Human risk is far more aligned with most organizations' strategic security priorities, and it is far more likely to gain leadership buy-in and resonate with a security team.

  > **Identify top human risks and the key behaviors that manage those risks.**

  Demonstrate how you can better support the security team with security policies, processes, and priorities. Measure key strategic security metrics that leadership cares about.

APPENDIX A: MATURITY MODEL INDICATORS MATRIX

Click here to download a digital copy of the Maturity Model Indicators Matrix. The digital version is much easier to read, share with others and customize your needs.

APPENDIX B: CAREER DEVELOPMENT FOR SECURITY AWARENESS PROFESSIONALS

One of the key takeaways from the 2021 report is that your compensation is in part driven by your training and skills, including your understanding of key security topics and the technologies involved. Rightly or wrongly, technical staff are often perceived as more valuable, and improving your technical skills can improve your ability to interact with your technical colleagues. As such, based on the data and findings we have defined a training path to help develop the skills you need to be more successful and be compensated adequately.

WHERE TO START

If you are new to the world of information security and/or security awareness, or haven't had the chance yet, the very first SANS course you may want to start with is:

- **MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program:** This two-day class lays the foundation of security awareness, managing human risk and ultimately changing organization behavior. For those of you new to security, you will learn concepts like risk, risk management, and risk analysis. For those of you new to communications and engagement, you will learn key concepts such as the AIDA model, Start with Why, Curse of Knowledge, and other models and principles. Course content is based on lessons learned from hundreds of security awareness programs from around the world. In addition, you will learn not only from your instructor, but from extensive interaction with your peers. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

WHAT NEXT

Once you have the basics down and want to develop yourself and your career, you may need to develop your security expertise if you do not have a technical or security background. Understanding the fundamentals will not only help you better understand the risks, but also the behaviors that manage those risks and empower you to more effectively communicate with your security team and security leadership. There are two different five-day courses to consider at this stage in your career. Each has its advantages, depending on what you hope to achieve.

- **MGT512: Security Leadership Essentials For Managers:** This course empowers you to become an effective security manager and get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. To accomplish this goal, MGT512 covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls are covered in conjunction with key management topics that address the overall security lifecycle. This also includes governance and technical controls focused on protecting, detecting, and responding to security issues.

- **SEC301: Introduction to Cybersecurity:** Jump-start your security knowledge by receiving insight and instruction on critical introductory topics that are fundamental to cybersecurity. This five-day course takes a technical approach for those new to cybersecurity. It covers everything from core terminology to the basics of computer function and networks, security policies, password usage, cryptographic principles, network attacks and malware, wireless security, firewalls and many other security technologies, web and browser security, backups, virtual machines and cloud computing. All topics are covered at an introductory level. The hands-on, step-by-step teaching approach enables you to grasp all the information presented, even if some of the topics are new to you. You'll learn real-world cybersecurity fundamentals to serve as the foundation of your career skills and knowledge for years to come.

Not sure which one of these two courses to take? If you are looking for more of a high-level or management perspective to the world of information security, we recommend MGT512. If you want a more hands-on, technical introduction to the tools and technology of cybersecurity, then we recommend SEC301.

INTERMEDIATE LEVEL

Once you have 2-4 years of experience in security awareness and feel confident in the concepts of both cybersecurity and organizational behavior, MGT521 is what we recommend next.

- **MGT521: Driving Cybersecurity Change - Establishing a Culture of Protect, Detect and Respond:** Cybersecurity is no longer just about technology - it is ultimately about organizational change. Change in not only how people think about security but what they prioritize and how they act, from the Board of Directors on down. Organizational change is a field of management study that enables organizations to analyze, plan, and then improve their operations and structures by focusing on people and culture. SANS MGT521 will teach leaders how to leverage the principles of organizational change, enabling them to develop, maintain and measure a security-driven culture. Through hands-on, real-world instruction and a series of interactive labs and exercises in which you will apply the concepts of organizational change to a variety of different security initiatives, you will quickly learn how to embed cybersecurity into your organizational culture.

ADVANCED LEVEL

Once you have 5-7 years of experience and want to truly develop your security leadership skills, consider SANS MGT514. This will walk you through the strategic planning process and challenges CISOs face. Many people consider this the "CISO Course", that helps develop new and experienced Chief Information Security Officers to become better security leaders. By better understanding CISO challenges, priorities and concerns, you can more effectively collaborate with them and communicate in their terms and language.

- **MGT514: Security Strategic Planning, Policy, and Leadership:** This course gives you tools to become a security business leader who can build and execute strategic plans that resonate with other business executives, create an effective information security policy, and develop management and leadership skills to better lead, inspire, and motivate your teams.

By actively growing your skills and knowledge, you can not only become a more effective leader, but also dramatically improve and broaden your career opportunities.

ACKNOWLEDGEMENTS

This report is developed *by* the community *for* the community We would like to thank everyone who contributed to this effort, including the team at the Kogod Cybersecurity Governance Center (KCGC) who assisted with the analysis of the data. The KCGC is a research initiative of American University's Kogod School of Business (KSB) focused on the governance and management of cybersecurity.

AUTHORS

Dan DeBeaubien

Product Director, SANS Security Awareness

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. Dan joined SANS in 2014 and serves as the Director of Business Technology focusing on SANS digital products and security awareness product strategy.

Lance Spitzner

Community Director, SANS Security Awareness

Lance Spitzner has over 25 years of security experience in cyber threat research, security architecture 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 security awareness and culture programs to manage their human risk. Lance is a frequent presenter, serial tweeter (@lspitzner) and works on numerous community projects. Before information security, Lance Spitzner served as an armor officer in the Army's Rapid Deployment Force and earned his MBA from the University of Illinois.

KEY CONTRIBUTORS

Heng Xu

Director for Kogod Cybersecurity Governance Center and Professor of Information Technology and Analytics at American University's Kogod School of Business

Dr. Heng Xu is a Professor of IT & Analytics at the American University's Kogod School of Business, where she also serves as the Director for the Kogod Cybersecurity Governance Center. Before joining the Kogod Cybersecurity Governance Center, Dr. Xu had both an academic and government background, serving as a professor at Penn State University for 12 years, as well as a program director at the U.S. National Science Foundation (NSF) for 3 years. Dr. Xu's current research focus is on information privacy, data ethics, and data analytics. Her work has received many awards, including the NSF Career Award in 2010, the Operational Research Society's Stafford Beer Medal in 2018, the IEEE ITSS Leadership Award in Intelligence and Security Informatics in 2020, and many best paper awards and nominations at various leading research conferences.

Nan Zhang

Professor of Information Technology and Analytics at American University's Kogod School of Business

Dr. Nan Zhang is a Professor of IT and Analytics at the American University's Kogod School of Business. Dr. Zhang is a world-renowned expert on database systems and data analytics, having published over 100 research papers and served as a program director at the U.S. National Science Foundation (NSF) for both fields. Before joining Kogod, Dr. Zhang was a Professor of Information/Computer Science at Penn State University, George Washington University, and UT Arlington. He has received several awards for his work, including the Communications of the ACM Research Highlight in 2020, the ACM SIGMOD Research Highlight Award in 2019, the NSF Career Award in 2008, and many best paper awards and nominations at various leading research conferences.

ABOUT SANS SECURITY AWARENESS

Since 1989, the SANS Institute has been the leading cooperative research and education organization in the field of information security. Through intensely high-quality training, certifications, degree programs, cyber ranges, and thousands of tools and resources published daily, SANS empowers cybersecurity professionals with the practical skills needed to help secure our world. More than 60 courses are the core of the SANS curriculum. The courses have been developed by respected industry leaders across all cybersecurity practice areas, including defense and blue team operations, offensive operations, incident response, digital forensics, cloud security, and cybersecurity leadership.

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 cybersecurity risk. SANS Security Awareness has worked with over 1,300 organizations and trained over 6.5 million people around the world. The SANS Security Awareness program offers globally relevant, expert authored tools and training to enable individuals to shield their organization from attacks and a fleet of savvy guides and resources to work with you every step of the way.

To learn more, visit
www.sans.org/security-awareness-training

SANS SECURITY AWARENESS