SANS SECURITY AWARENESS

SANS 2022 Security Awareness Report™

Managing Human Risk

Table of Contents

Executive Summary

People have become the primary attack vector for cyber attackers around the world, so humans rather than technology now represent the greatest risk to organizations.[1] Security awareness programs, and the professionals who manage them, are key to managing that human risk. The SANS 2022 Security Awareness Report analyzes data provided by more than a thousand security awareness professionals from around the world to identify and benchmark how organizations are managing their human risk. The goal of this data-driven report is to provide actionable steps and resources to enable organizations to mature their awareness programs and benchmark them against others.

This report is divided into two sections. The first section looks at how to grow and mature your security awareness program. It provides not only the data and what the data mean, but also actionable steps you can take to better manage your organization's human risk. The second section focuses on how security awareness professionals can develop their skills and grow their career, including information about salaries and career development paths. In addition, the report includes the Security Awareness Maturity Model Indicators Matrix, which enables you to easily identify your security awareness program's maturity level and presents steps to improve on that level of maturity and key metrics to measure it.

[1] See Lance Spitzner, "Verizon Data Breach Incident Report Insights," SANS Blog, June 9, 2022, at https://www.sans.org/blog/2022-verizon-dbir-what-does-it-mean/

Key Findings

Maturing Your Program

This year's report once again identifies what we have seen over the past three years: that the most mature security awareness programs are those that have the most people dedicated to managing and supporting it. These larger teams are more effective at working with the security team to identify, track, and prioritize their top human risks, and at engaging, motivating, and training their workforce to manage those risks. The key to gaining leadership support to facilitate this success is to demonstrate how awareness programs are no longer just annual training to check the compliance box but are critical for organizations to effectively manage their human risk.

Growing Your Career

For the second year in a row, this report identifies a large pay gap between those who are dedicated part-time versus full-time to security awareness. Those dedicated part-time to security awareness are paid as much as $30,000 more annually than those who work at it full-time, as they are often compensated more for their other, more technical responsibilities. Awareness professionals can grow their career (and compensation) by developing their skills not only in communication and training, but also in the fundamentals of cybersecurity and how to work closer with and better support their security team.

Measuring Program Maturity

A key goal of this report is to enable you to build and manage a mature security awareness program. By mature, we mean an organization's ability to effectively identify, manage, and measure its human risk. To measure the maturity of awareness programs, we leverage the Security Awareness Maturity Model. Established in 2011 through a coordinated effort by more than 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 mature security awareness programs not only change their workforce's behavior and culture, but also measure and demonstrate their value to leadership via a metrics framework. You can easily determine your program's maturity level (and how to improve it) by using the Maturity Model Indicators Matrix, included separately with this report. The maturity levels are as follows:

Non-existent

There is no security awareness program in any capacity. Employees have no idea that they are a target or 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 provided on an annual or ad hoc basis. Security awareness professionals are disconnected from and do not work with the security team. Employees are unsure of organizational policies and/or their role in protecting their organization's information assets.

Promoting Awareness and Behavioral Change

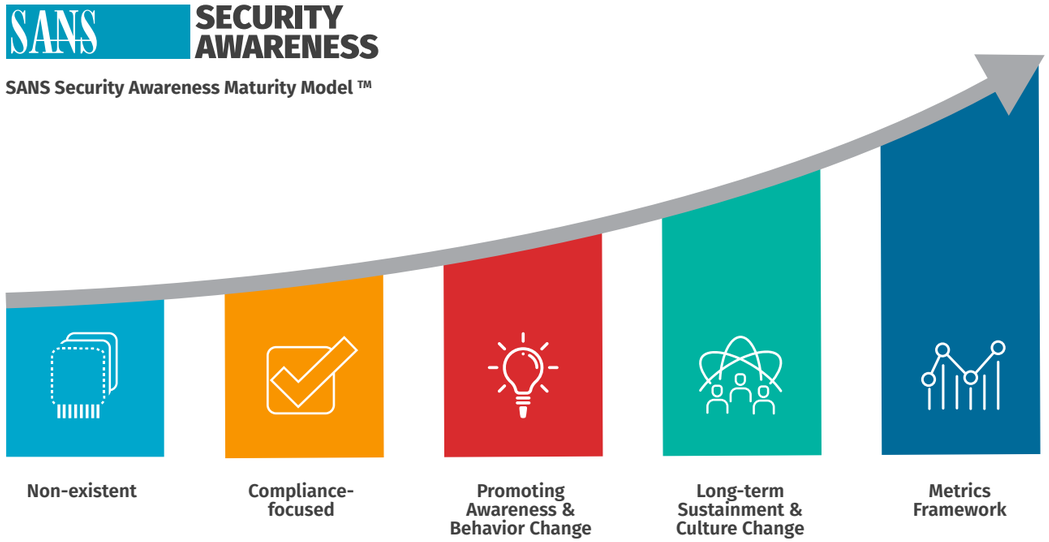
The security awareness team is part of and actively works with the security team. The program identifies the target groups and training topics that have the greatest impact on managing human risk and ultimately supporting the organization's mission. The program goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavioral change. As a result, people understand and follow organization policies and actively recognize, prevent, and report incidents.

Long-Term Sustainment and Culture Change

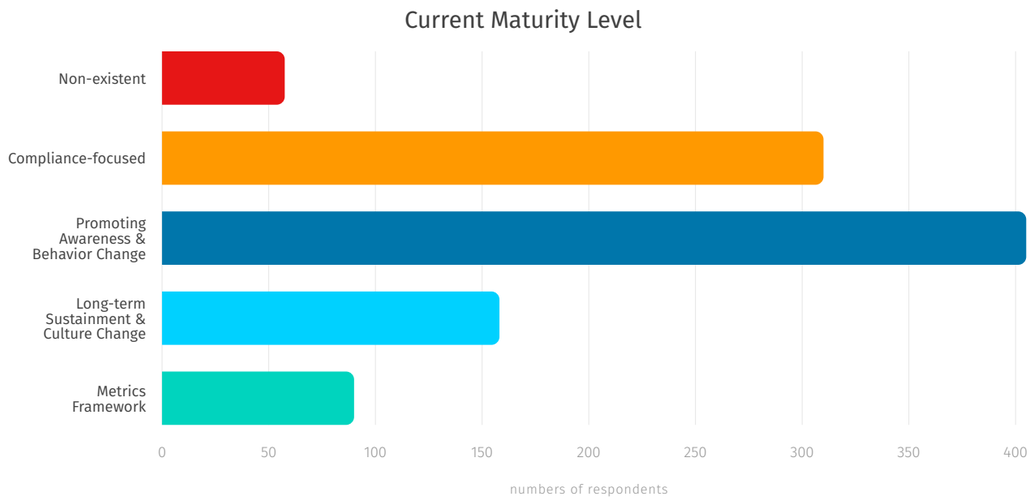
The program has the processes, resources, and leadership support in place for a long-term life cycle, including (at a minimum) an annual program review and update. As a result, the program is an established part of the organization's culture and is current and engaging. The program has gone beyond changing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

Metrics Framework

The program has a robust metrics framework aligned with the organization's mission and leadership priorities to track 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 level of the maturity model; this level simply reinforces that to truly have a mature program, you must go beyond change and have a framework that demonstrates value to leadership.

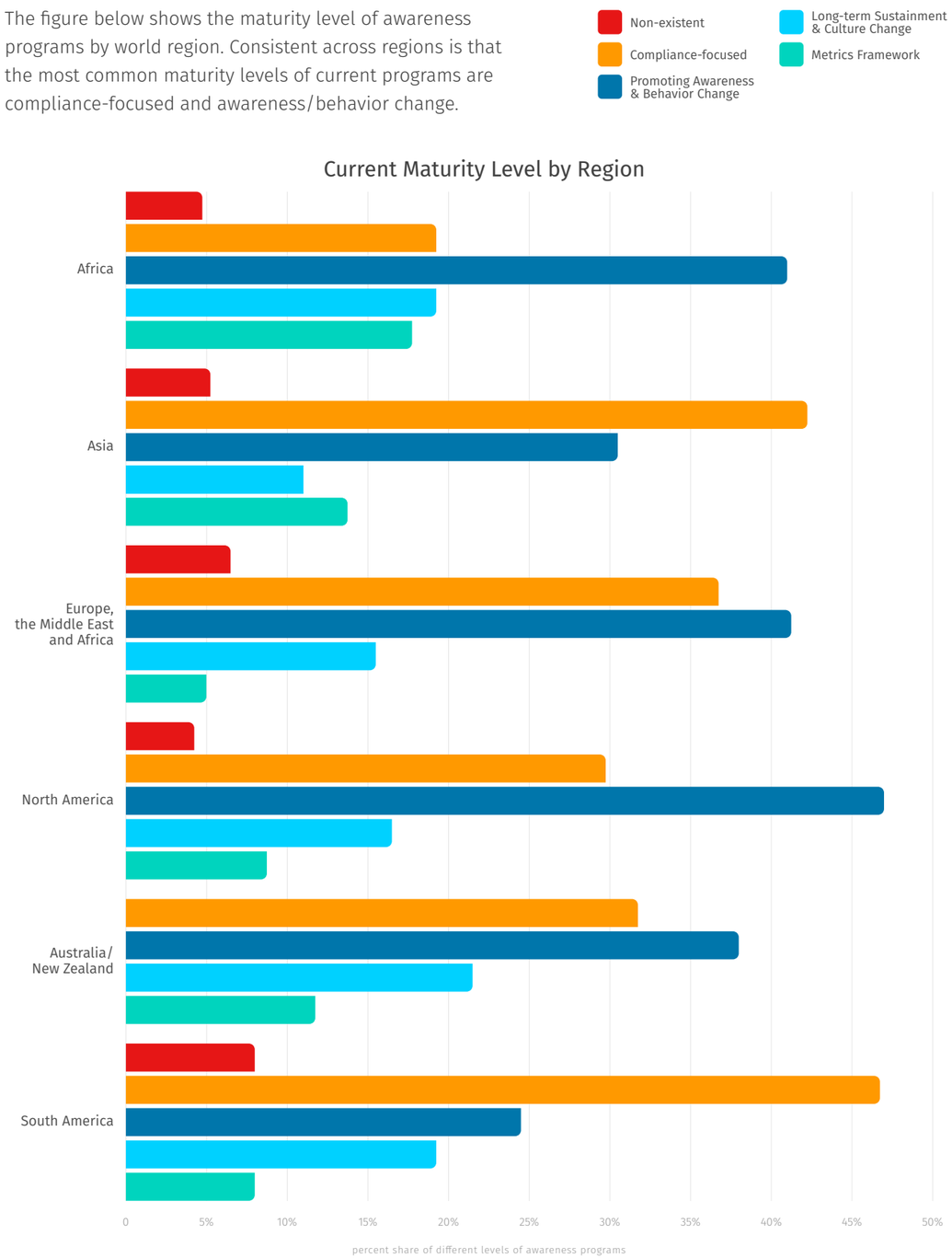


The survey that is the basis for this report asked respondents to determine the maturity level of their program, as shown in the figure below. The biggest change from last year is an 8 percent increase in compliance-driven programs (level two of the model) and a 10 percent decrease in behavior change programs (level three of the model). This may seem counter-intuitive, as it appears that programs have become less mature since last year. However, there are several possible explanations for this. The first is that there is an increase in more organizations starting new awareness programs, with most programs beginning at the compliance level. A second is that organizations have become better at understanding and determining their maturity level. As a result, they are taking a more realistic measurement of their program and identifying that it is still at the compliance level and perhaps not as mature as they may have originally believed.



Maturity by Region

The figure below shows the maturity level of awareness programs by world region. Consistent across regions is that the most common maturity levels of current programs are compliance-focused and awareness/behavior change.



Top Concerns/Risks

The top three security risks that security awareness professionals are concerned about are:

1 Phishing

By phishing, we mean almost any type of phishing attack, including email-based phishing, SMS-based smishing, and voice-based vishing. This is no surprise and reflects the same findings from numerous other security reports, including the Verizon DBIR and Microsoft Digital Defense Reports.

2 Business Email Compromise (BEC)

Also commonly known as CEO Fraud, BEC is in many ways a targeted type of phishing attack, but one that does not use an infected email attachment or malicious link. Instead, BEC is a highly targeted, fraud-based attack normally targeting an organization's accounts payable department. The cyber attacker creates a highly believable email requesting either a payment or a change in payment information. This is a very effective billion-dollar fraud industry that does not get much public attention because most organizations that fall victim to BEC attacks do not have to go public about it.

3 Ransomware

Not surprisingly, ransomware is also in the top three, tied with BEC. These attacks often get the most attention because they are highly public and often require an organization to provide a breach notification to its customers or to a reporting authority. The vast majority of ransomware infections either start with a phishing attack or with exploiting weak passwords, both human-based risks.

How to Grow and Mature Your Program

A key goal of this report is to identify the key drivers of program maturity and enable organizations to focus on and prioritize those drivers. For a security awareness program to be truly successful, these drivers are what we found to be critical.

1 Leadership Support

The most mature awareness programs are those that have had the greatest leadership support. This is not a surprise, as this has been a consistent finding for the past three years, and it aligns with findings from other organizational change programs and related research.

2 Team Size

The most mature awareness programs have the largest security awareness teams. Managing human risk is not a technology challenge, it is a human challenge, and as such it requires people to solve the problem.

3 Frequency

New for this year, we measured training frequency for organizations. The most mature awareness programs also had the most frequent training for their workforce.

As you review the findings, notice how all three of these drivers are interrelated. The larger your security awareness team, the more effectively you can partner with other departments and the more frequently you can train and engage and communicate with your workforce. The stronger your leadership support, the larger your security awareness team, but also the greater the resources and support you'll have to effectively train, partner, and engage with your workforce.

The sections that follow cover each of the three critical drivers in more detail and recommend action items.

Leadership Support

Similar to last year, most security professionals (70 percent) feel they have the leadership support they need. However, to grow your program you may need to increase that support and sustain it over the long term. Below are some ways to do it.

Action Items for Greater Leadership Support

Talk in Terms of Risk

Far too often, security awareness is perceived as a compliance effort, or security awareness professionals are perceived to be in an "entertainment" business that focuses on getting employees excited about cybersecurity but has little perceived business benefit to the organization. To effectively engage leadership, focus on and use terms that resonate with them and demonstrate support for their strategic priorities. Don't talk about what you are doing, talk about WHY you are doing it, and specifically and demonstrate how security awareness is effectively managing your organization's human risk.

Create a Sense of Urgency

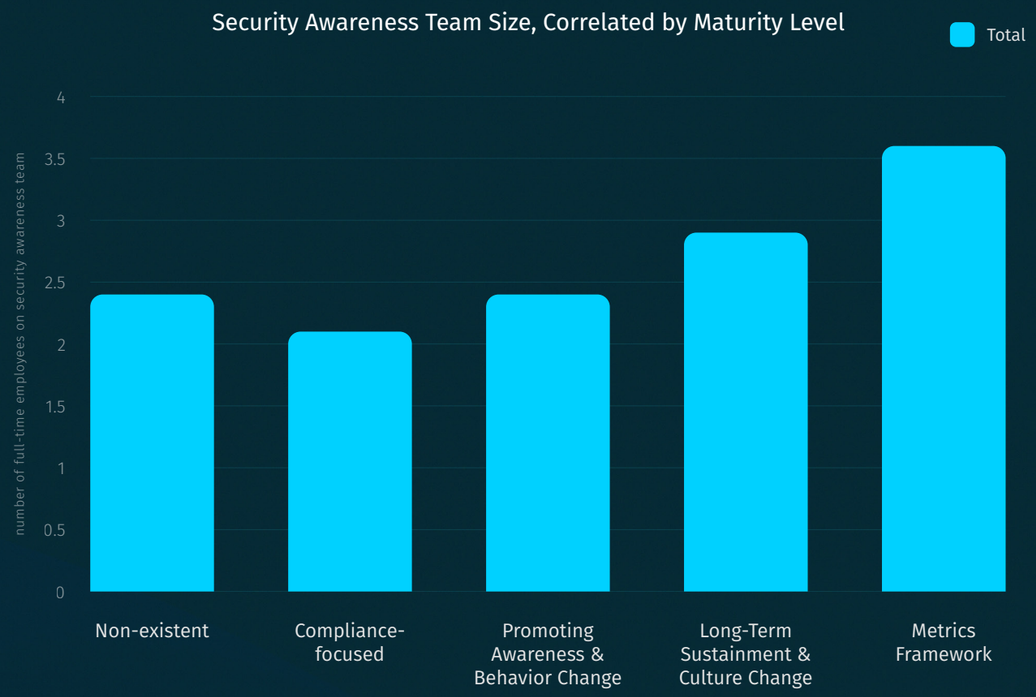
Does leadership perceive the human as a significant risk? Leverage data and statistics to demonstrate to leadership the need to address human risk. Work with your Security Operations Center, Incident Response, or Cyber Threat Intelligence teams to better document key human risks and show how people are one of the largest drivers for incidents at your organization.

Communicate the Impact

Dedicate two to four hours a month to collecting metrics about the impact and value of your awareness program and communicating it to leadership. This information can include informal metrics, established key performance indicators, or even success stories. Enable leadership to better understand and regularly see the value that your program is providing. Not sure what metrics to collect? Review the Maturity Model Indicators Matrix included with this report.

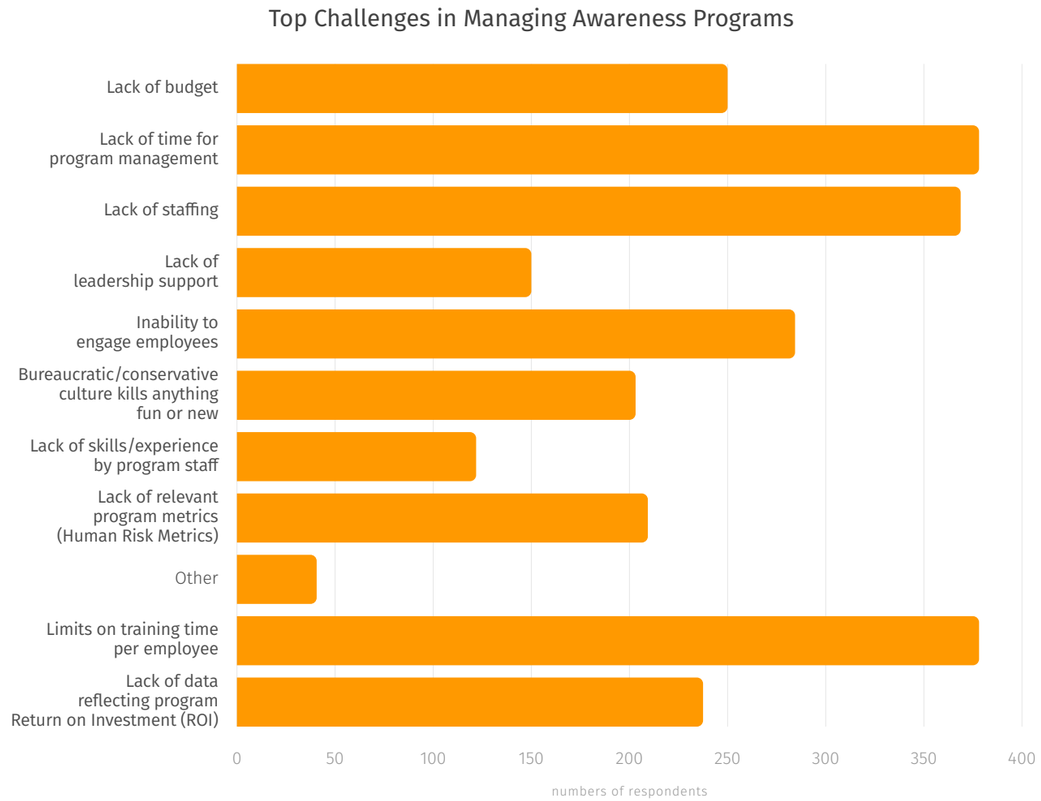
Team Size

Once again, a direct correlation was found this year between team size and program maturity: the larger your security awareness team, the greater your program's maturity level. This makes sense, as managing human risk is a people problem and it requires people to drive the solution. Organizations with the largest security awareness teams are able to most effectively partner with multiple departments, understand and address their top human risks, and frequently engage with and train their workforce. The most mature awareness programs (either at the sustainment/culture change or metrics framework levels) had at least three full-time employees dedicated to or helping manage the program.

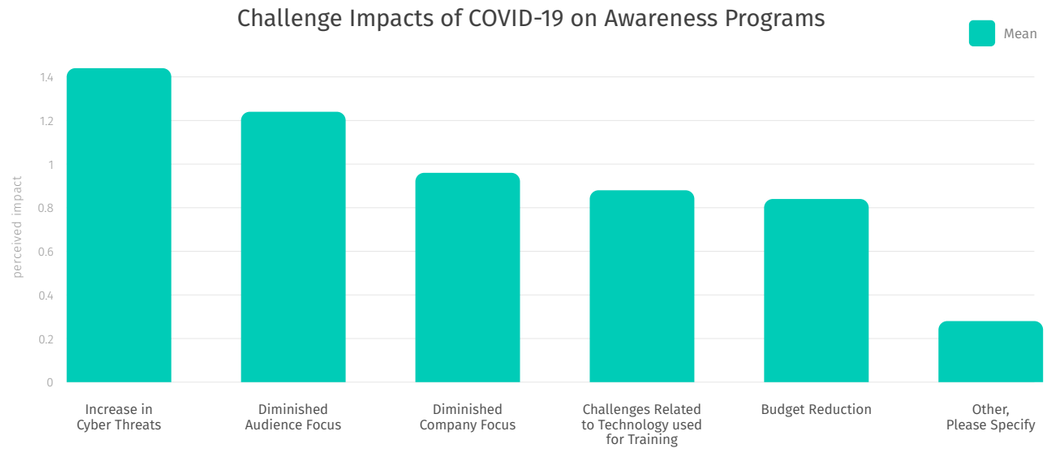


One of the questions asked of respondents was to identify the top challenge they face in building and managing an awareness program. The top three responses were all related to lack of time: "Lack of time for project management," "Limits on training time engaging employees," and "lack of staffing."

These challenges were and still are compounded by COVID-19. We asked respondents how the pandemic impacted them. Their top two responses were that it has not only created a far more distracted and overwhelmed workforce but has also created an environment where human-based cyber attacks have become more frequent and effective.



As stated earlier, managing human risk is a people problem, and for the past three years our findings have reinforced that to effectively manage human risk, people are also the solution. A dedicated and sufficiently large security awareness team is key to managing and measuring a mature, high-impact security awareness program.



Action Items to Increase Team Size

The greater the leadership support, the easier it is to build a larger security awareness team. Below are some ways to make that happen.

Document Security Team Discrepancy
Explain that while in many ways organizations have become quite effective at securing technology, they have invested little to secure their workforce. A simple but effective way to demonstrate this is to count how many people are on your security team. Then out of all those individuals, determine how many employees on the security team are dedicated to technology versus how many are dedicated to the human side of risk. As a starting point, consider having a 10 to 1 ratio of technical security professionals to human- focused security professionals.

Break Down Your Needs
Document all the different steps and initiatives you need to take for your security awareness program to be effective. These can include working with the security team to identify and monitor your top human risks, working with Audit and Legal for compliance purposes, partnering with Human Resource and Communications for employee outreach and training, working with IT, developers, and other technical staff to design role-based training, etc. If you can identify and document the number of full-time employees needed for each of these efforts, and at the same time demonstrate the value of these efforts, leadership will have a better understanding of why you need more help. If you can't hire full-time employees on your team, see if you can hire short-term contractors to take on and help manage specific initiatives.

Develop Partnerships
You can't do everything yourself. The more you can partner with other departments in your organization, the more effective your team will be. Partner with Communications to help engage and communicate with your workforce and even train them. Work with Human Resources to help with new hires or in measuring and building a strong culture. Work with Business Operations to help analyze metrics and data points.

Training Frequency

New this year, we looked at the frequency of training, specifically how often organizations train their workforce. The data showed that the organizations that had more frequent training often had the most mature programs. Organizations that engage and train their workforce only annually or an ad hoc basis cannot effectively change behavior and are thus stuck at the compliance level, checking the box. We recommend that organizations communicate to, interact with, and/or train their workforce at least once a month.

Action Items for Training Frequency

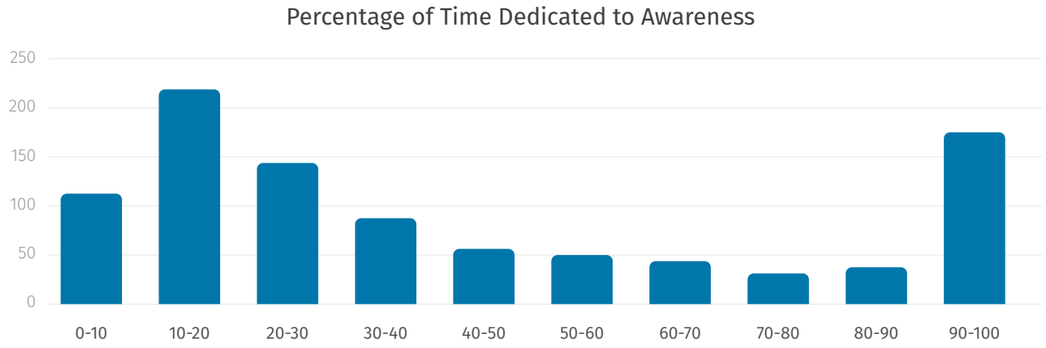
Keep it Simple.
Training does not have to be complicated or costly, such as complex, gamified computer-based training. It can be something as simple as leading a virtual webcast on ransomware, bringing in a guest speaker from law enforcement to talk about identity theft, releasing a fun micro-video with local employees as actors, hosting an online Ask Me Anything session with leadership, publishing a monthly podcast from the security team, sending out an infographic on how to create a secure home, or launching a fun scavenger hunt. What's important is not so much the modality you use to train your workforce, but rather how often you are effectively engaging them and making that training simple to understand and follow. In many ways training is just like working out – it is the frequency that is important. Your security team most likely has an active vulnerability management program where you are patching systems on at least a monthly basis. We need to do the same for the human operating system.

How to Grow and Mature Your Career

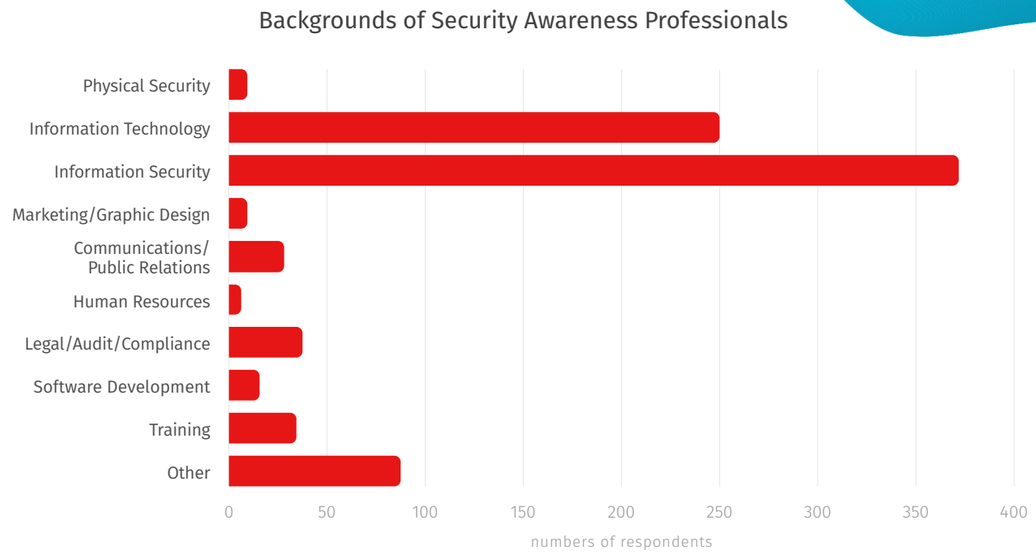
The second goal of this report is to enable security awareness professionals to grow their careers, including their compensation. The hope is that in the near future we will begin to see CISOs who started their careers on the human side of cybersecurity.

The Part-Time Awareness Professional – The Curse of Knowledge

Among security awareness professionals, 69 percent are part-time, spending less than half their time on security awareness and focusing on other priorities. Only 18 percent of awareness professionals are dedicated full-time to supporting their awareness program. We define full-time as someone dedicating 70% or more of their time on security awareness.



In addition, the large majority (72%) of security awareness professionals have a technical background. The data implies that most people leading or managing awareness programs are most likely already part of the security or IT team with technical responsibilities. They have been assigned to manage their organization's awareness program in addition to their other normal responsibilities. This can help explain why so many awareness programs struggle to engage their workforce. Having a strong technical or security background is valuable, as it enables people to understand the common technologies and behaviors that pose a risk to the organization and the tactics, techniques and procedures of cyber attackers. However, having "too technical" a background can also sometimes mean the person lacks the skills to effectively communicate those risks or meaningfully engage employees.



The term sometimes used for a person who has expertise but struggles to communicate that expertise is "Curse of Knowledge," a type of cognitive bias. The more expertise people have 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 technology related to it are 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, difficult, intimidating, and even overwhelming for non-experts***. This not only creates less effective training materials, it also impacts communication to leadership and ultimately can create a negative security culture. Security awareness professionals with strong technical and security backgrounds should take care to be aware of their Curse of Knowledge.

Action Items for Technical Professionals

Know Your Bias

If you have highly technical skills or 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.

Access or Develop Communication and Engagement Skills

Be sure you have someone on your awareness team who has the skills required for effective communication and engagement. This can include training someone on your security team, partnering with your Communications or Marketing Department, or even embedding a staff member from those departments in your security awareness team. Or, consider acquiring the appropriate skills yourself to more effectively engage your workforce. Review the Career Development section in Appendix B.

If you are among that small percentage of security team members devoted full-time to security awareness, or among the small percentage that does not have a technical background, you will find the next section on compensation very interesting.

Compensation – Part-Time versus Full-Time

This was the second year we asked about compensation, and, like last year, the findings were surprising. First, the average salary for a security awareness professional was $110,309, which is an increase from last year (a good thing). However, those dedicated full-time to awareness were paid on average only $86,626 while those who are part-time averaged $117,584, a $30,000 difference. Why such a disparity? We believe the answer is perceived value. The data suggest that those who are part-time are often already part of the security or information technology team and security awareness is simply an addition to their other responsibilities. Their higher salary could be a reflection of them being compensated for other security or technical skills. Those who are dedicated full-time to awareness often have non-technical backgrounds, such as communications, and are compensated specifically for their security awareness role, which is often not as valued as most other security roles.

The key challenge here is perception. Too often, security awareness professionals are perceived as being in the "entertainment business" because they talk exclusively about engaging and training the workforce. But this overlooks the fact that security awareness professionals are not just in the business of changing human behavior; ultimately they are key to managing human risk. Here are key steps you can take to address such misconceptions, improve your credibility, and ultimately increase your compensation.

Action Items for Non-Technical Professionals

Reframe the Perception
Leadership or security teams often perceive security awareness not as part of security, but rather as a compliance effort that has little relevance to managing risk. To help change such perceptions, focus on 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. Help your security team identify your top human risks and the key behaviors that manage those risks. Demonstrate how effective communications, training, and engagement is changing those key behaviors and reducing human risk.

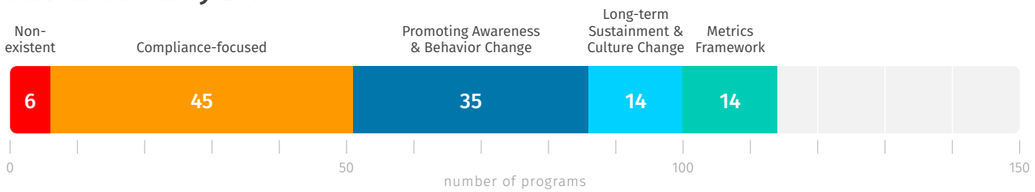
Expand Your Role
Far too often, security awareness professionals are perceived simply as the individual responsible for the annual computer-based training or some similar activity. However, as a leader in managing human risk, your role can and should be so much more. Work with the security team to improve and simplify its communications with your workforce, help manage security tool rollouts to your workforce (such as multi-factor authentication), work with the security team to create policies that are easier for people to understand and follow, and partner with the Incident Response team to assist in any incident communications, internally or externally. Work with senior leadership on table-top exercises to rehearse senior leadership incident response abilities. You have a huge number of opportunities to expand your value to the security team and leadership, so make the most of them!

Develop Your Skills
Review Appendix B on Career Development. Develop your understanding of security fundamentals so that you have a better understanding of the terms, technologies, and challenges involved. You are not expected to become a technical expert (that is what a security team is for), but it is important to have an understanding of the models, frameworks, and terminology. This will enable you to better understand your organization's risks and communicate with others about them, and you will be perceived as more valuable by your more technical team members.

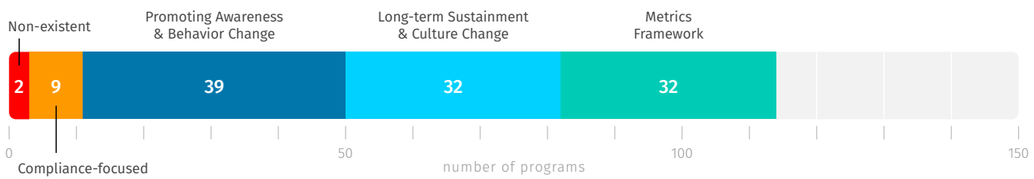
In closing our discussion of compensation, it should be noted that security awareness professionals in Australia/New Zealand had the highest average annual compensation ($121,236), while those in South America had the lowest ($56,960). In North America, one notable finding is that the higher the maturity level of an organization's security awareness program, the higher the salary for the awareness professionals who work there.

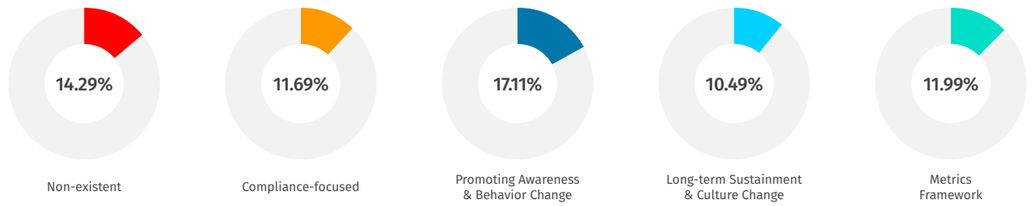
Geographic Data – APAC

Current Maturity Level

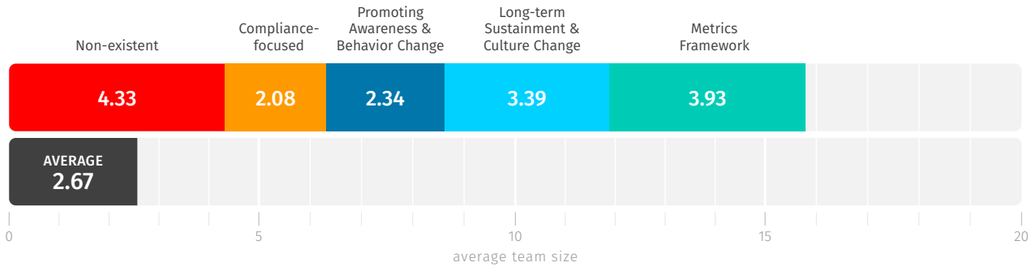


Desired Maturity Level

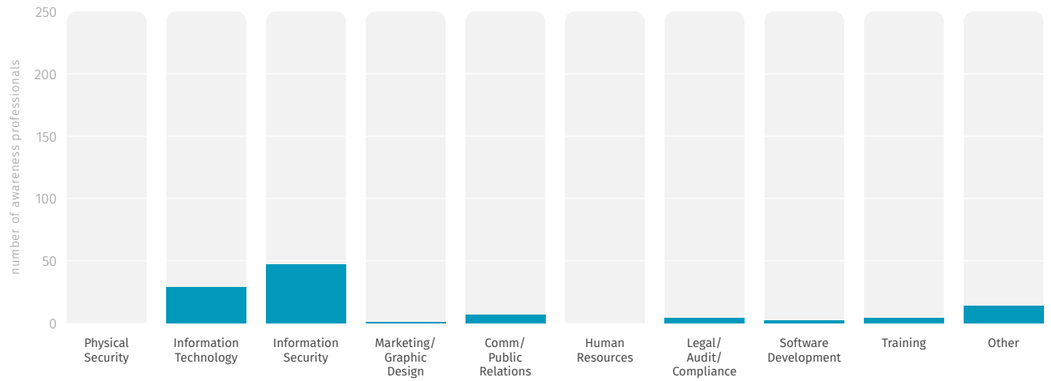




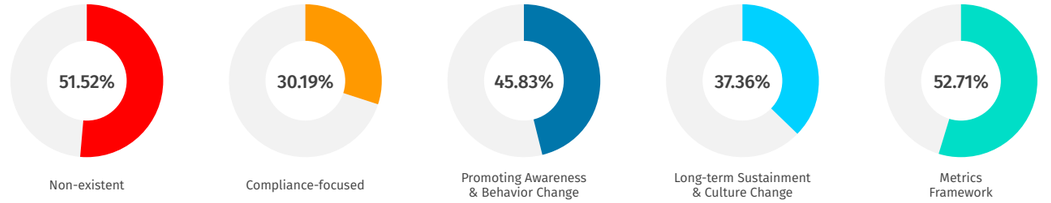
Team Size by Maturity Level



Background

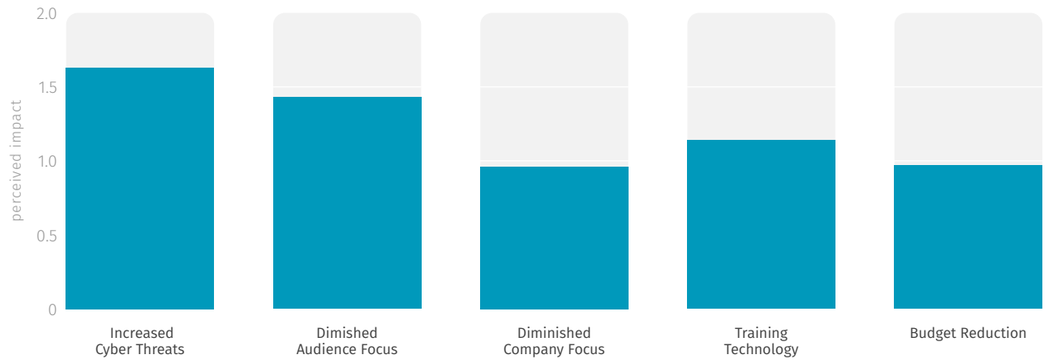


Average Percent of Time Spent on Awareness, by Maturity Level



Salary

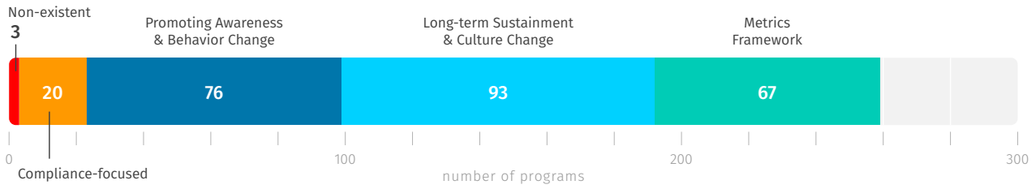
COVID Challenges

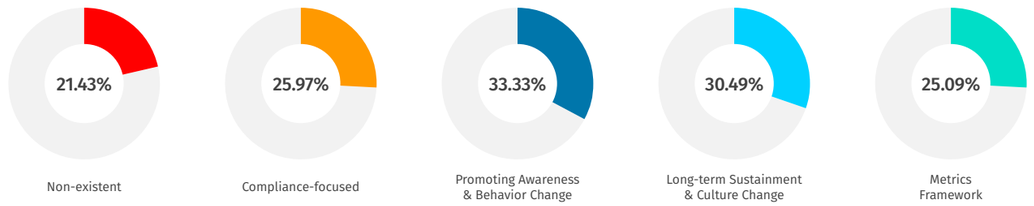


Geographic Data – EMEA

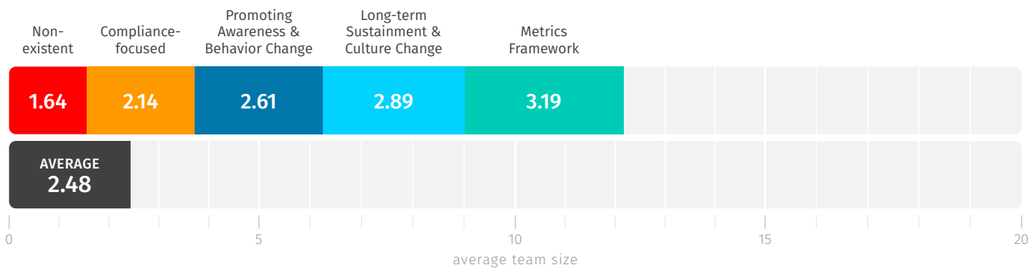
Current Maturity Level

Desired Maturity Level

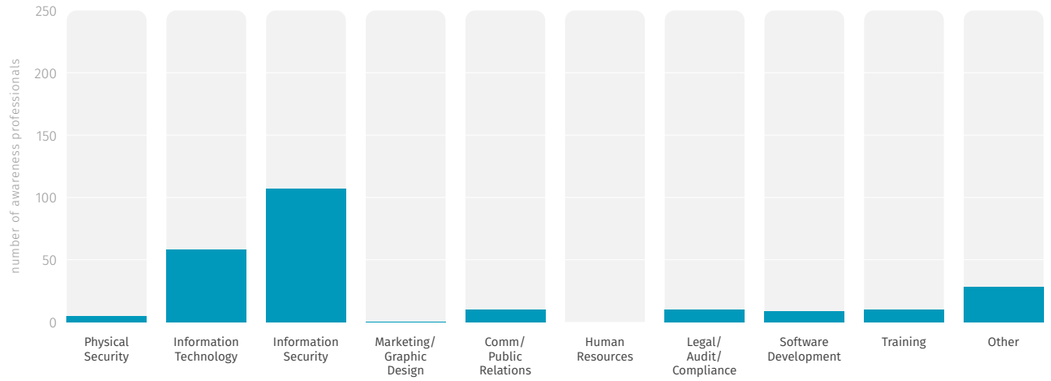




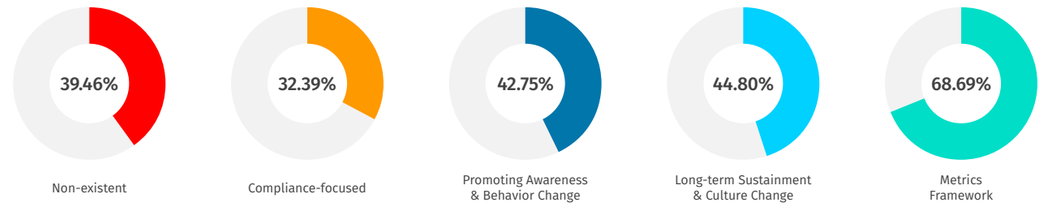
Team Size by Maturity Level



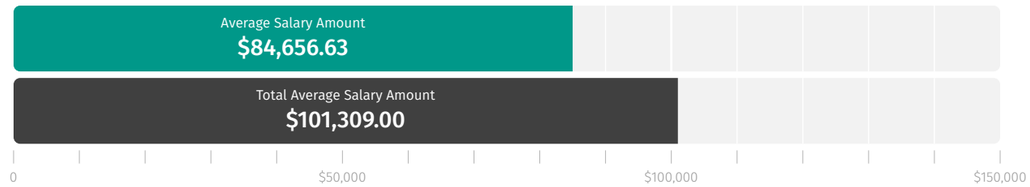
Background



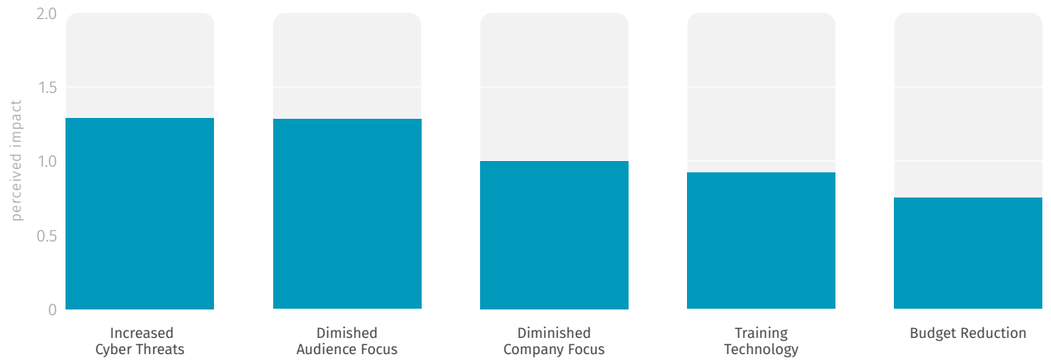
Average Percent of Time Spent on Awareness, by Maturity Level



Salary

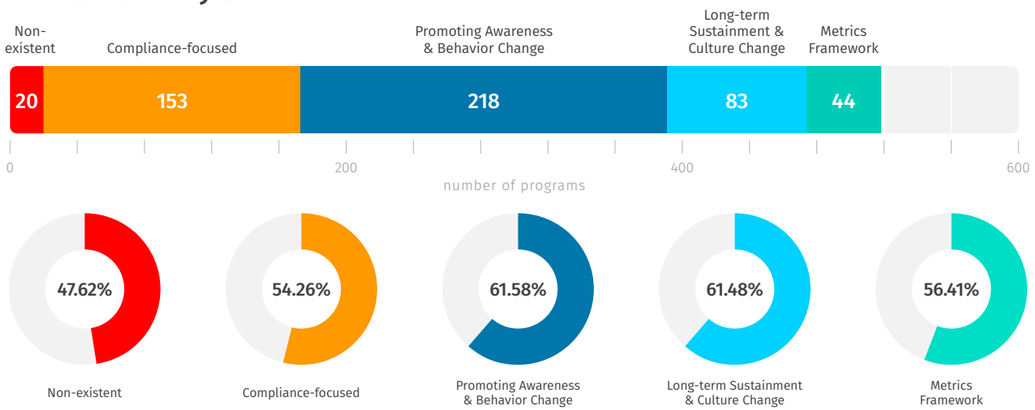


COVID Challenges

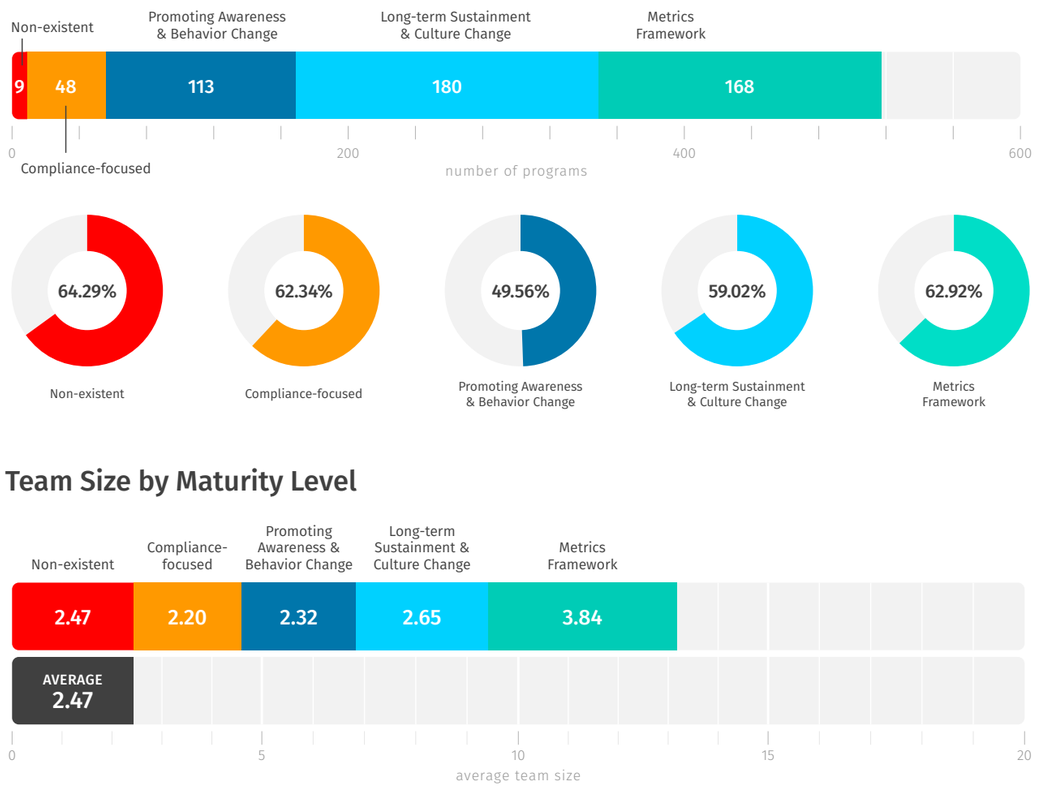


Geographic Data – NALA

Current Maturity Level

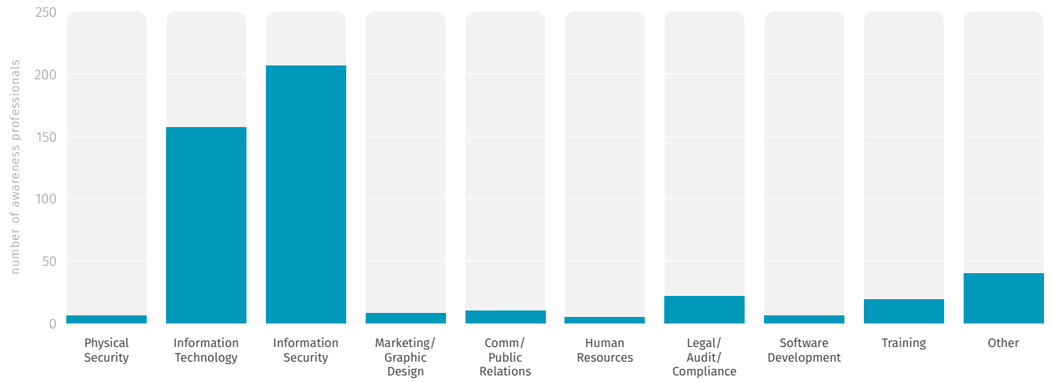


Desired Maturity Level

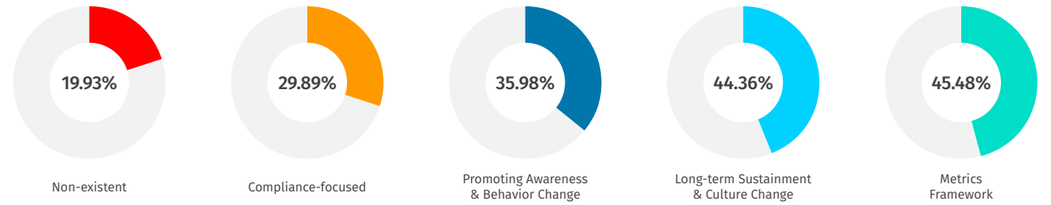


Team Size by Maturity Level

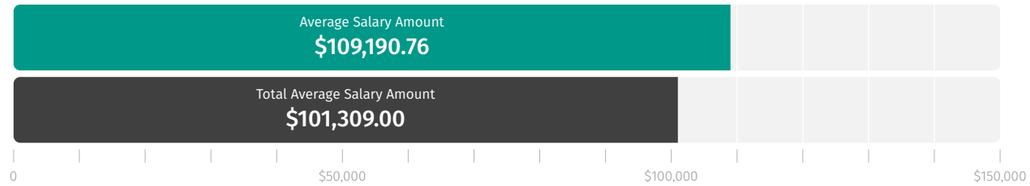
Background



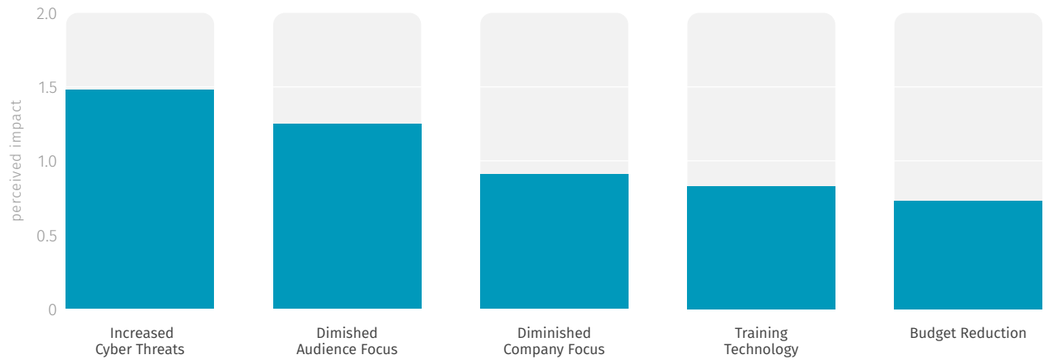
Average Percent of Time Spent on Awareness, by Maturity Level



Salary



COVID Challenges



Summary of Key Action Items

Maturing Your Program

Talk in Terms of Risk

Far too often, security awareness is perceived as a compliance effort, or security awareness professionals are perceived to be in an "entertainment" business that focuses on getting employees excited about cybersecurity but has little perceived business benefit to the organization. To effectively engage leadership, focus on and use terms that resonate with them and demonstrate support for their strategic priorities. Don't talk about what you are doing, talk about WHY you are doing it, and specifically demonstrate how security awareness is effectively managing your organization's human risk.

Create a Sense of Urgency

Does leadership perceive the human as a significant risk? Leverage data and statistics to demonstrate to leadership the need to address human risk. Work with your Security Operations Center, Incident Response, or Cyber Threat Intelligence Teams to better document key human risks and show how people are one of the largest drivers for incidents at your organization.

Communicate the Impact

Dedicate two to four hours a month to collecting information about the impact and value of your awareness program and communicating it to leadership. This information can include informal metrics, established key performance indicators, or even success stories. Enable leadership to better understand and regularly see the value that your program is providing. Not sure what metrics to collect? Review the Maturity Model Indicators Matrix included with this report.

Document Security Team Discrepancy

Explain that while in many ways organizations have become quite effective at securing technology, they have invested little to secure their workforce. A simple but effective way to demonstrate this is to count how many people are on your security team. Then, out of all those individuals, determine how many employees on the security team are dedicated to the human side of risk. As a starting point, consider having a 10 to 1 ratio of technical security professionals to human-focused security professionals.

Break Down Your Needs

Document all the different steps and initiatives you need to take for your security awareness program to be effective. These can include working with the security team to identify and monitor your top human risks, working with Audit and Legal for compliance purposes, partnering with Human Resource and Communications for employee outreach and training, working with IT, developers, and other technical staff to design role-based training, etc. If you can identify and document the number of full-time employees needed for each of these efforts, and at the same time demonstrate the value of these efforts, leadership will have a better understanding of why you need more help. If you can't hire full-time employees on your team, see if you can hire short-term contractors to take on and help manage specific initiatives.

Develop Partnerships

You can't do everything yourself. The more you can partner with other departments in your organization, the more effective your team will be. Partner with Communications to help engage and communicate with your workforce and even train them. Work with Human Resources to help with new hires or on measuring and building a strong culture. Work with Business Operations to help analyze metrics and data points.

Keep it Simple

Training does not have to be complicated or costly, such as complex, gamified computer-based training. It can be something as simple as leading a virtual webcast on ransomware, bringing in a guest speaker from law enforcement to talk about identity theft, releasing a fun micro-video with local employees as actors, hosting an online Ask Me Anything session with leadership, publishing a monthly podcast from the security team, sending out an infographic on how to create a secure home, or launching a fun scavenger hunt. What's important is not so much the modality you use to train your workforce, but rather how often you are effectively engaging them and making that training simple to understand and follow. In many ways training is just like working out – it is the frequency that is important.

Growing Your Career

For Part-Time or Technical Individuals

Know Your Bias

If you have a highly technical or 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.

Develop Communication and Engagement Skills

Be sure you have someone on your awareness team who has the skills required for effective communication and engagement. This can include training someone on your security team, partnering with your Communications or Marketing Department, or even embedding a staff member from those departments in your security awareness team. Or, consider acquiring the appropriate skills yourself to more effectively engage your workforce. Review the Career Development section in Appendix B.

For Full-time or Non-Technical Individuals

Reframe the Perception

Leadership or security teams often perceive security awareness not as part of security, but rather as a compliance effort that has little relevance to managing risk. To help change such perceptions, focus on 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. Help your security team identify your top human risks and the key behaviors that manage those risks. Demonstrate how effective communications, training, and engagement is changing those key behaviors and reducing human risk.

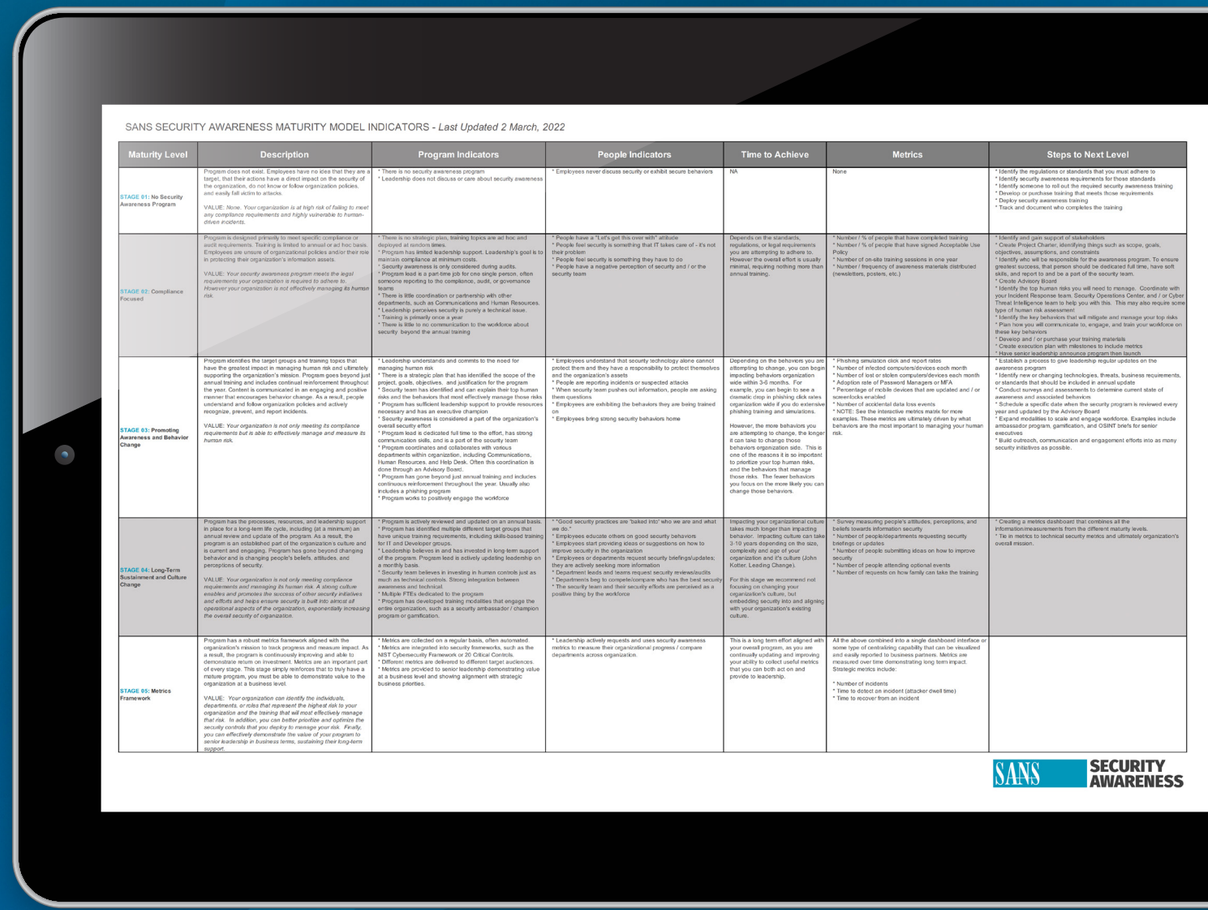
Expand Your Role

Far too often, security awareness professionals are perceived simply as the individual responsible for the annual computer-based training or some similar activity. However, as a leader in managing human risk, your role can and should be so much more. Work with the security team to improve and simplify its communications with your workforce, help manage security tool rollouts to your workforce (such as multi-factor authentication), work with the security team to create policies that are easier for people to understand and follow, and partner with the Incident Response team to assist in any incident communications, internally or externally. Work with senior leadership on table-top exercises to rehearse senior leadership incident response abilities. You have a huge number of opportunities to expand your value to the security team and leadership, so make the most of them!

Develop Your Skills

Review Appendix B on Career Development. For those of you without a security or a technical background, you may want to develop your understanding of security fundamentals so that you have a better understanding of the terms, technologies, and challenges involved. You are not expected to become a technical expert (that is what a security team is for), but it is important to have an understanding of the models, frameworks and terminology. This will enable you to better understand your organization's risks and communicate with others about them, and you will be perceived as more valuable by your more technical team members.

Appendix A. Maturity Model Indicators Matrix



Download

Appendix B. Career Development

A critical takeaway from the 2022 report is that your compensation as a security awareness professional is in large part driven by your training and skills, including understanding key concepts of cybersecurity and risk management. Security awareness is ultimately about risk management, so the better you understand the concepts of security, the more effective you are not only at managing human risk but at communicating that risk (and your value) to leadership. Skills such as communications, project management, and partnership are key to a successful security awareness career, but as this field matures you also need to understand the fundamentals of cybersecurity. You neither need nor are expected to develop a deep set of technical security skills, but you do need to build and understand key fundamentals such as security frameworks, risk assessments, and cyber threat actors and their relevant tactics, techniques, and procedures. As such, this appendix presents a career development path to help you strengthen your security knowledge.

Where to Start

If you are new to the world of information security and/or security awareness, the very first course you may want to start with is:

SANS MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program. This two-day course lays the foundation for understanding security awareness, managing human risk, and ultimately changing organizational behavior. Those new to security will gain a better understanding of concepts such as risk management and risk analysis. Those new to communications and engagement will learn key concepts such as the Attention, Interest, Desire, and Action Model and the Start with Why and Curse of Knowledge concepts, along with other models and principles. Course content is based on lessons learned from hundreds of security awareness programs from around the world. 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 further develop your skills and 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 and the behaviors that manage those risks, but also 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.

SANS MGT512: Security Leadership Essentials for Managers. This five-day 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.

SANS SEC301: Introduction to Cybersecurity. Jump-start your security knowledge with 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 functions 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 on 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 two to four years of experience in security awareness and feel confident in the concepts of both cybersecurity and organizational behavior, we recommend MGT521.

SANS 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. The two-day MGT521 course teaches 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 where 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 five to seven years of experience and want to truly develop your security leadership skills, consider MGT514. This course will walk you through the strategic planning process and challenges faced by Chief Information Security Officers (CISOs). Many people consider this the "CISO course," helping develop new and experienced CISOs 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.

SANS MGT514: Security Strategic Planning, Policy, and Leadership. This five-day course gives you the 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 become a more effective leader and at the same time dramatically improve and broaden your career opportunities.

Acknowledgments

The 2022 Security Awareness Report was developed by the community for the community, in partnership with the SANS Institute. The following key contributors produced this report.

Authors

Dan DeBeaubien

Dan joined SANS in 2014 and serves as the Director of Digital Innovation focusing on digital products and Security Awareness and Human Risk product strategy. Dan is a 30-year veteran of information technology and a former CTO for 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 held the positions of Chief Information Security Officer and Chief Information Compliance Officer.

Lance Spitzner

Lance Spitzner has more than 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 his founding of the Honeynet Project. In addition, Lance has published three security books, consulted in more than 25 countries, and helped more than 350 organizations build security awareness and culture programs to manage their human risk. Lance is a frequent presenter and a serial tweeter (@lspitzner), and he works on numerous community projects. Before entering the information security field, Lance served as an armor officer in the U.S. Army's Rapid Deployment Force and earned his MBA from the University of Illinois.

Key Contributors

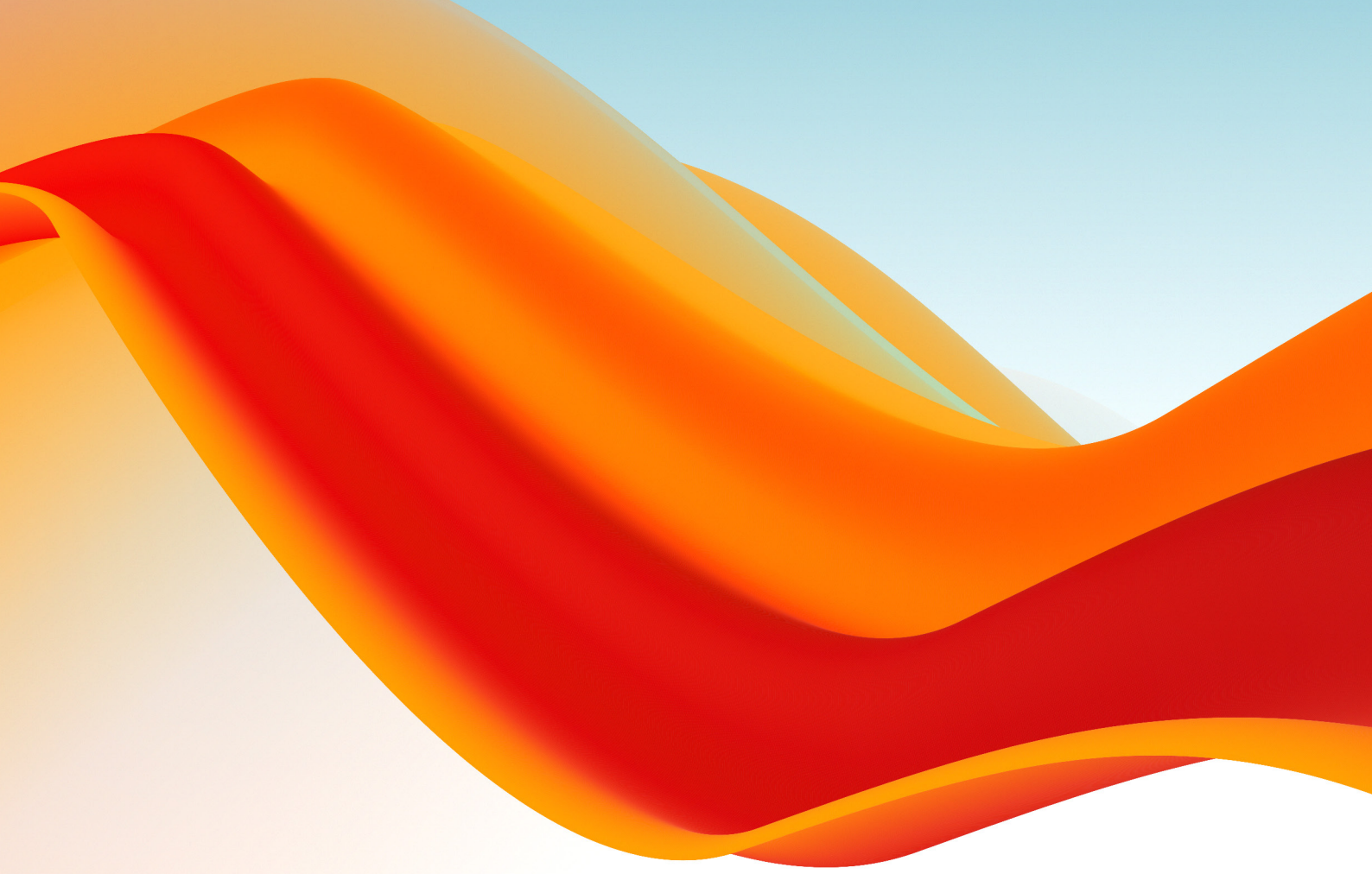
The authors would like to thank the team from the Kogod Cybersecurity Governance Center (KCGC) for their key role in the independent analysis of the data in this report. KCGC is a research initiative of American University's Kogod School of Business that conducts research to equip today's business leaders with the best actionable intelligence on cybersecurity and privacy. KCGC's expertise spans multiple areas, including data privacy, cybersecurity, data management, and data analytics.

Dr. Heng Xu

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 Kogod, she had both an academic and government background. She was a professor at Penn State for 12 years, as well as a program director at the U.S. National Science Foundation (NSF) for three years. Dr. Xu's current research focus is on information privacy, data ethics, and data analytics. She has received many awards for her work, including the Woman of Achievement Award in IEEE Big Data Security (2021), the IEEE ITSS Leadership Award in Intelligence and Security Informatics (2020), the Operational Research Society's Stafford Beer Medal (2018), the NSF CAREER Award (2010), and many best paper awards and nominations at various conferences.

Dr. Nan Zhang

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 more than 100 research papers and served as a program director at the U.S. National Science Foundation (NSF). Before joining Kogod, Dr. Zhang was a Professor of Information/Computer Science at Penn State University, George Washington University, and UT Arlington. His has received several awards for his work, including the Communications of the ACM Research Highlight (2020), the ACM SIGMOD Research Highlight Award (2019), the NSF CAREER Award (2008), and many best paper awards and nominations at various leading research conferences.



About SANS Security Awareness

SANS Security Awareness, a division of the SANS Institute, provides organizations with a comprehensive security awareness solution that enables them to easily and effectively manage their human cybersecurity risk. SANS Security Awareness has worked with more than 1,300 organizations and trained more than 6.5 million people around the world. The program offers globally relevant and expert-authored tools and training to help individuals shield their organization from attacks, as well as a fleet of savvy guides and resources to guide their work every step of the way.

SANS SECURITY AWARENESS

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