THE HUMAN FIX TO HUMAN RISK

5 STEPS TO FOSTERING A CULTURE OF CYBER SECURITY AWARENESS

LISE LAPOINTE

AND HER DEDICATED TERRANOVA SECURITY TEAM

FOREWORD BY PIERRE-LUC REFALO

The Human Fix to Human Risk

THE HUMAN FIX TO HUMAN RISK

5 STEPS TO FOSTERING A CULTURE OF CYBER SECURITY AWARENESS

LISE LAPOINTE

and Her Dedicated Terranova Security Team

THE HUMAN FIX TO HUMAN RISK
5 Steps to Fostering a Culture of Cyber Security Awareness
Second Edition

ISBN 978-1-5445-4046-7 *Hardcover*
978-1-5445-4044-3 *Paperback*
978-1-5445-4045-0 *Ebook*
978-1-5445-4047-4 *Audiobook*

This book is dedicated to my team, whom I deeply appreciate, and Jamal, Stéphanie, and Mathieu for their contribution and unconditional support for more than a decade in helping make Terranova Security a global leader in Security Awareness.

CONTENTS

FOREWORD

According to three well-known sayings, "Security is 20 percent technical and 80 percent organizational," "The real security problems are found between the seat and the keyboard!" and even "Security is a cocktail of tools, processes, and people." In short, dare we say that it's all a question of behavior and culture. *This is what Lise Lapointe is pointing out in her comprehensive vision to fix human risks in the digital space*.

Addressing cyber security acculturation requires a clear definition of what we are talking about, well beyond raising awareness among the public. Acculturation is a little-used but highly relevant term because it is based on "*a process that allows an individual or group of individuals to acquire a culture that is foreign to them*." It is an addition, and not a subtraction nor a submission! How does this apply to cyber space?

If there is a cyber security culture to be developed, it cannot succeed by disregarding the corporate culture (its history, its management, its business, its geographies) and, more importantly, the digital culture (digitalization, innovation). Whether individually or collectively, we will find very different visions and approaches within an organization. The question of leadership arises to guide acculturation in the right direction.

The acculturation to cyber security must address in a coherent and relevant way: first **the risk culture**, then **the access culture**, **the culture of secret**, and finally, **the culture of control**. The first is the most important and the most difficult to address in large organizations. The second is tricky because it imposes a major paradigm shift: the end of ownership in the age of cloud computing. It is because confidentiality is regressing that the third about secrecy and privacy is more than ever important. And the fourth must be developed in a transparent and balanced way between a level of risk/threat and the criticality/value of the asset to protect or objects to control.

In concrete terms, the acculturation process must be part of both a strategic and a programmatic approach:

- The culture of risk will be fundamental during a change in governance or a reorganization.
- The culture of access will be essential to address during a "move to cloud" program or a major acquisition.
- The culture of secret will be relevant during a transition to the cloud and any innovation program as well.
- The culture of control will be addressed in any Compliance program but also after a major incident (internal or impacting a competitor, customer, supplier).

The question today, even more than in the past, is not how to communicate, raise awareness or train people, or to whom to convey messages. Transmitting knowledge, improving behaviors, or reinforcing skills are now well-understood fundamentals. At the end of the day, the essential question is, "**How to bring an individual to do what he has to do in his own will?**" Specialists and program managers must

consider six degrees: ***Unawareness*** addresses the issue of risks and threats. ***Ignorance*** addresses the issue of policies and security rules. ***Resistance*** addresses the applicability of rules and best practices. ***Bypass*** is a natural attitude that must be mastered. ***Overconfidence*** is aimed at the most mature organizations. ***Fraud*** is an ultra-minority in a population but growing with huge potential impacts.

The acculturation program will have an effect on only the first four degrees, and not on overconfidence and fraud. The balance between the "fear marketing" and the "moralism" must be found for each context and each culture.

Lise's book will help executives and managers as well as all individuals to understand how to practically make each individual a first line of defense.

—PIERRE-LUC RÉFALO
Vice President of Capgemini—Group Cybersecurity

TELL ME
AND I FORGET,
TEACH ME AND I
MAY REMEMBER,
INVOLVE ME
AND I LEARN.

—BENJAMIN FRANKLIN

PREFACE

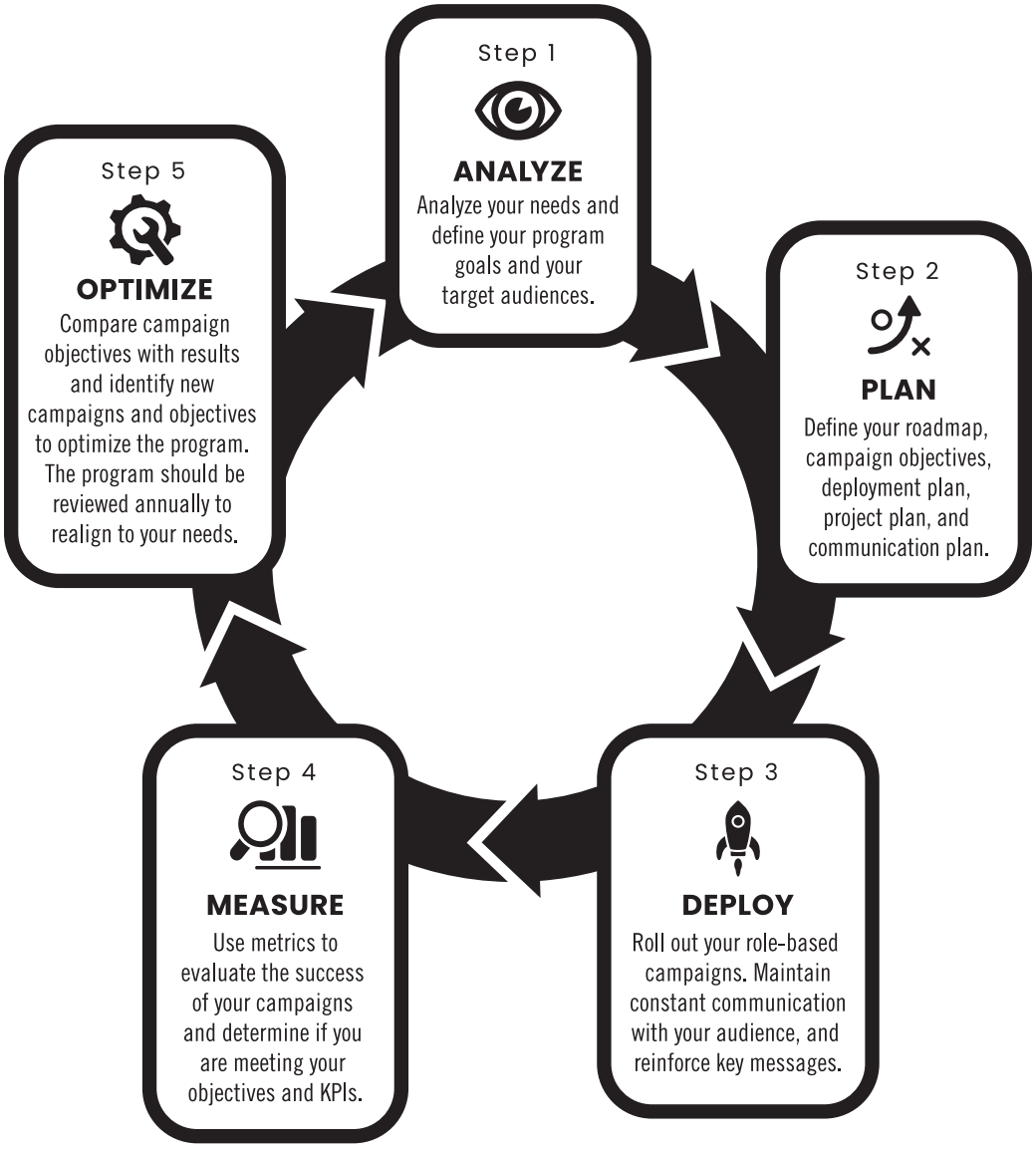
I am honored that you have decided to read the second edition of my book, *The Human Fix to Human Risk*.

This revised and expanded text will guide you through the process of building a security awareness program with the easy-to-use Terranova Security Awareness 5-Step Framework. More than two decades of industry experience are at your fingertips, highlighting lessons my team and I have learned from delivering tens of thousands of successful security awareness programs to millions of end users worldwide.

Now more than ever, organizations must invest in awareness training that addresses the human risk factor in cyber security. The global COVID-19 pandemic accelerated digital transformation initiatives, such as implementing online collaboration tools and using various cloud-based services from any location and device. The resulting business landscape, where hybrid and remote work models have fueled an increase in technology adoption, has multiplied the security challenges the average organization faces.

The regulatory landscape for protecting personal information continues to evolve, demanding more from organizations and employees.

The Terranova Security Awareness
5-Step Framework at a Glance



Respecting the laws and preventing data breaches has become an enterprise risk for many organizations.

To reduce risk and strengthen information security, managers and security awareness administrators must go beyond simply sending end users stand-alone courses and phishing simulations. Instead, they must create a strong security-aware culture, with best practices in mind across all business units.

By embedding cyber security into your organization's culture, you make it much easier, in the long run, to reach behavior change objectives and tie this mission to business risk.

Why Implement a Security Awareness Program?

Security awareness is key to constructing a cyber security-aware culture in any organization. Today, however, you must evolve beyond just offering training to your end users once in a while. Building a strong security awareness program requires continuous education. Changing behavior and culture takes time, and users need to be reminded and trained to recognize the risks to be able to avoid them. Additionally, executives must support and fund initiatives, managers must promote and encourage training participation, and a security awareness manager must run awareness programs.

In this broader context, security awareness training gives the user the knowledge and skills they need to make the right decision when faced with a potential cyber attack. By making end users accountable and encouraging them to buy into a culture of cyber security, your organization can:

- **Reduce risk** by building critical cyber threat resilience across all business units
- **Maintain compliance** with data protection, privacy, or IT governance regulations
- **Maintain credibility and trust** with customers, clients, internal and external stakeholders, and auditors
- **Train the users with best practices that they can apply in their home environment**

How I Became a Security Awareness Entrepreneur

I come from a family of entrepreneurs. Still, my father always hoped his children would attend university and choose a different career path. Initially, I did exactly that—I became a teacher. Starting out in education in the early 1980s, my future seemed clear.

I didn't expect my brother Michel to help me jump-start my career as an entrepreneur.

He was working at IBM, which had recently launched Displaywriter, a new word processor. IBM wanted to introduce Displaywriter into schools and colleges, but a local college wouldn't sign a deal with my brother without a teacher to train employees. But he knew a teacher—me!

I agreed to do it. At the time, I was twenty-three years old and had nothing to lose. I did have one condition—that IBM would train me on their system so I could develop the course. Not long after, my brother came to me with a new business idea: providing accounting software to small businesses that could be run on Displaywriter, which previously was only used for word processing.

My brother, my husband, and I spent all our spare time programming this new software until we were ready to launch our business:

Microcode. Within five years, I started a training department at Microcode, which was eventually recognized as one of North America's largest Microsoft Training Centers. In 1998, Microcode's training center was sold to Canadian telecom giant Telus Business Solutions.

After that, I knew I needed to create something new in training and IT—a solution-oriented company to scale internationally. As a result, I formed Terranova Security in 2001 and brought its first security awareness training course to the market in 2003.

Timing Is Everything

The moment couldn't have been riper for me to lay the foundations of my business. As the internet's popularity grew, so did instances of fraud and cyber crime. Companies and individuals alike were taking notice—they knew they needed to train employees on cyber security best practices as soon as possible. Harnessing this sense of urgency is one of the many steps required to succeed in behavior change—you must help others see the need for change and the importance of taking immediate action.

Unfortunately, urgency alone is not sufficient for success. Research from McKinsey and Company shows that 70 percent of all transformations fail. Why? For many reasons: a weak culture that isn't aligned with the mission, lack of participation and buy-in, undercommunicating a powerful vision, overcommunicating a poor vision, insufficient training or resources, and so on.[1] The more we implemented security

1 Harry Robinson, "Why Do Most Transformations Fail? A Conversation with Harry Robinson," McKinsey & Company, July 10, 2019, https://www.mckinsey.com/capabilities/transformation/our-insights/why-do-most-transformations-fail-a-conversation-with-harry-robinson.

awareness programs, the clearer the need for a comprehensive framework to help Chief Information Security Officers (CISOs) became.

Although this era gave birth to many excellent technology security firms, I decided to focus on the people aspect.

Terranova Security Timeline

- November 2001—Terranova Security created.
- 2002—Market analysis completed.
- 2003—Security awareness online course developed.
- September 2003—Security awareness training sold to first clients (grocery chain, pharmaceutical industry).
- 2003–2006—Continued business growth (banks, ATVs, federal and provincial government agencies).
- 2006—Learning Management System and assessment tool developed.
- 2007—Awareness training for building a security-aware culture introduced and targeted to the US market.
- 2009—European and worldwide services offered.
- 2015—Terranova Security highlighted as an industry leader in its Gartner's Magic Quadrant.
- 2016—New phishing simulation platform developed.
- 2017–2018—New integrated platform developed.
- 2019—First global annual Gone Phishing Tournament™ launched.
- 2019–2021
  - Serious Game training modules and first mobile responsive training library developed.
  - Security Awareness Virtual Summit launched, cosponsored by Microsoft.

    - Cyber Security Hub featuring working-from-home kit launched.
- 2020–2021—Click-and-launch and program blueprints for the quick-and-easy deployment of training programs developed.
- 2021–2022—Content hub, Security Awareness Index, Culture Index, and the Campaign Manager developed.

Do It Right

It's the educator in me, more than any other aspect of my makeup as CEO, that compelled me to author this book. I sincerely believe in offering a product that solves problems, delivers consistent results, and supplies value to clients in all industries. Because of this, I want organizations to invest in training their employees to use technology in a secure way and stop using security awareness as compliance box-ticking. They need to change employee behaviors and instill a security-aware culture in their organization to protect their sensitive information.

INTRODUCTION

"You don't have to be a genius or a visionary or even a college graduate to be successful. You just need a framework and a dream."

—**MICHAEL DELL**

As the number of cyber attacks continues to rise worldwide, security departments face increased pressure. The most significant new trend—working remotely—introduces new cyber security challenges that many organizations don't know how to tackle on their own.

According to Stéphane Nappo, Vice President Global Chief Information Security Officer, Groupe SEB: "Education has always been a profit-enabler for individuals and the corporation. Education, both conception and delivery, must evolve quickly and radically to keep pace with digital transition. Education is a part of the digital equation."

Periods of change such as this one offer opportunities to implement a comprehensive security awareness training plan that both mitigate risk and feeds into a cyber security-aware organizational culture.

Cyber crime is reaching ever-higher levels and infiltrating more areas of our lives than we ever imagined was possible. We are all

concerned. We are all targets. We are all being affected, businesses and consumers alike.

In light of this threat, you must ensure your employees recognize the dangers and know how to defend against them. You can do that by heightening awareness of the human risk factors and holding your employees accountable for protecting the data and systems they have access to.

The Impact(s) of a Security Breach

Cyber attacks have a significant impact on individuals, organizations, and the professionals who serve them.

Impact on the Individual

Criminals can use information like social security numbers, birth dates, healthcare information, and credit card information to commit identity theft, disrupt lives, and push people into financial ruin. Personal data reflect real people's lives. Shielding a person's data is the same as protecting the individual.

Impact on Your Organization

In addition to the devastating economic impact a breach can have on your organization, there are also nonfinancial repercussions to consider. For instance, you may face loss of credibility, revealed trade secrets, or drops in market value.

Impact on Your Cyber Security Professionals

Cyber security professionals have the daunting task of protecting against a myriad of cyber attacks with limited resources, while cyber

criminals are often well funded and have access to all the time and tools they need to achieve their goals. And yet, when something goes wrong, cyber security and other executive leaders are often blamed for not implementing adequate protections. They need the support of every manager and user in the organization.

Security awareness is an incredibly vital component of an effective security plan. To avoid these impacts, we need to address human risk.

How Do We Address Human Risk?

You may already understand the importance of protecting your organization, your customers, and yourself from the harmful effects of an information security breach, but what are you doing about it? This human risk factor, the most significant point of vulnerability, is often called the "weakest link," but it might be more appropriately called the "neglected link" because many security strategies leave it unaddressed.

Fortunately, you can turn the human element into the "strongest link" and make people part of your cyber security defense strategy by developing a security awareness mindset throughout your organization. Security awareness must be more than a set of rules your people follow; it must be deeply understood so that alertness and attentiveness become second nature.

In other words, it isn't enough for the people in your organization to go through the motions of security awareness training. They actually have to put their new knowledge into action, staying alert to new threats and keeping data secure over the long term.

There are countless reasons why security awareness programs fail to effectively reduce security breaches, including:

1. Security awareness is regarded as a project, not as an ongoing process.
2. We start at the deployment phase, releasing online courses and/or videos without proper analysis and planning.
3. We only want to check the box of compliance.
4. We don't establish a baseline to determine priorities.
5. We don't set goals for our program and campaigns.
6. We don't establish key performance indicators (KPIs) or measure results.
7. We don't make our campaigns exciting and interactive for participants.
8. We don't customize content to reflect our organization's or audience's reality.
9. We don't engage the proper stakeholder and contributors.
10. We don't allocate the proper human resources with the right skillset to manage the program.

To succeed in changing human risk behaviors, we need to do things differently. We need to instill strong security awareness programs using a proven framework and apply a people-centric approach. The framework I provide in this book will give you the tools and the structure to do it right the first time, by forcing you to analyze critical factors before starting, plan strategically, and measure results to improve your approach. Although comprehensive, the framework is also easy to follow because it lays out a series of checkpoints to ensure that you stay on track and that your program is successful.

Behavior and Culture Change

If you handle security awareness, you are in the business of creating behavioral change and developing a culture of security in your organization. You are trying to get people to change their habits to adopt secure behaviors—not a simple task.

If you want to change people's behaviors, you need to do more than ask them to do fifteen minutes of intermittent training or sit down in front of their computers for an hour once a year. Security must stay top of mind. To support that constant awareness, you need to roll out a complete program of multiple smaller campaigns.

How does culture change happen? Consider the nearly ubiquitous use of seat belts in cars over the past twenty or thirty years.

When I was a kid, we weren't too concerned about seat belts. The family car didn't even have seat belts in the back seat. But today, everyone agrees seat belts are important. The first thing we do when we get in the car is buckle up.

So what changed? We were slowly exposed to the idea that buckling up would save lives. We started seeing awareness ads everywhere, citing statistics, laws, and benefits. The public service announcements on television and radio were persistent, intense, and frequent. Over time, we integrated this new knowledge into action.

The lesson here is that **you must use repetition and reinforcement to change behaviors**.

And you must continually communicate security awareness best practices by a variety of means, including:

- *Storytelling*: Telling a story is particularly useful if it is a story that speaks to both sides of the brain: emotional and

rational. People will join and mobilize if it makes sense to them.

- *Communication*: Making a cultural change takes a lot of communication. In the tech world, we often use the ADKAR change management model:
  - *Awareness*: Ensure everyone in your organization understands the need for change.
  - *Desire*: Make your case so that everyone involved wants the change.
  - *Knowledge*: Provide the information each person needs on how to accomplish their part of the change process.
  - *Ability*: Make sure all employees have the skills and training they need to successfully do their part.
  - *Reinforcement*: Continue to work with employees and stakeholders after the change is accomplished to make sure they stay on top of doing things the new way.[1]

Change Is a Process, Not a Project

To effectively change behaviors and build a security culture throughout your organization, you must view security awareness not as a project but as an ongoing process.

Often, during a change, we communicate information and expect that people will immediately adapt. However, several studies say that it takes two months (and not twenty-one days as we have often heard)

1 Kristen Hicks, "Top 8 Change Management Models: A Comparison Guide," *Zendesk Blog*, May 12, 2020, https://www.zendesk.com/blog/change-management-models/.

to change behavior. So don't underestimate the importance of the steps employees must take and the time they need to make this lasting behavior change.

It is essential to understand the stages of adopting a change:

- Step 1: Awareness (I am informed.)
- Step 2: Understanding (I understand.)
- Step 3: Acceptance (I accept.)
- Step 4: Adoption (I put it into practice.)
- Step 5: Integration (I do things according to the new standards.)

To build a comprehensive program, you also need to have a clear vision of your organization's specific objectives and communicate it internally. Achieving those objectives will require you to create individualized learning paths based on an end user's role, responsibilities, and requirements, both in terms of prior knowledge and the risk levels associated with their profile.

Your awareness training campaigns also act as internal marketing for a security-aware organizational culture. Prepare a persuasive communication plan and make sure there's a consistent drumbeat of security-centric messaging that employees receive and engage with.

Proper tracking metrics are also required to ensure you can report accurately on program performance. The data you record will allow you to adjust your priorities down the road and implement improvements to reach your objectives.

The Terranova Security Awareness 5-Step Framework was created to help you with all of these initiatives and more. Without it, creating a strategy, communicating the right messages, and tying them to your cyber security culture will be far more challenging.

Terranova Security Awareness 5-Step Framework Overview

Before Deployment

Step 1—Analyze: Take a clear look at your organizational culture, level of security, maturity, target audiences, employee motivation, strategic goals, compliance obligations, and other external, internal, or industry drivers for your awareness program.

Gathering this information will enable you to complete ***Step 2—Plan***. In this step, you will make strategic decisions about defining your campaigns—particularly the objectives and KPIs of each campaign—so you can measure your success compared to your goals.

During Deployment

Step 3—Deploy: Prepare and deploy all the learning, reinforcement, and communication activities that you identified for the campaigns. Before kickoff, do pilot testing to ensure the campaign runs smoothly without any technical issues. During the campaign, send reinforcement to each user, tailored to their results.

Security awareness training deployment should be automated based on risk and knowledge levels. These data points are collected using a feature like our Security Culture Index, which allows organizations to quickly identify high-risk users or profiles, pinpoint specific behavior change areas, and personalize the resulting training campaigns to suit those unique realities.

Based on their performance and risk levels, users may be:

- Assigned additional training
- Engaged with more frequent feedback and touch points
- Included in additional phishing simulations

Combining personalized risk scoring with automated, risk-based campaigns directly tied to a user's or profile's unique knowledge and risk levels gives organizations increased flexibility in their awareness training. By tailoring the learning paths and training campaigns to target specific end user behaviors, security leaders can feel confident that their awareness training will reduce risk and foster a cyber-aware culture across all teams, departments, and regions.

After Deployment

Step 4—Measure: Use the metrics and KPIs that you identified in ***Step 2—Plan*** to measure the human risk, evaluate the effectiveness of your campaigns, and determine if they meet your objectives.

Analyzing this information will give you essential insights into how to complete ***Step 5—Optimize***. In this stage, you compare campaign objectives with results and identify new goals so you can tweak subsequent campaigns to make them even more impactful.

Before You Start: Let's Talk Project Management

One of the most significant, yet underrated, aspects of any security awareness program is project and infrastructure resource management. To set your awareness campaigns up for success, you must solidify who will oversee each stage of the process and how each aspect will be executed.

If you don't assign a dedicated project manager or, at the very least, designate a led-by-committee process at the outset, you may set your security awareness initiatives up for failure. If project management processes aren't ironed out, then entire campaigns may never be launched, ultimately leading to an unrealized return on investment (ROI).

To help you navigate the initial project management setup, use the following checklist as a directional guide.

Security Awareness Project Management Checklist

Analysis and Planning

- Identify priorities and the organization profile.
- Complete any analysis questionnaires.
- Identify project and program roles.
- Propose choice and grouping of topics.
- Review responses to analysis and provide feedback.
- Conduct interviews with stakeholders.
- Prepare awareness plans.
- Present strategy to senior leadership team.

Platform and Content Preparation

- Identify platform administrators.
- Upload content based on selection.
- Integrate Single-Sign-On (SSO).
- Import user list (SCIM Provisioning or Excel import).
- Configure IP allow lists for phishing.
- Prepare communications messages.
- Brand with colors, logos, and images of your organization.
- Ensure platform administrators receive appropriate training.

Phishing Simulation Analysis

- Identify scenarios for baseline phishing simulation.
- Obtain approval for scenario selection.
- Inform IT team/SOC of upcoming event.

- Prepare phishing simulation.
- Test phishing simulation.
- Launch phishing simulation.
- Analyze results.
- Present results.

Quiz or Survey Analysis

- Identify questions; evaluate your campaigns' success.
- Prepare communications for the quiz.
- Prepare the quiz.
- Test the quiz.
- Launch the quiz.
- Analyze quiz results.
- Communicate quiz results.

Launch the Awareness Program

- Prepare program announcement.
- Distribute program announcement.
- Launch of the first course.

This book will delve deeper into some aspects of this list, but the important takeaway is that your organization's reality will dictate when, by whom, and how quickly each phase is completed. Coupled with your program's overall maturity level, these techniques will evolve as security awareness engagement increases across all teams.

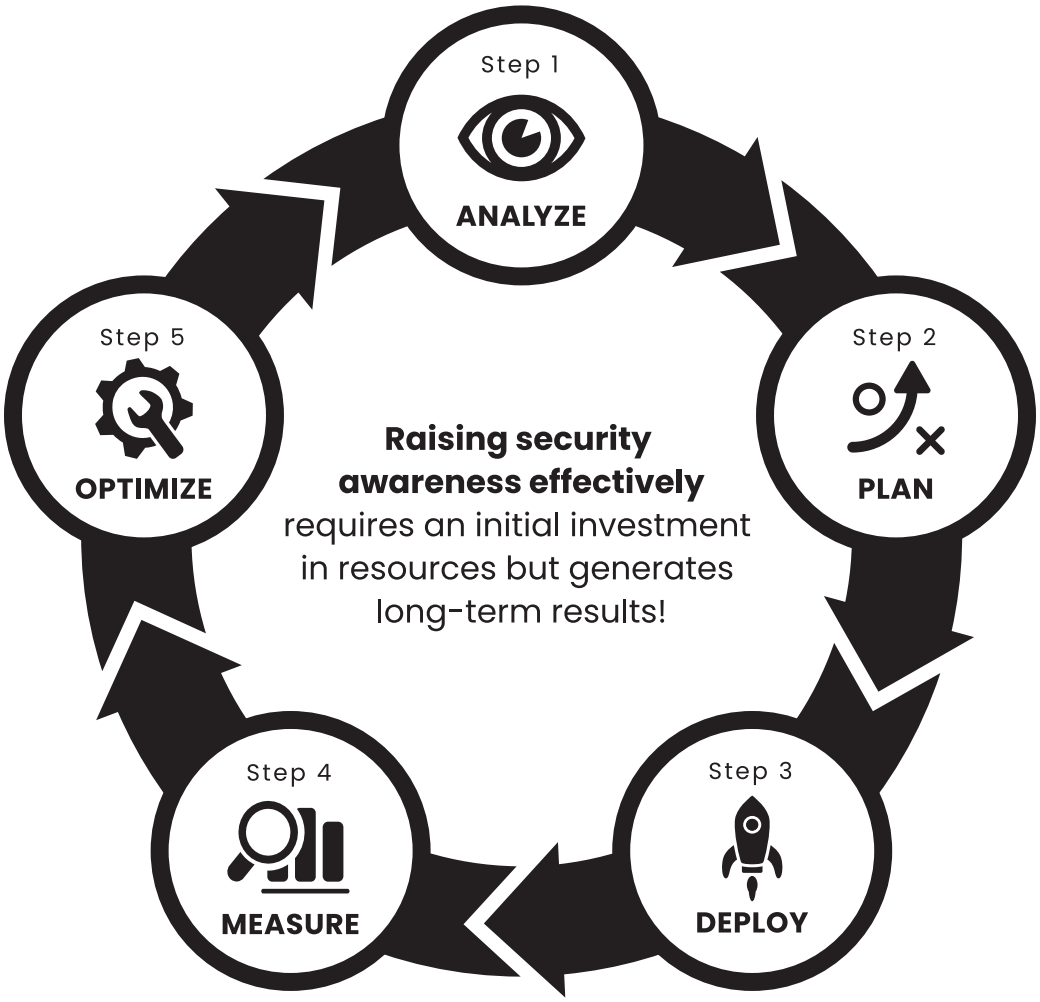
If you complete the checklist, that doesn't mean your security awareness program is set up for good. You must begin again at the top and, depending on your cyber security goals for the fiscal year or quarter, relaunch each stage of the project management accordingly.

Focused on Your Success

At Terranova Security, our clients are our partners. My team and I want your people to adopt a security mindset and protect your organization from breaches. I take it to heart, so much so that I have built my entire business on it.

We want you to succeed. Let's get started.

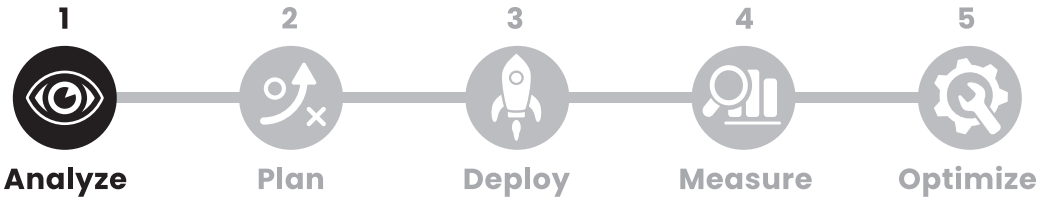
Welcome to the Terranova Security Awareness 5-Step Framework



LAYING A SOLID FOUNDATION IS ESSENTIAL TO THE SUCCESS OF YOUR SECURITY AWARENESS PROGRAM.

ONE

STEP 1: ANALYZE



Welcome to Step 1 of the Terranova Security Awareness 5-Step Framework—Analyze.

No matter how big or small your organization is, analysis is essential. It provides you with crucial insights required to create and implement a security awareness program that addresses the actual needs of your current organizational culture and environment.

You need to analyze, but you don't need to overthink this. In this book, I provide you with most of the questions you need to ask in the analysis stage. You can dig deeper in your analysis and focus on the details that will allow you to deliver an effective and successful security awareness program. Terranova Security can also offer consultation services to help you with the analysis phase. Our platform, using Campaign Builder, enables you to automate the complete process.

You need to devise a tailor-made program for your organization. Your organizational culture is different from the one down the street, and so are your risk factors, staff motivation levels, compliance obligations, internal culture, and ability to deploy a program.

It is essential to take a step back to find a solution that fits—one that will lead to behavioral change among the people at your organization. One that harnesses their strengths and addresses their weaknesses, such as motivation to learn and gaps in their security awareness understanding.

In this first step of the Terranova Security Awareness 5-Step Framework, you will determine your strategic program goals. These broad high-level goals are the primary outcomes you intend to achieve through your security awareness program.

You will also look at a range of factors relevant to your organization. You will identify risks, your target audiences, their motivation to participate in your program, compliance obligations, the topics you need to cover, and your primary data-gathering categories. Furthermore, you will assess your organization's current level of security awareness and its capacity to deploy awareness activities, as well as determine the resources and budget you will need.

The data you gather now will give you all the information you need to build your plan in Step 2.

Starting Your Analysis

Take some time now to reflect on the following questions. Doing this exercise now will guide your thinking, and the direction of your program will begin to appear.

Consult with people in your organization, if necessary, to get as complete a picture as possible. Don't hesitate to consult a substantial number of people in the organization; both "positive" and "negative/critical" people can provide valuable information. It is important to collect the different views.

Your analysis should focus on twelve primary data-gathering categories:

1. Program Drivers
2. Goals
3. Compliance
4. Target Audiences
5. Level of Maturity
6. Level of Knowledge and Behavior
7. Motivation and Culture
8. Scope of Your Program
9. Additional Inputs
10. Support Resources
11. Globalization
12. Costs

1. Program Drivers

The first vital step in constructing a cyber security awareness program relevant to your organization is to ask yourself the "why" questions. You're defining your awareness initiatives' purpose(s) and the expected benefits. How you centralize all these considerations will depend on your program, external, and industry drivers.

Program Drivers

These drivers will influence the strategic objectives you choose to pursue and how you measure program effectiveness. To ensure thorough preparation and decision making, consider all drivers, whether you are working with a preexisting list or discovering them via a quiz in the Terranova Security Awareness Platform.

External Drivers

The external drivers are elements that organizations may not have complete control over, yet they impact organizations and expectations from their employees. These can include (but are not limited to):

- Cloud adoption and reliance
- Dependency on external development and supply chain partners
- Accelerated technology growth (e.g., blockchain, Internet of Things, etc.)
- Hyperconnected world, productivity apps and devices used, and time spent online
- Increased complexity, frequency, and consequence severity of cyber attacks

- Global regulatory laws focusing on information protection and data privacy

Industry Drivers

Certain drivers for key stakeholders are purely industry based. These reflect an organization's reality regarding compliance, data privacy, information security standards, and technological norms specific to their sector. As a result, security leaders in healthcare will have different considerations than those working in IT or finance.

Industry drivers break down as follows:

- Personal data protection requirements
- Cyber threats that can target sensitive information in each sector
- Established procedures for handling personal data

When looking at industry drivers, it can also be useful to compare your security awareness performance and/or cyber security policies to those of similar parties in the same sector. This process can provide relevant benchmarks and establish data-driven insights.

Internal Drivers

This list of internal drivers is your starting point; it will continue to evolve alongside your awareness program. Campaigns and initiatives will address these factors, especially those impacting safeguarding information assets and cyber attack prevention.

- Information assets: information classification and handling
- Cyber attacks: phishing, social engineering, ransomware, and others

- Incident management: incident reporting and related processes
- Increased organizational agility: continuous program reinforcement
- Alignment with your overall mandate: defined organizational objectives
- Culture considerations: motivating users to learn and apply knowledge

Internal drivers will also change based on your organization's financial and operational outlook, both now and down the road. It's important to revisit all three driver categories to ensure the most pertinent information shapes your security awareness strategy.

2. Goals

Now that your drivers have been established and you've begun solidifying your organization's short- and long-term needs, you must create your strategic goals.

Although industry and region-based requirements should be considered, your security awareness goals must also suit your organization's unique definition of success and future outlook. In other words, there's no one-size-fits-all solution to crafting strategic goals.

It is essential to clearly identify what you aim to achieve. Your strategic program goals must be concrete and tangible, not vague and ambiguous.

Outlining what you intend to achieve will help you get all the key players on board, including any decision makers who must approve or fund your program and the people you want on your team to support the initiative.

EXERCISE

IDENTIFY YOUR DRIVERS

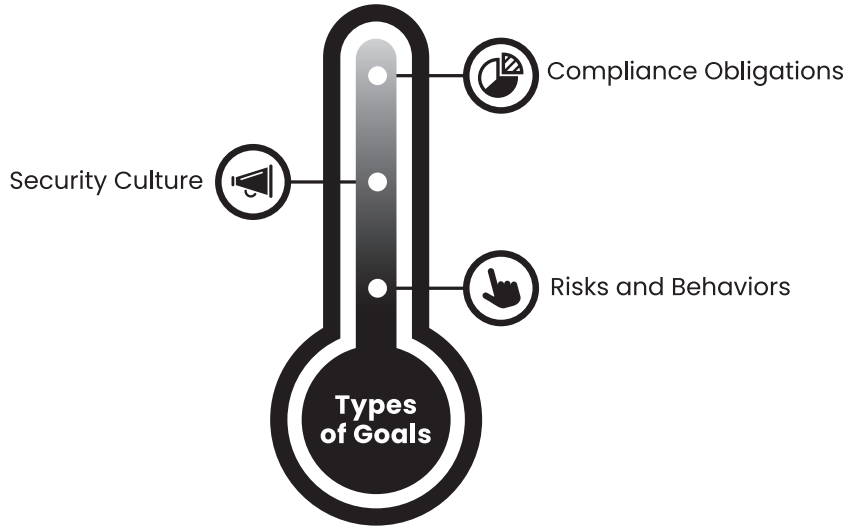
Write down your security awareness program drivers.

1. Identify 3 to 5 external drivers that may affect your awareness program implementation. Examples:
    a. Transitioning IT services to cloud service providers.
    b. Adoption of new technology to deliver products and services
    c. Increased reliance on partners and suppliers to deliver products and services.
    d. New or modified laws and regulation in area of jurisdiction or targeted client regions.
    e. Increase of threat actor activity against organization.

2. Identify 1 to 2 industry drivers that may affect your awareness program implementation. Examples:
    a. Processing large number of records containing personal information.
    b. Industry standards and best practices defined for our sector.
    c. Processing large number of records containing financial.
    d. Organization qualifies as critical infrastructure.
    e. Increase of threat actor activity against sector.

3. Identify 3 to 5 internal drivers that may affect your awareness program implementation. Examples:
    a. Requirements for information classification and protection according to organizational policies.
    b. Reduce the occurrence of employees falling victim to cyber attacks.
    c. Create a cyber security aware culture across all levels of the organization.
    d. Communicate requirements and responsibilities as defined in organizational security policies.
    e. Inform existing and new employees on the cyber threats and best practices associated with the use of technology.

Defining Your Strategic Program Goals



Categories of Strategic Program Goals

Your strategic security awareness program goals might belong in any or all of these three categories:

- Risks and behaviors to reduce risk and instill behavioral changes
- Security culture to instill or reinforce a culture of security
- Compliance obligations to ensure compliance with your organization's security obligations

Tip: Clearly defined, concrete program goals are essential. They will enable you to plan strategically and develop a security awareness program that is focused on producing tangible results.

EXERCISE

DEFINE YOUR STRATEGIC PROGRAM GOALS

What are the strategic goals of your security awareness program? Identify ALL the goals that apply:

Risks and Behaviors

Your goals could be to reduce risk and foster behavioral changes such as:

- Reducing human errors
- Applying security best practices
- Reducing end user-related security incidents
- Making positive changes in security-related behaviors and decisions
- Addressing the rapid changes in the organization's threat landscape

Security Culture

Your goals could be to instill or reinforce a culture of security by:

- Demonstrating the importance of information security
- Mobilizing managers as security and awareness ambassadors
- Changing end users' attitudes toward security
- Encouraging end users to consider the security implications of their actions
- Ensuring end users understand their responsibilities about protecting information assets

3. Compliance

All around the world, there are increasingly enforceable security-related regulations you must consider and contractual obligations you may have to fulfill for activities such as credit card processing.

Compiling your organization's compliance obligations will help you design a laser-focused program that meets all requirements and avoids

any oversights or omissions. What's more, completing this part of the process will help you find the specific target audiences you will need to include in the different campaigns of your security awareness program.

It is essential to note whether your target audiences need both compliance and security awareness training:

- Compliance-specific awareness covers training on the policies and procedures required by regulation for protected information.
- Security awareness covers standard security policies and procedures to prevent, detect, contain, and resolve security incidents.

Key Compliance Obligations

- Contractual obligations
- Governmental regulations
- Industry-related obligations
- Financial services
- Healthcare
- Manufacturing
- Energy and power
- Automotive
- Retail
- Critical infrastructure
- Privacy obligations

EXERCISE

IDENTIFYING YOUR COMPLIANCE OBLIGATIONS

Specify the name of the obligation and the essential requirements you need to include when planning your security awareness program. Identify all the obligations that apply to your organization.

- Contractual obligations
  - Client
  - Partner
  - ISO/IEC 27001:2013 (most referenced standard by many sectors)
- Governmental regulations
  - Personal Health Information (PHI), Personally Identifying Information (PII)
  - GDPR
  - Other country- or region-specific regulation
- Industry-related obligations
  - PCI-DSS
  - NERC
  - HIPAA/HITECH
  - Other industry

4. Target Audiences

When you implement a security awareness program, you are essentially working in the field of change management, helping people adopt and apply security best practices in their day-to-day work. Specifically, you want them to recognize the importance of security awareness, understand their role, and complete the awareness campaign willingly.

Changing behaviors is the name of the game. To achieve that, you must adapt your language and message to those you are talking to. If you want everyone to be enthusiastic, you must speak their language.

Who Are Your Target Audiences?

Any potential data breaches will have varying levels of severity depending on the individual, role, or department targeted within the company's hierarchy. Because everyone's cyber security knowledge will differ, train the person responsible for various compliance and security-related tasks accordingly.

Consider all those in specialized roles within your organization, such as the accounts receivable staff who process payments, a business unit with specific security challenges, or an employee with a standardized role. An example would be a cashier with PCI DSS compliance duties or a receptionist who buzzes in visitors.

Then adapt different training paths according to specific roles and responsibilities.

By offering training and simulations that are concrete and practical, with real cases where the participant must respond to his or her mistakes on the spot, you make it easier for the participant to understand the relevance of the lesson.

IMPORTANT NOTE ON THIRD PARTIES

Although not your primary focus, you should also keep in mind all those who do business with your organization—third parties who may have access to your sensitive information, either physically or electronically, or those who visit your premises or work for you off-site.

In this book, I address third parties in much the same way as those with a specialized role in your organization.

Your In-House Target Audiences

Executives

Executives and upper management must be aware of their organization's risks so they can support and fund security awareness initiatives. Executives must be ready in case they are questioned to this effect by the board of directors or the advisory committee during a risk meeting.

Managers

Raising managers' awareness about the organization's risks should mobilize them to act as ambassadors and security role models.

End Users (General Staff)

Your program should increase end users' understanding of security threats and communicate the best practices and behaviors you want them to adopt.

IT Staff

How you raise awareness about IT security among the IT staff will depend on your organization's information security best practices, the network, systems, and application vulnerabilities in your environment.

Specific Business Roles (People in the Various Functions or Departments of Your Organization)

Raising awareness about information security for specific roles will depend on your organization's structure, possible threats, or the regulations they must follow.

In other words, the question is, what people in which departments? See the following list as a starting point:

- HR
- Sales
- Marketing
- Legal
- Finance
- IT/Development
- Support
- Product
- Operations
- Third parties
- Contractors
- Clients
- Other

Third Parties: Additional Specialized Roles

Contractors

Contractors should be considered the same as direct, permanent employees and should have security awareness. This includes freelancers, consultants, interim workers, temporary staff, or service providers who work for your company either on your premises or off-site.

Business Partners

You may take all the necessary information security precautions, but are your partners or associates doing the same? Business partners must have the same security awareness level to ensure that the information you share is safe and confidential.

Clients

You may want to offer data security tips to your clients as an added value. An excellent example would be a bank or internet service provider offering suggestions to help protect clients from fraud and theft. This would also help reduce the number of incidents the organization has to process.

University Professors and Students

In many situations, professors and students have access to a university's systems or research that must remain protected. Therefore, faculty, staff, and students must participate in security awareness campaigns.

Suppliers

A business can be a bustling place. Suppliers are coming and going all day long or may be offering specific services and there may be specific security procedures you need them to be aware of and follow.

EXERCISE

IDENTIFYING YOUR TARGET AUDIENCES

Review the target audiences outlined in the previous section and identify all those target audiences that are applicable to you.

Groups of People Who Work for Your Organization

- Executives
- Managers
- End users (general staff)
- IT staff
- Specialized internal roles (people in various functions or departments of your organization)

Additional Specialized Roles—Third Parties

- Contractors
- Business partners
- Clients
- University professors and students
- Suppliers

5. Level of Maturity

The importance of assessing an awareness program's maturity cannot be underestimated as part of the development and strategy processes. It will influence the resulting security awareness campaigns' efficiency, productivity, risk levels, and overall performance ceiling.

Terranova Security aligns with the recognized Capability Maturity Model Integration (CMMI) method of streamlining process improvement and encouraging continuous program growth and development.

The CMMI model helps organizations of all sizes boost their performance and breaks them down into the following categories:

Level 0: Incomplete

At this level of maturity, the desired outcome may or may not be reached based on the processes (or the lack thereof) in place. This procedural state stems from goals not being established, and if processes are in place, they don't support the organization's needs or current mandate.

Level 1: Initial

This maturity level is often associated with reactive processes and initiatives. At this stage, an organization's work environment may feel unpredictable or volatile, with completed projects often delayed and delivered disjointedly. As a result, inefficiency and corresponding risk levels increase dramatically.

Level 2: Managed

The project management waters become far less choppy when an organization reaches this maturity level. Even though there are still efficiency and performance issues to address, projects are increasingly planned and controlled, and performance is measured to a greater degree. Because of this, risk levels decrease but don't disappear completely.

Level 3: Defined

Getting to this state ensures that an organization's project management has turned a corner and become more proactive than reactive. Typically, organization-wide standards and policies provide high-level

guidance across different programs and portfolios. Organizations also better understand their goals, improvement areas, and how the latter can help them better attain the former.

Level 4: Quantitatively Managed

At this level of maturity, an organization's processes are at near-optimal levels of control and proactive measurement. Using quantitative data, we can define actions and initiatives that best support the needs and goals of different teams and stakeholders. Due to these data-driven insights, the organization can spot deficiencies more easily and sidestep resulting risks.

Level 5: Optimizing

At this stage, an organization's processes are a well-oiled machine—durable, secure, and flexible enough to adapt to the marketplace and internal changes. From this point, they will continuously improve, responding to minor performance issues with agile innovation in mind.

Many organizations start at the lower maturity levels. At these levels, security awareness is usually focused on the tactical steps to secure business activities or meet regulatory compliance mandates. Organizations generally recognize the business risks due to user vulnerabilities but lack clearly defined security policies or procedures.

In these stages, most security awareness activities are reactive—they happen in response to incidents, rather than emerging from a proactive program with defined objectives. In most organizations with a low level of maturity, accountability for security awareness is

assigned to an IT security analyst, with little involvement or buy-in from senior executives. As maturity increases, organizations begin to embed information security into the company culture. Security policies and procedures are documented and reviewed, with adequate delivery mechanisms to enable awareness and compliance. Organizations with a medium level of maturity usually manage awareness activities centrally, by leveraging solutions for training and/or phishing simulations. At the highest maturity levels, organizations have control over the security awareness needs of the organization, responsiveness to evolving threats, solid monitoring of the program, and benchmarking of program performance. Security awareness program metrics are collected, and the program is regularly reviewed and updated. Information security is embedded into the organization's culture, with high participation rates, executive support, and orchestrated activities across all levels of the organization.

No matter your security awareness program's maturity level, the Terranova Security Awareness 5-Step Framework ensures you have a blueprint for creating and deploying initiatives that make sense for your organization. Because the blueprint's steps are rooted in proven behavior change methodologies, your awareness initiatives will support your organization's goals and ensure you can evolve your information security practices to meet regional, industrial, and other standards.

To confirm the program maturity level, you can evaluate the level of knowledge, behavior, and culture of your organization using quizzes (surveys) and establish your baseline using a phishing simulation.

EXERCISE

SECURITY AWARENESS PROGRAM MATURITY

Your security awareness program maturity level is the first key indicator of what you may need to do to create a culture of secure behavior across your organization.

What steps do you take in building an awareness program?

- Analyze user behaviors and knowledge (e.g., survey, phishing simulation).
- Consult with business stakeholders.
- Seek input from internal assessment and audits.
- Review internal metrics (e.g., incident reports).
- Review public security reports.

Which audience is included in your program?

- Current users
- New hires
- Temporary employees
- Partners/suppliers
- Clients

Which departments contribute to the implementation of your ISA program?

- IT Security
- HR
- Communications
- Change Management
- Legal/Privacy

How do you distribute training based on your audience?

- General training for all employees
- Targeted training based on function (e.g., HR, IT)
- Targeted training based on technology or risk exposure
- Manager training
- Executive training

continued...

EXERCISE

What activities are part of your awareness program?

- E-learning
- Phishing simulations
- Social engineering tests (USB drops, vishing, tailgating)
- Articles/blogs/videos
- Screensavers/desktop images

What elements do you include in your awareness program?

- Best practices
- Corporate policies
- Learning games and exercises
- Real-life scenarios
- Instructions for reporting incidents

What type of metrics do you collect?

- E-learning participation
- Knowledge retention (e.g., via a quiz)
- User behaviors (e.g., simulations, observed)
- Repeat offenders
- Content appreciation by audience

How do you follow up on user's behaviors?

- Negative consequences for insecure behavior
- Positive consequences for secure behavior
- Provide just-in time feedback
- Communicate insecure behaviors at large
- Communicate secure behaviors at large

How are collected metrics used to report on program performance?

- Reporting to ISA program manager
- Reporting to ISA program sponsor
- Reporting to Executive Security Committee
- Reporting to department leads
- Reporting to program audience

continued...

EXERCISE

What steps do you take to optimize your program?

- Review reports and compare against objectives.
- Optimize at least annually.
- Adjust program based on stakeholder feedback.
- Evaluate risk landscape affecting your organization.
- Consider changes of policies, laws, and contractual requirements.

6. Level of Knowledge and Behavior

The most effective learning path will be designed to fill in the knowledge gaps of each target audience. That's why getting a grasp of each target audience's knowledge and understanding of security is critical.

Doing so will allow you to give them new knowledge that will compel them to change their behaviors. After all, acquiring new knowledge is the foundation of change.

Your next task is to measure the level of knowledge for each target audience and identify any knowledge gaps. By completing this task, you will ensure that your choice of security awareness topics aligns with your organization's real-world needs. That means you can design effective course content that will change actual behavior.

To confirm your choice of topics and make a final decision on content, it is essential to compare your assumptions to the reality in the field. Your "assumptions" are the topics you listed per target audience in the previous exercise.

Measuring Your Target Audience's Level of Knowledge

To assess the current level of knowledge of your target audiences, you can use different sources of information:

- Questionnaires
- Simulations: phishing, vishing, smishing, etc.
- Risk analysis and audit reports
- Compliance status reports

Questionnaires

You can create questionnaires in the form of quizzes or surveys.

You might use surveys to assess user behaviors, understand culture, and collect opinions on certain matters (e.g., topics of interest, preferred method of learning, etc.).

You might use an awareness assessment quiz to help you determine the strengths and weaknesses of your target audiences. The quiz can reveal their security awareness knowledge and the gaps between current habits and desired security best practices.

Giving a specific questionnaire to each target group (end users, managers, IT staff, other specialized roles) will allow you to tailor your program to the needs of each group and prioritize content that directly addresses any knowledge gaps they may have. Align your questions with the scope and topics you selected in the previous section.

Phishing Simulations

Another way of assessing your target audience's alertness to cyber crimes and scams is to send out phishing simulations. Essentially, you are testing their awareness levels without their knowledge. Phishing simulations offer a fast, efficient way to measure employee vulnerability and the seriousness of the risk to your organization.

Phishing refers to cyber attacks aiming to obtain confidential information through fraudulent emails and websites. What makes this type of attack so effective is its ever-increasing complexity and people's general lack of awareness or understanding of key warning signs.

The problem is that anyone can execute phishing attacks. They require little work beyond a quick Google search to identify the names and roles of an organization's employees and can easily go unnoticed.

Creating a Phishing Baseline

We always recommend doing an initial simulation in Step 1—Analyze to establish a baseline for comparison purposes following a security awareness campaign deployment. For example, most organizations we work with that perform phishing simulations experience a 20–30 percent simulation failure rate the first time. (That means 20–30 percent of the target users clicked on the fake link!) After training, the organization administers another phishing simulation, hoping to see a lower failure rate.

Recurrent simulations are required to reduce rates to the desired level. Remember, security awareness is not a project but rather an ongoing process.

Because so many people fall prey to this kind of attack, it is crucial to understand how phishing threats operate and learn to spot common tactics. This knowledge is integral to any successful security awareness program. Here are some examples.

Email or Text Message. The most basic phishing attack is an email or text message that appears as if it's coming from a legitimate source. This type of attack doesn't just happen at work. It's also common for these messages to end up in personal inboxes.

Social Engineering. Using information gleaned on social media or through other means, social engineering attacks use specific language to entice their targets to divulge sensitive information. They may refer to coworkers by name or use another type of information that makes them appear trustworthy, making it far more likely their request will elicit a response.

A particularly dangerous strain of phishing attacks is CEO fraud. As the name entails, the criminal passes himself as an organization's CEO and asks for an employee to fulfill an urgent request. The victim, trying to do good and win points with their superior, overlooks the red flags and transmits the required information.

This kind of attack doesn't only compromise personal information; it can lead to direct financial loss. These attacks, which may involve a fake invoice or a request for a wire transfer to a different account, can easily go under the radar and have a devastating impact. Accounting departments rarely know the direct reason behind an invoice.

Ransomware. Ransomware is a type of malware and cyber crime that holds data for ransom. Access to data on computer networks, mobile devices, and servers is locked until the victim pays a ransom.

These attacks are carried out by installing vector ransomware software that takes over the computer and infiltrates the entire computer network, locking everyone out of their computers, the network, and other connected systems.

The goal of ransomware is to convince the victim to pay to unlock their data. Typically, the criminals behind ransomware attacks will demand payment in cryptocurrency because it is largely untraceable. Once the payment is secured, the victim should receive an unlock code or decryption file that releases the data on the computer network, mobile device, or servers.

Spoofing. These attacks use a technological component such as an edited website or malware to pose as a trusted site. The most faked websites are login pages of popular social networks and email providers. These pages are often rather simple looking, easy to replicate, and accessed so often that people hardly look at them anymore. When they enter their login information, that information is transmitted to the hacker. Often, the victim doesn't realize their mistake, even after giving their information, which makes these attacks difficult to detect.

Another prevalent threat comes from fraudulent Wi-Fi hotspots deployed in public places like airports, coffee shops, and shopping malls. Joining a fraudulent Wi-Fi network is enough to give a hacker complete control over a computer and all its data. With more workers doing their tasks remotely, this type of attack will likely increase in popularity.

Phishing attempts happen every day to businesses and individuals alike. The good news is that even though these attacks are highly prevalent, they can easily be avoided through user behavior changes.

A Brief Overview of Risky User Behaviors

The goal of a cyber security awareness program is to modify the main risky user behaviors that lead to successful hacks. Learning these behaviors will help you identify those most present within your organization so you can address them adequately.

Downloading Attachments

Individuals are increasingly inclined to click on or download attachments without closely examining the file or link. This quick action can lead to malware downloading automatically, infecting the computer and any connected systems or networks.

It is vital to look further than the file title and inspect the file extension before downloading an attachment. Hackers will often try to name an executable file something inconspicuous like "Q1 Earnings Report" so the user will open it.

Trusting Website and Email Interactions

Whether clicking on a button or entering a password, users must pay attention to what they are doing. A simple action such as highlighting a URL to check its legitimacy can prevent most issues. They should use similar logic when entering a username and password on a website; verifying that the URL is genuine can prevent most malicious attacks.

Sharing Confidential Personal and Organizational Information

People spend a sizable portion of their days online, which means sharing information digitally is now second nature. So much so that it has led to dangerous situations such as sharing personal financial and company information in plain text over email. If users understand that financial institutions never ask for this kind of information over email and that any organizational transaction has a built-in approval process, they can avoid inappropriate information sharing.

Overlooking Physical Security

As workers spend more and more time out of the office, the odds of lost and stolen devices continue to increase. This trend can become

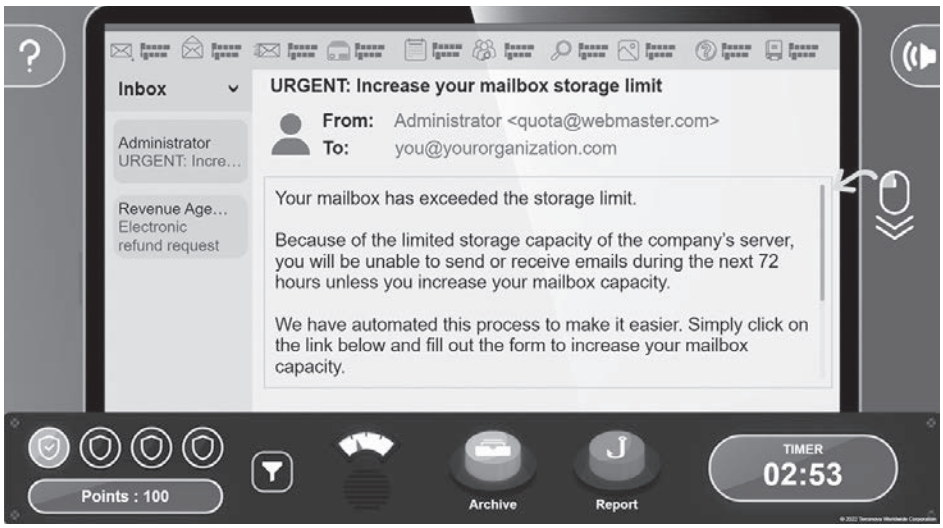
exponentially more dangerous if users keep confidential information on their physical drives. This risk can be mitigated by putting in place a firm policy of cloud data storage for sensitive company documents.

Using Weak Passwords

Although the initial breach might happen via a phishing attempt like the ones outlined earlier, such a breach can be contained to that one account if users have strong, unique passwords for each account. The real danger comes from repeated passwords.

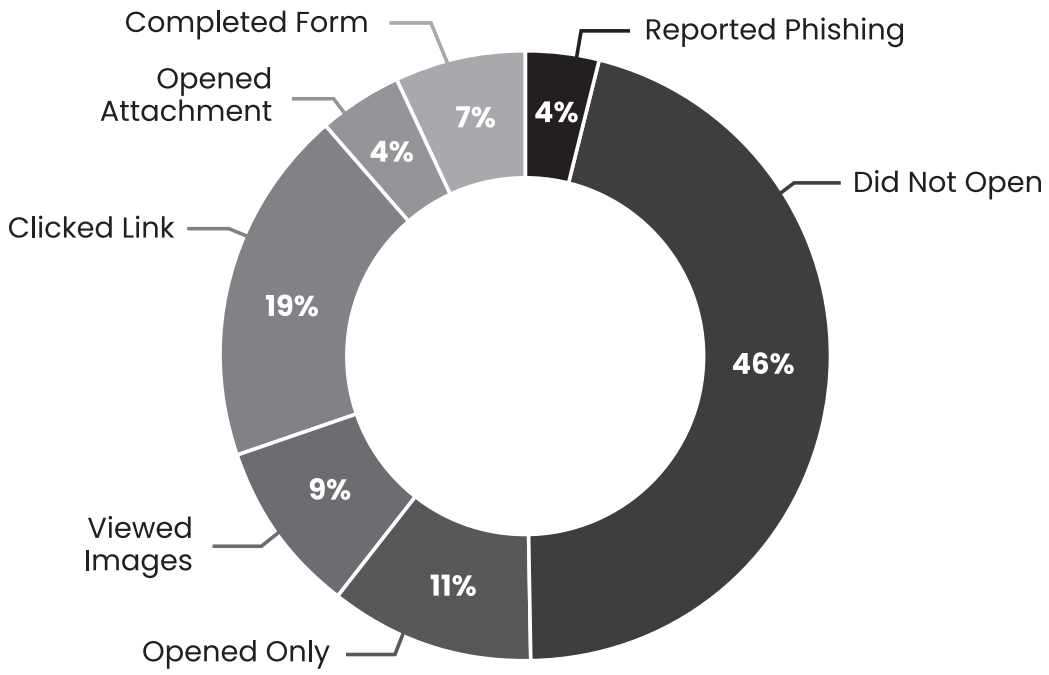
Another common issue is weak passwords. Many people pick passwords that are easy to remember, often including personal information like their birthday or a pet's name. Not only are the resulting passwords often not long enough to be secure, but they're also easy to guess through social engineering and other tactics employed by cyber criminals.

Sample Phishing Simulations Used to Assess Current Security Awareness Knowledge



Phishing Dashboard Showing Where Your Organization Is at Risk

Recipient Actions Summary



The advantage of using a phishing simulation package, such as the ones we have created at Terranova Security, is that it supplies built-in detailed reporting so you can analyze the results and have tangible evidence of the weaknesses in your security.

EXERCISE

RISK ANALYSIS AND AUDIT REPORTS

All companies, organizations, and even you are under constant threat of cyber attack. Up-to-date risk analysis reports will identify risky behaviors within your organization (e.g., sharing passwords or downloading web documents) that have resulted in security incidents. This analysis will, in turn, help you define your security awareness program goals.

When conducting your analysis, you should compile and assess:

- All security incidents within the past year or since your last security awareness campaign
- Helpdesk support tickets (e.g., malware infections and phishing attacks)
- Physical security incident reports (e.g., theft/loss of devices and tailgating at entrances)

Make a list of all your target audiences and then indicate which surveys, quizzes, and/or phishing simulations you should plan for each.

- Executives
  - Surveys
  - Phishing simulations
  - Interviews
  - Others
- End Users
  - Surveys
  - Phishing simulations
  - Interviews
  - Others
- Managers
  - Surveys
  - Phishing simulations
  - Interviews
  - Others

EXERCISE

COMPLIANCE STATUS REPORTS

If you have gone through all the exercises in the book sequentially, you have already listed all the compliance obligations your organization must meet.

Compliance obligations can be regulatory, contractual, industry-related, privacy-based, or financial. Many of them require annual assessments or compliance status reporting. These are essential tools to find specific weaknesses that need to be corrected. Some, such as PCI DSS or GDPR, require compliance awareness training.

- Make a list of all relevant reports regarding your organization's or industry's security incidents or threats.
    - Public research reports
        - Research reports from security firms identify user behaviors that lead to information security incidents
    - Internal audit reports
    - External audit reports
    - Compliance reports
        - SOC 2 Type 2
        - ISO 27000 Series
        - NIST CSF

  Tip: The most effective security awareness program will be one designed to fill in the knowledge gaps of each individual and target audience.

- List all your organization's compliance obligations and any available compliance status reports.

7. Motivation and Culture

How motivated are people to change how they do things and adopt best practices to protect your organization against cyber attacks?

When a person receives information about risk, their brain will analyze it on two levels (more or less consciously):

1. Is the threat credible? Am I affected by this risk?
2. Can I implement the recommendations? Do I feel capable of doing it?

To change a behavior, a person must want it; they have to be motivated.

Being motivated is nothing more than perceiving more advantages than disadvantages. If my change in behavior allows me to reduce the risk of injury (advantage), but it also means I waste more time and lower productivity (disadvantages), I'm unlikely to change my behavior.

Remember the example of drivers wearing seat belts? Some drivers are motivated to wear a seat belt because they believe it will save their life. They are highly motivated by this advantage. Others won't participate no matter how hard you try to convince them to buckle up

because they perceive the disadvantages, such as discomfort, to outweigh the possible advantages.

You will surely encounter a spectrum of motivation levels throughout your organization. This is perfectly normal. Some people are motivated; others are not. It is typical human behavior, and you will have to deal with the variations.

And that is exactly why a strong communication plan is critical to your program's success. Marketing your security awareness initiatives to a variety of audiences is just as important as deploying them since it helps promote the value in changing behaviors. Even more crucially, it helps people shift to a security-first mindset.

The denser and more frequent your security awareness campaigns, the more important clear, engaging reinforcement communication becomes.

Making It All about Them

One of our clients, a small corporation located a few hours outside a major urban center, has about 200 employees. This company is an essential employer in the region; the local population depends on it and it depends on the local population. They came to us for assistance, and together, we created a "Lunch and Learn" conference for all employees.

Given this corporation's set-in-their-ways culture, it would prove exceedingly difficult to impose behavioral changes to reduce the security risks faced by the company.

But if employees change their behavior in their personal lives to protect themselves, they will instinctively employ the same best practices at work. Thanks to the danger signs discussed during the Lunch and Learn, they would pause and say, "Wait for a second; this doesn't look quite right."

Understanding the Role of Motivation

Motivation is key to influencing behavioral change. You must get your target audiences to want to participate.

When implementing your security awareness program and campaigns, you may face resistance from your target audiences, especially if part of your campaign involves exercises unrelated to their jobs. They might, as a result, underestimate their responsibilities and the impact of their actions on your organization's overall IT security.

Several reasons your target audiences may not be motivated to participate in your security awareness program include:

- Training is not mandatory.
- The importance of security is not adequately communicated.
- They feel they already know everything.
- They think it is a waste of time.
- They have a heavy workload.
- They don't understand the benefit.
- There are union restrictions.
- They are not interested in changing.

Want to know if there is room for error in the company? Suppose an employee realizes they have made a mistake (e.g., clicking on a fraudulent link). Will they try to hide their mistake because they are afraid of repercussions, or on the contrary, will they go to see the superior to declare it? Will they try together to find a solution and ensure that the behavior does not repeat itself?

Motivation is also influenced by organizational culture.

EXERCISE

ASSESSING MOTIVATION

Motivation plays a fundamental role in your security awareness program. You, therefore, must determine:

- How motivated are your target audiences to participate in your security awareness program?
- How can you motivate them when motivation is low (amotivation)?

Create a working group with people from various departments to discuss and find solutions to the elements that will emerge from the survey. These people will later become excellent ambassadors of change. The mistake often made in change is that it is only the top management who is involved, but it is in our best interests to include people from different hierarchical levels and with diverse points of view and experiences.

Survey Objectives

This survey will shed light on two key elements:

1. The number of employees (percentage) in your target audience who do not feel compelled to participate in awareness activities (amotivation).

2. The motivating factors for those who feel compelled to participate. Do they believe that awareness activities will be beneficial (intrinsic motivation)? Are they participating in meeting expectations and fulfilling corporate obligations (extrinsic motivation)?

Suggested Survey Script

"Our company is rolling out a new security awareness program to keep our employees better protected against phishing scams, malware, and other cyber threats."

Please tell us how you feel about the following statements:

1. I would participate in this security awareness program because it is both interesting and will be beneficial for myself and the company.

continued...

EXERCISE

2. I would participate in the security awareness program because I must.
3. There may be good reasons to do this activity, but I do not see any.

Scoring and Interpreting Your Results

The results collected using questions like these will illuminate one of the following patterns:

1. More agreement with question #1 shows intrinsic motivation—*Motivated/See benefits*.
2. More agreement with question #2 indicates extrinsic motivation—*Motivated/Obligated*.
3. More agreement with question #3 demonstrates amotivation—*Not motivated/Not interested*.

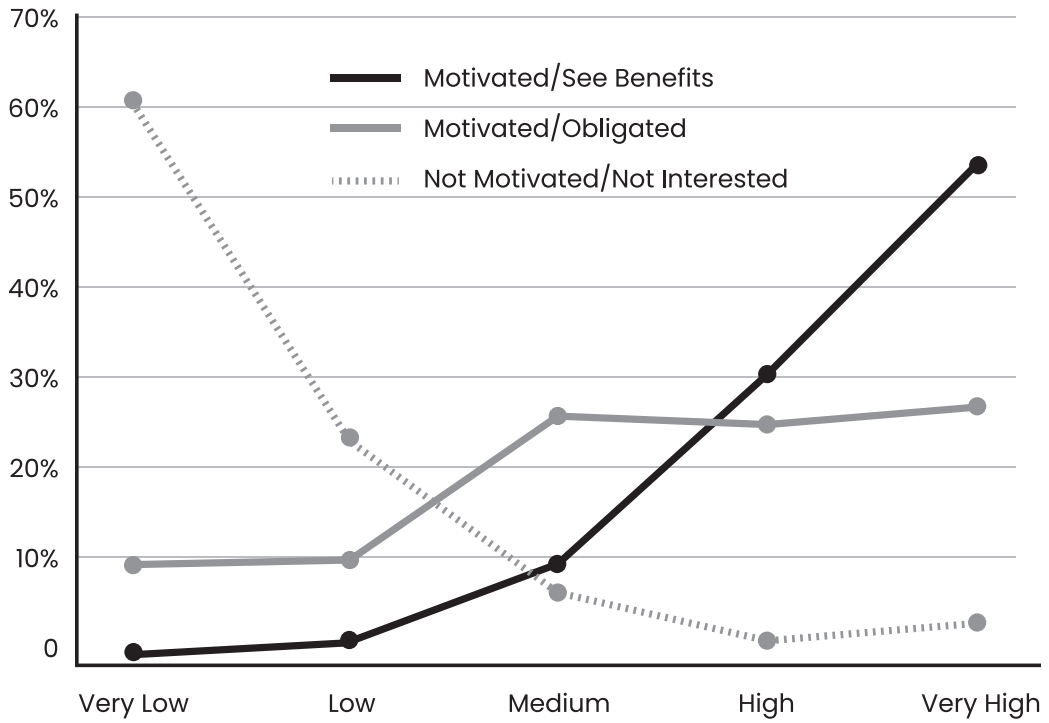
The scope of your security awareness program will depend on the percentage of intrinsic motivation versus extrinsic motivation versus reason among your target audiences.

The higher the percentage of amotivation, the more effort and creativity you will need to entice them to participate.

Considerations Based on the Results of Your Motivation Survey

- Participants with high scores on the *intrinsic motivation* scale are willing to learn new skills and behaviors. They believe the training will be helpful and are the first to complete the program. Select these users as your security awareness champions or participants in the pilot test, which we will discuss in more detail later.

User Motivation



- Participants who are *extrinsically motivated* will comply if learning activities are mandatory or if there is a reward for compliance. Think of fun ways to reward them for participation (e.g., a coffee shop gift certificate, promo items). You might also try to get them more involved through gamification, by creating competitions between individuals or departments.

- Participants who score high on the *amotivation* scale do not understand the importance of implementing a security awareness program or following best practices. They

may not know how they are responsible for protecting information assets. These participants ask questions such as "What's in it for me?" Your challenge will be to show them what is in it for them.

8. Scope of Your Program (Topics)

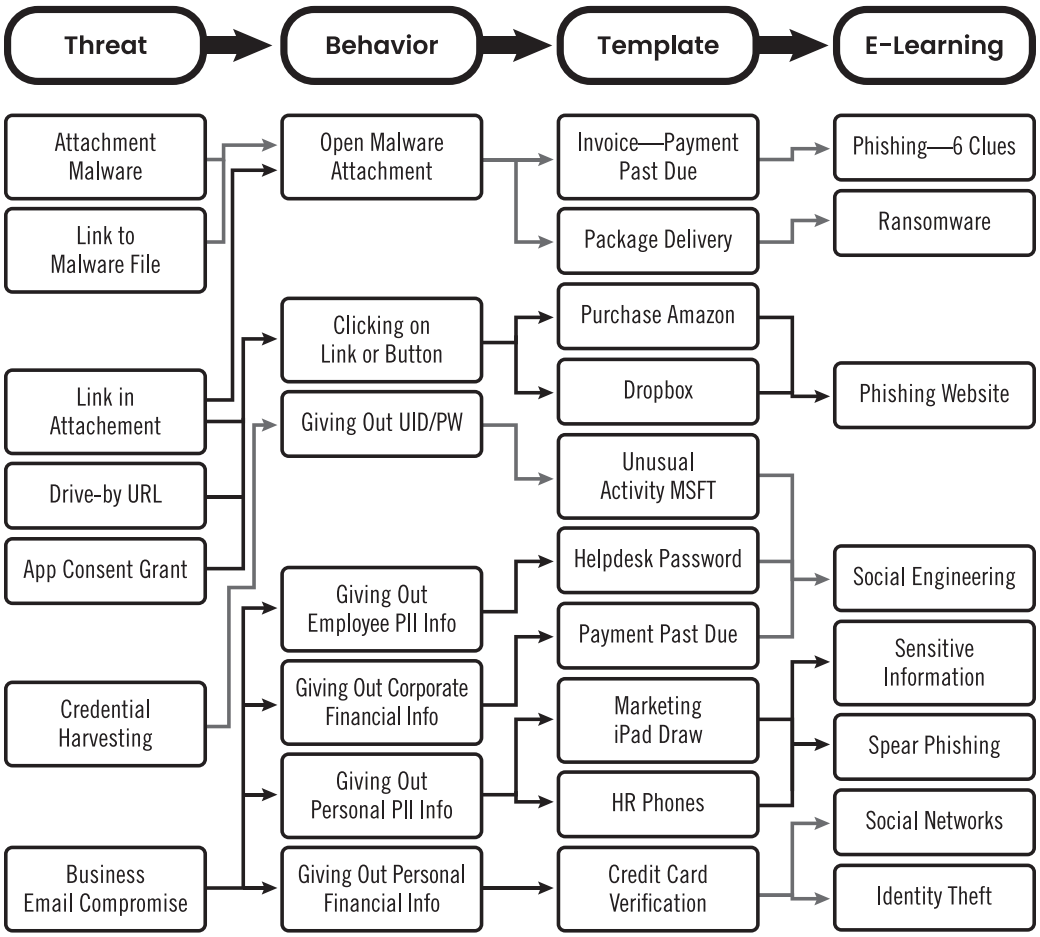
In this part of Step 1—Analyze, you will determine what topics you will cover in each campaign for the whole organization or each of your target audiences.

Essentials of Effective Awareness

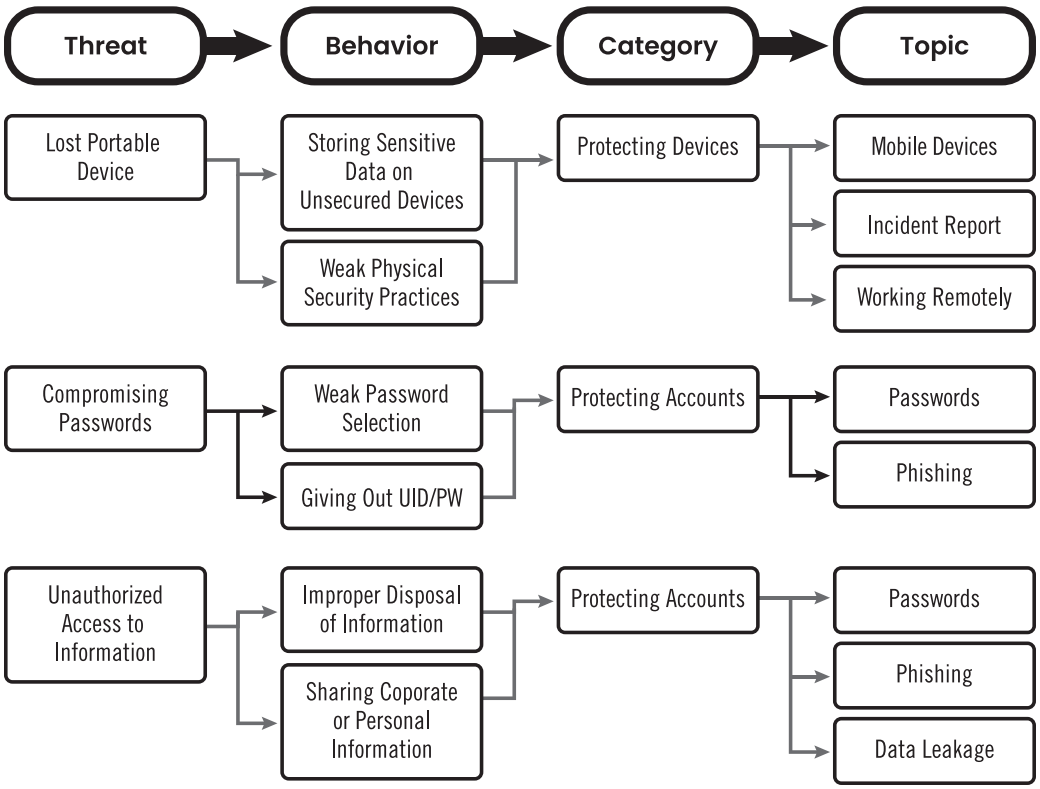
- The topics must be relevant to the individual.
- The topics should be relevant to their day-to-day activities.
- You need to use a level of language they can relate to and understand.
- The format you use to deliver your message has to be engaging and interesting.
- You must deliver the information in sections that are easy to learn and retain.
- For maximum retention, provide your awareness material in all official languages of your organization.
- Repeat, repeat, repeat.

Using all the results of your knowledge, behavior, culture questionnaires and phishing simulation results, you can identify the threats you want to address and behaviors you want to change. Here are some tables that can help you choose:

Risk-Based Phishing



Risk-Based Awareness Campaigns



Scoping Out Your Topics per Audience

Once you decide on the threats, behaviors, and topics you want to address, you can go a little further and scope them per audience.

Over the past two decades, the Terranova Security team and I have seen every imaginable scenario for security awareness. This experience has allowed us to zero in on the topics relevant to each target audience and identify where we need to correct risky behaviors and strengthen security alertness. I've listed the most important ones below.

Executives

Executives and upper management must be aware of your organization's risks to support and fund security awareness initiatives.

Topics to consider:

- Risks and threats facing your organization
- Secure use of mobile technology
- Safe handling of sensitive information
- Typical attacks and scams targeting executives
- Your organization's security and awareness compliance obligations

Managers

Raising managers' awareness about the risks facing your organization should mobilize them to act as security awareness ambassadors, champions, and role models.

Topics to consider:

- The previously mentioned topics for executives and upper management (or variations of them)
- An overview of information security and governance
- An overview of your organization's information security environment and your proposed security awareness program
- An overview of IT security controls
- Their responsibility in terms of implementing security policies and standards

End Users (General Staff)

Your program should increase overall understanding of security threats and communicate the best practices and behaviors you want your general staff to adopt.

Topics to consider:

- Information security and privacy
- Security essentials (password creation, email use, malware)
- Internet usage essentials (social media, safe browsing, cloud computing)
- Common phishing and social engineering techniques and cyber attacks
- Secure handling of sensitive information and mobile technology
- Physical security and the "clean desk" principle
- Information classification and management

IT and Developer Staff

How you raise awareness about IT security within the IT staff will depend on your organization's information security best practices and the network, systems, and application vulnerabilities in your environment.

Topics to consider:

- Network security overview
- Secure development
- Open Web Application Security Project (OWASP)
- Application security overview

- Shared network and application attacks
- System development life cycle (SDLC) and secure coding
- Security framework
- Cryptography and key management
- Privacy by design/default

Specialized Roles

How you raise awareness about IT security for those in specialized roles will depend on your organizational structure, the threats they may encounter, the type of data they access, and the regulations they must comply with.

The topics and target audiences to consider:

- Social engineering attacks for helpdesk personnel
- PCI DSS awareness for finance, retail, and client services
- Privacy (for human resources personnel and managers)
- Internal security policies (for third parties)
- Financial fraud for processors of financial transactions

EXERCISE

DEFINING YOUR TOPICS PER TARGET AUDIENCE

Identify your topics using the results of your quiz and simulations to fill in the knowledge and behavior gaps identified.

Target Audience Key Topics for Your Security Awareness Programs

- Executives
- Managers
- Specialized roles (both internal and third party)
- End users (general staff)
- IT staff

9. Additional Inputs

Deploying a security awareness program requires a deep understanding of every department within an organization, and you shouldn't expect to have all the required information without reaching out to stakeholders. The individual heads of teams or departments will be better than you at assessing the level of training required and other internal considerations for the program.

The best way to gather this information is through simple interviews with the various stakeholders. Depending on your level of access to these people, you can pose these questions in person or via video chat. If there are insurmountable time zone issues, you can correspond by email, but in-person interviews are recommended; they are the best way to stimulate a productive discussion.

Regardless of the form your interviews take, your primary goals are to get an idea of the respondent's objectives with the program, concerns they may have about it, past issues, and most importantly, their ability to participate or contribute. This step provides an excellent opportunity to identify internal champions you can rely on during deployment and build the training program.

Interview Questions

Security Awareness Program: Phishing Simulations

1. Has your team observed any behaviors that would not be considered secure (e.g., forwarding non-work-related email, visiting questionable websites, opening unexpected attachments in email messages, etc.)?
2. In your opinion, are employees security aware and how likely are they to spot suspicious email messages?

3. Does your team have any concerns with the decision to send phishing simulation messages to all employees of the organization?
4. Do you have any other recommendations on how to increase employee awareness on the phishing threat?
5. Put the following objectives in the order of importance for your team to maintain information security:

Objectives	**Ratings** Rate from Most Important (1) to Least Important (10)
Ensure passwords are not disclosed.	
Ensure the protection and proper handling of personal information.	
Reduce corporate exposure due to the misuse of business email accounts.	
Reduce the risk of system compromise by malware resulting in a degradation of business activities.	
Reduce the number of incidents/compromises that result from an email attack (phishing).	
Reduce the risk of information leakage/data breach.	
Ensure responsible use of the email service.	
Ensure responsible use of the internet service.	
Increase staff awareness on how to detect email phishing attacks.	
Increase staff awareness on how to detect phone or text phishing attacks.	

Security Awareness Program

1. How is your team involved in maintaining information security at our organization?
2. What type of security culture does your team expect at our organization, and have you observed the right security behaviors to support this culture?
3. What are the key information security messages from your team and how are they communicated?
4. How does your team encourage employees to think and act in a security-conscious manner?
5. What methods should we consider or do we already have for delivering security awareness messages?
6. How much time can/should your team dedicate annually to the security awareness program?
7. What would you consider a reasonable amount of training time for personnel, leaders, and security specialists, and how much of it should be mandatory?
8. Do you see a lack of awareness of information security policies among employees?
9. We are planning to roll out a new security awareness program to keep employees better protected against phishing scams, malware, and other cyber threats.

In your opinion, please tell us how employees in the organization feel about the following statements on a scale of 1 to 5.

1 = Strongly disagree
2 = Disagree
3 = Neither agree nor disagree
4 = Agree
5 = Strongly agree

	1	2	3	4	5
They would participate in this security awareness activity because it is interesting and will be beneficial.					
They would participate in this security awareness activity because they must.					
There may be good reasons to do this activity, but they don't see any.					

Assessing Previous Activities

The analysis of previous security awareness campaign efforts is a crucial step that is likely to give you surprisingly valuable insights. This process will once again rely on interviews, but this time you'll want to divide the respondents into two groups: the project team and the audience.

Project Team Audience

The questions to the project team will be more detailed and broken down into three distinct stages:

Process Evaluation. The purpose of these questions is to identify any underlying issues with how the program was initially designed. The answers will suggest the best channels to deliver the program, what kind of messaging to use, and which audiences you should focus on.

Outcome Evaluation. This is the step where you'll look at the data generated from previous security awareness campaigns within the organization. You should be able to quickly show whether the objectives were met or not, identify specific activities that changed user behavior, and assess any potential adverse effects of the campaign.

Resources Evaluation. The main purpose of these questions is to compare previously available resources to your current situation. You might be able to start filtering out previous issues that would be fixed by a better communication method or security awareness platform. It is also critical to look at the budget initially attributed to the program. Although not a resource per se, money spent is a crucial qualifying factor for all the available data.

Original Security Awareness Audience

The fourth set of questions will be directed at the original audience of the security awareness program. Once again, you'll want to break down the questions into sections.

Feedback from Audience.

Program Feedback. The focus of this section should be on the program's themes and content. You'll want to know if the users were aware of the issues discussed beforehand, if they felt a benefit from the program, and if it instilled behavior changes once completed.

Platform Feedback. The goal here is to see if the tools used to deliver the content were conducive to adequate learning. Issues with the platform may even need to be broken down further. Maybe the software itself was appropriate but users struggled with accessibility or proper content localization. Make sure your questions encompass a wide variety of potential platform issues.

Sample Questions

Project Team Questions—Process Evaluation.

- Did the program target the correct population with the appropriate topics?

- Do we need to consider another audience?
- Did the program take into consideration the needs of the target population?
- How satisfied were the target audiences?
- What delivery mechanisms worked the best?
- Were the mechanisms used to deliver the program effective? Did the message reach the target audience?
- Do we need to consider different methods for delivering our messages?

Project Team Questions—Outcome Evaluation.

- Did our program address the problems or end user behaviors we initially identified?
- Were any assumptions made at the start of the program correct?
- Were any actions taken to compensate for unforeseen events?
- Were the objectives met? If so, how? If not, why not?
- Did any of the program team members receive direct feedback on the program, and if so, what was it?
- Were the program activities beneficial to the target population?
- To what extent does the security awareness program change behavior?
- Which activities in the program made a positive difference in user behaviors?
- Were there any adverse effects?
- Is our program aligned with current policies?
- What can be done to improve the security awareness program?

Project Team Questions—Resources Evaluation.

- Does everyone on the program team understand their roles and responsibilities?
- Does the security awareness program team need any additional resources?
- Are the costs of the program's activities reasonable in relation to the benefits?
- Does the security awareness program have the required budget to continue its activities?

End User Questions—Feedback from Audience.

- Were you satisfied with the convenience and ease of access of the training material?
- Were you satisfied with the quality of the material?
- Was the tool easy to navigate?
- Did you feel that the amount of information and resource materials provided met your needs?
- Were you satisfied with the program, and did you feel that it was a beneficial use of your time?
- Do you feel more confident in your ability to address the threats presented during the program?
- What changes did you make in your work activities because of training you received in the past year?
- How will you apply what you learned in the program to protect your personal information?
- Do you understand how your behavior can impact the security of the organization's information or your own?
- What specific support would be helpful to you to implement the new practices presented in this program?

- Will you act as an information security ambassador and share what you have learned with others?

EXERCISE

OBTAIN FEEDBACK FROM STAKEHOLDERS

Identify the activities you will use to obtain feedback from the various stakeholders:

- Interviews with program contributors
- Feedback from project team
- Feedback from users

10. Support Resources

It is impossible to deploy a security awareness program in a vacuum. There are always many factors at play and there will always be challenges to overcome.

For example, what if your current organizational culture is not conducive to raising awareness? Perhaps the people in your organization believe that security is the responsibility of the IT department, or your organization is undergoing significant structural or operational changes. To be successful in any of these environments, you are going to need support.

When choosing awareness-raising activities, you must consider your allocated budget, your support resources and their availabilities, and the equipment you need. You may have to rely on the assistance

of different departments within your organization or even call on the services of external resources. We have determined the top three support resources: upper management support, security awareness champions, and operational support.

Identifying Your Available Support Resources

Deploying a security awareness program does not happen in a vacuum. There are many factors at play.

Upper Management Support

Getting dedicated support from management will help you secure the budget you need for your security awareness program. Furthermore, it will legitimize and raise the visibility of your program. Motivation and participation rates will undoubtedly be higher if management is actively behind you.

Therefore, before planning and implementing your program, you should solicit support from upper management. You will need to find an executive to act as your program sponsor—someone engaging who would be an effective spokesperson for your security awareness program and someone your target audiences recognize.

The program sponsor would typically send or sign program announcement messages before the launch of activities.

Security Awareness Champions

To raise security awareness effectively, many organizations use security awareness champions to liaise with a significant site, a business function, or a business unit. Security awareness champions act as an interface between the users and the security awareness program manager. They remind users about ongoing activities and bring user questions back to the program manager.

These ambassadors are intrinsically motivated people. Ideally, they are businesspeople with an in-depth understanding of the inherent risks of technology. They should also be engaging speakers so they can enthusiastically explain why the security awareness program is so important to your target audiences.

Operational Support

Before and during your security awareness program deployment, you will undoubtedly need active support from your IT department (for user list file transmission, synchronization considerations for single sign-on, internet bandwidth sizing, helpdesk interventions, etc.).

Your Human Resources department should be included in your support resources as well, particularly if you want training to be mandatory for new hires.

Working with a behavioral change expert or the user change management team can also be extremely helpful, especially if you have never headed up a security awareness program before. This type of expert can guide you with development, rollout, and evaluation.

EXERCISE

IDENTIFYING YOUR AVAILABLE SUPPORT RESOURCES

Take a few moments to identify groups or individuals whom you may require to support your efforts.

- Obtain upper management support for your security awareness program.
  - Sponsor:
  - Executive Leadership:
- Identify potential information security awareness champions and ambassadors.
- Identify the operation support required to run your security awareness program.

11. Globalization

Globalization may have an impact on two key aspects of your security awareness program:

- Possible need for customization (e.g., language, cultural nuances, etc.)
- Deployment coordination (e.g., time zones, language barriers among teams, etc.)

Complexities like multiple locations or multilanguage environments can also make the deployment of your security awareness program a little bumpy, so identify and address them early on. Imagine putting so much effort and planning into deploying your security awareness program worldwide, only to realize that one of your teams speaks predominately Portuguese, but your program is not currently available in that language.

Identify the languages of your program.

EXERCISE

ANALYZING GLOBALIZATION

Do you have multiple offices or facilities?

- If yes, what are they?
- Are they local, national, or international?

Do you need to offer the program in more than one language?

- If yes, what languages are they?

Are there any cultural nuances you need to take into consideration?

- If yes, what are they?

Are there any local or industry-specific training requirements that must be considered?

- If yes, what are they?

Are there any local contact or support details that you need to include for each location?

- If yes, what are they?

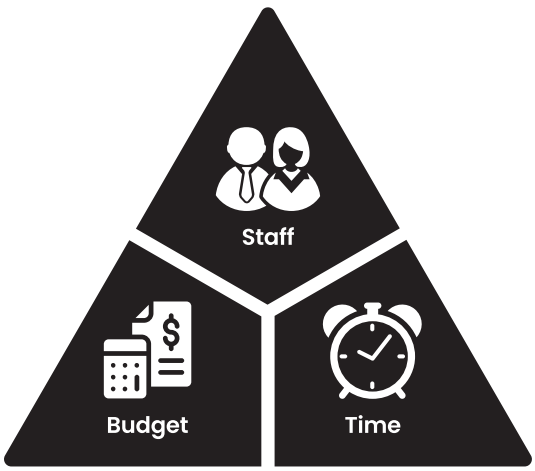
Are there any local support departments or are they centralized?

- If yes, what are they?

12. Costs

As with all project management, you must present a budget to decision makers and stakeholders. You must confirm the availability of any required support resources, determine the time allotted for the program, and work out the details of your budget.

Take a few moments to complete the following worksheet. It will give you some insights into the types of costs you can expect with the development and implementation of your program. It will help you decide if you have all the resources you need in-house or if you must keep external professional services.



The following is a list of cost considerations that will go into calculating your budget.

Direct Costs

- Number of users per audience (this will affect the cost of any licensed products)
- Security awareness platform to deliver your awareness training or phishing simulations
- Purchase or development of awareness content
- Purchase and/or production of awareness material (e.g., posters, mousepads, handouts)
- Costs associated with ongoing improvements and system maintenance fees

- Professional services or managed services to supplement your security awareness team
- Videos by the program sponsor to kick off your program
- Translation costs, if needed
- Live presentations and seminars

Indirect Costs

Always remember that "time is money." Although your organization already budgets these items, don't forget to attribute these indirect costs to your security awareness program:

- Number of staff assigned to designing and running the program and time spent
- Project manager(s), especially during Step 1—Analyze and Step 2—Plan
- Time hourly-wage workers will spend away from work while doing your awareness training (this can be a high operating cost for large organizations)
- Program sponsor's time
- Time spent reviewing the overall content by legal and HR departments and others
- Time spent confirming translations

Customization and Branding

A program that features an organization's branding, colors, and logo creates a sense of belonging among participants and is more likely to compel them to complete their training.

That is why we recommend choosing content that can be customized whenever possible—for example, branding emails and web

banners announcing the launch of a new module with the company colors, logo, and slogan.

Calculating the Costs of External Services and Products

You may decide to purchase products or retain external security awareness professional services for some or all of the development and implementation of your security awareness program. Below is a list of the costs to consider when deciding:

- Hours required to prepare your security awareness program
- Hours needed to prepare your security awareness campaigns
- Hours required to deliver your security awareness campaigns
- Hours needed to monitor your security awareness campaigns
- Cost of consulting services
- Cost of security awareness platform
- Cost of purchased content
- Hours needed to develop customized content
- Annual maintenance fees
- Other costs

EXERCISE

WORKING OUT YOUR COSTS

Presenting a comprehensive budget to decision makers is essential in order to secure the funding you need to run a successful security awareness program.

Take a few moments to complete the following worksheet. It will give you some insights into the types of costs typically associated with the development and implementation of your program, and it will help you determine if you have all the resources you need in-house or if you have to retain external professional services.

- Do you need any full-time employees to design your program? If yes, how many?
- Do you need any full-time employees to run your program? If yes, how many?
- Do you need a project manager to oversee the project? If yes, at what steps? (As you go through this book, you may want to come back to this question in order to decide if you need a project manager to oversee more steps in your security awareness program.)
    - Step 1—Analyze
    - Step 2—Plan
    - Step 3—Deploy
    - Step 4—Measure
    - Step 5—Optimize
- Do you need the services of an external security awareness professional to help you develop your training program?
    - If yes, at what steps? (As you go through this book, you may want to come back to this question in order to decide if you need a project manager to oversee more steps in your security awareness program.)
        - Step 1—Analyze
        - Step 2—Plan

continued...

EXERCISE

  - Step 3—Deploy
  - Step 4—Measure
  - Step 5—Optimize

- How many participants per target audience will take the training?
- How many product licenses will you therefore need?
- What security awareness platform will you be using to deliver your training and/or phishing simulations?
- Will you purchase or develop awareness content?
- Will you require awareness material (e.g., posters, mousepads, handouts)?
- What are your costs of ongoing improvements and system maintenance fees?
- Do you have to factor in the time participants will spend away from their function while doing the awareness training?

CONGRATULATIONS!

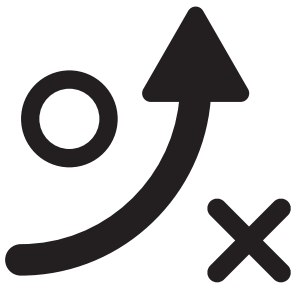
You have just completed Step 1—Analyze of the Terranova Security Awareness 5-Step Framework.

You have compiled some very important data, information, and insights that will guide your decisions in Step 2—Plan.

Summary of Analysis Data-Gathering Categories

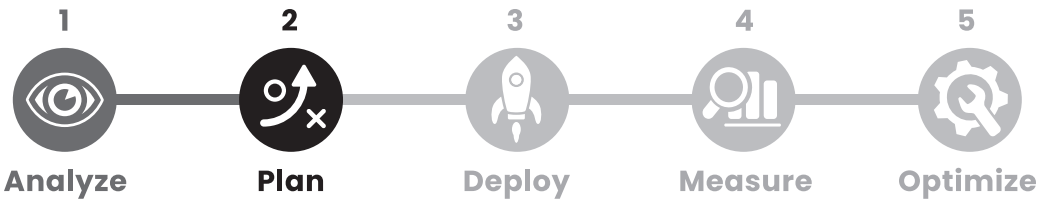
- Program Drivers
- Goals
- Compliance
- Target Audiences
- Level of Maturity
- Level of Knowledge and Behavior
- Motivation and Culture
- Scope of Your Program
- Additional Inputs
- Support Resources
- Globalization
- Costs

BY TAKING THE TIME TO **PLAN PROPERLY AND WORK OUT THE FINE DETAILS,** YOU ARE PUTTING SUCCESS ON YOUR SIDE.



TWO

STEP 2: PLAN



"Failing to plan is planning to fail."
—**BENJAMIN FRANKLIN**

Welcome to Step 2 of the Terranova Security Awareness 5-Step Framework—Plan.

In Step 1—Analyze, you defined the "why," and in the following pages, you will determine the "who, what, when, and how"—the

logistics of your security awareness program.

In the Analyze phase, you surveyed to measure employees' current level of security knowledge, behavior, and culture. Next, you studied the company's reports related to information security issues. You then asked all the essential questions: Were any security incidents resulting from employee behaviors such as virus infections or social engineering scams? Did any employees fall for these scams?

After reviewing the results, you prioritized topics based on internal weaknesses. Example: "Your employees are strong with passwords, so we can address that later in the program. However, they are more vulnerable to social engineering, so we will start with appropriate training to address that pain point."

This is where the planning begins.

Planning allows you to anticipate and address roadblocks, stay aligned with your objectives, stick to your timelines and budget, and ultimately, be more likely to succeed. If you simply dive into building a security awareness program hoping for the best, your outcomes will be hit or miss, and you will probably fall short of what you expected to accomplish.

Planning also allows you to:

- Meet compliance obligations
- Anticipate and address roadblocks
- Stay aligned with your goals and objectives
- Respect your timelines
- Coordinate with other organization-wide activities
- Identify blackout periods
- Stay within your budget
- Set up your program for success
- Identify program performance evaluation opportunities

I would never run a program without a plan. One of the key reasons I have been successful in business is that I set clear goals and carefully plan my steps to reach them. I incorporate all five steps of the Terranova Security Awareness 5-Step Framework (Analyze—Plan—Deploy—Measure—Optimize) into all my business strategies, recognizing that Step 2—Plan is essential.

Planning takes time, but when you are well prepared, your deployment runs smoothly. You deliver a more solid program—in scope, on time, and on budget—because you plotted out your steps. As a result, you are far more likely to meet your target objectives and run a successful program.

Tip: Assessing all the variables and laying out a plan from the outset will get you from point A to point B in the shortest amount of time.

You want your security awareness program to go off without a hitch and lead to real behavioral change in your organization. It is a big responsibility. By taking the time to plan appropriately and work out the fine details, you are putting success on your side.

Sometimes high-value tasks are the most daunting and complex, but they also yield the most significant rewards. In the Terranova Security Awareness 5-Step Framework, we have included everything you need to focus on crucial details. Efficiency and productivity are the very reasons why we developed the Framework and why I wrote this book.

So let's consider where you should focus your efforts. In this step, we will explore ways to:

- Build your team
- Define your roadmap

- Select content and platforms
- Customize content
- Select measurement tools
- Define KPIs
- Create a communication plan
- Select and customize communications materials
- Present your program
- Create and run an ambassador program

In the planning phase, you must also take into consideration some typical constraints you may face:

1. Users may not be interested in learning or may feel it is not their responsibility.
2. Users do not understand the need for security awareness or are unaware that everyone has a role to play.
3. Users are not motivated to participate because they don't see how it will benefit them.
4. Users do not have the time as they may already have a heavy workload.
5. Users in diverse roles and different knowledge levels require individualized campaigns.
6. Users need to be able to access learning content from anywhere, on any device, and in their native language.

EXERCISE

STARTING STEP 2—PLAN

Take some time now to review all the answers you provided in Step 1—Analyze

1. Program drivers
2. Goals
3. Compliance
4. Target audiences
5. Level of maturity
6. Level of knowledge and behavior
7. Motivation and culture
8. Scope of your program
9. Cyber security awareness
10. Support resources
11. Globalization
12. Costs

Building Your Team

Now it's time to build your team and get the right resources. I cannot stress enough the importance of surrounding yourself with a fantastic team. Everyone should bring something of value to the table so that together, they create a synergy that moves your security awareness

program forward. And I speak from firsthand experience; I truly believe Terranova's success is largely due to the team we have built together.

You will need the skillset of a multidisciplinary team to help you with a wide range of tasks, from the initial planning to the preparation, rollout, and monitoring of your campaigns. Consider colleagues with experience in focus groups, marketing, writing and editing, graphic design, production, and program analysis.

Departments with a stake in security awareness (training, communications, change management, HR, legal, compliance, privacy, risk management, and audit) should also be involved. These departments may provide additional resources, help secure funding, or ensure that participants understand why the security awareness campaigns are necessary.

Most importantly, choose enthusiastic team members. Seek out those you discovered as "intrinsically motivated" when you sent out motivation surveys.

A diverse, enthusiastic team will provide you with unique perspectives you would otherwise miss out on. It's like the old saying, "Two heads are better than one."

Your Dream Team

Reach out beyond security and IT to build your dream team. Here's who might be included on your team:

Program Sponsor

The program sponsor is the spokesperson for the security awareness program. They are most likely a senior executive (i.e., upper management) who may not be involved in operational activities. Still, this should be someone participants will recognize and support.

Responsibilities include:

- Liaising with upper management
- Keeping decision makers informed
- Securing funds and resources to operate the program
- Choosing the program manager/coordinator
- Approving the program

Program Manager/Coordinator

Although the program manager/coordinator may not be a full-time position, security awareness activities should be a significant part of

this person's day-to-day activities to ensure your program is successful.

Responsibilities include:

- Managing projects during the analysis and plan phases
- Building the security awareness team
- Defining, planning, and managing the program
- Overseeing the preparation of awareness content
- Coordinating campaign deployment
- Gathering and interpreting program/campaign metrics
- Reporting results to the program sponsor
- Conducting surveys and interviews to obtain feedback

Communications Advisor

The communications advisor will oversee the communication strategy and planning. Ideally, this person will have a change management background or be a member of your communications department.

Responsibilities include:

- Outlining change management strategies
- Defining the communication strategy
- Drafting memos and emails
- Establishing the communication calendar
- Sending messages leveraging organizational communications tools
- Sharing lessons learned from other organization-wide campaigns

Subject Matter Experts (SMEs)

SMEs may come from the security team or other departments depending on the campaign topics.

Responsibilities include:

- Reviewing awareness material for relevance
- Guiding topic selection and priorities
- Identifying risk profiles for the Security Culture Index
- Developing/customizing online courses and reinforcement tools
- Assisting with the collection of metrics related to behavioral KPIs

Security Awareness Platform Administrator(s)

The security awareness platform administrator(s) supports the implementation of the technical components of your security awareness program.

Responsibilities include:

- Configuring and administering the security awareness platform
- Configuring and deploying phishing simulations
- Maintaining up-to-date lists of participants
- Setting up the platform's Single-Sign-On (SSO) functionality
- Participating in functional testing
- Configuring permission lists and filters to allow phishing simulations
- Configuring parameters and assigning activity values for the Security Culture Index
- Supporting the security awareness team

Additional Contributors

I also recommend reaching out to additional contributors who may not be directly involved in the day-to-day activities of the security awareness team but who can provide support for the overall program.

Responsibilities include:

- Acting as awareness ambassadors
- Providing end user support
- Gathering feedback
- Reviewing content customization and translation as well as geographical nuances for campaigns in multiple countries and/or in various languages
- Identifying additional requirements for security awareness training (e.g., regulatory or contractual compliance, insurance, industry, etc.)

Defining Your Security Awareness Program Roadmap

Next, you need to define your security awareness program roadmap and set a timeline for the deployment of each campaign.

This task isn't complex, but it requires a strategy and planning since each unique campaign will include specific activities, respect various resource considerations, and strive to meet certain objectives and milestones.

Elements of a Security Awareness Campaign

A security awareness campaign consists mainly of online security awareness modules on the topics you identified in Step 1—Analyze.

EXERCISE

BUILDING YOUR TEAM

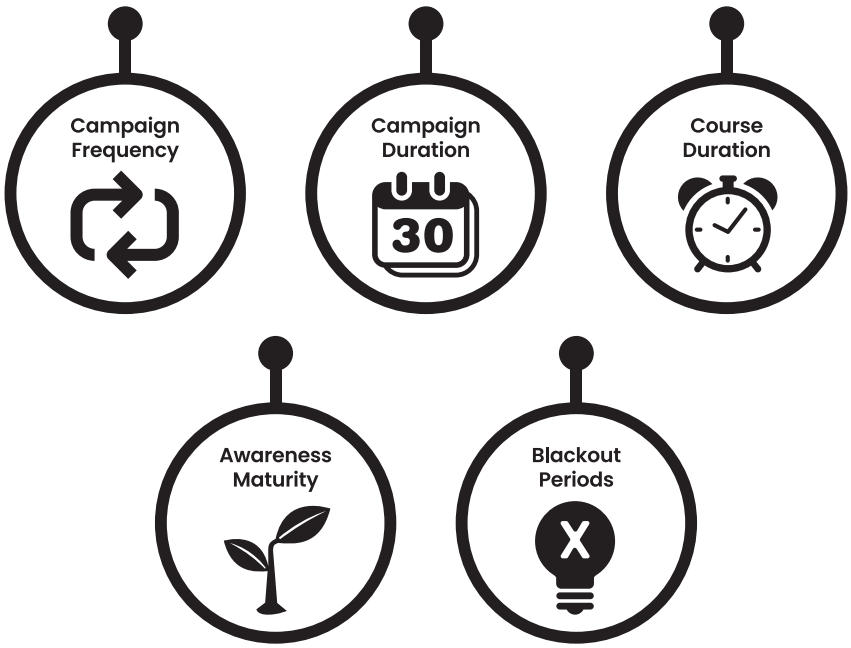
The time to put your team together is now, before you proceed with any more planning. Team building comes first because you will want input from all team members as you decide on critical factors such as timelines, program content, and communication strategies.

Possible Team Members

- Program sponsor(s)
- PM/coordinator(s)
- Security awareness program manager
- Communications advisor(s)
- Security experts
- Security awareness platform administrator(s)
- Local site coordinator
- Pilot team
- Simulation manager
- IT administrator(s)
- HR/Training
- Legal/Compliance
- Pilot team
- Physical security
- Additional contributor(s)

Surround yourself with a multidisciplinary team of experts who can draw on their experience and know-how to make your security awareness program a success.

If you don't have the resources you need, you can work in close collaboration with your security awareness provider. They can supplement your internal security awareness team and help ensure the success of your security awareness program.



Your campaigns will include:

- A learning module, distributed to one or all of your target audiences, depending on its relevance
- Security awareness modules, released on an established schedule
- A communication plan to announce the upcoming activities, invite users to participate, and remind them of the ongoing security awareness campaign activities
- Various reinforcement tools (e.g., newsletters, posters, videos, games) issued between campaigns to reiterate critical messages and keep information security top of mind, released on an established schedule

You will also use several defined performance metrics to evaluate the success of a given security awareness campaign. These metrics will allow you to evaluate the campaign's performance against the objectives you defined and adjust for future campaigns if needed.

Remember, your security awareness program is your overall plan defined by the strategic goals you set out in Step 1—Analyze. Your security awareness program consists of a number of smaller campaigns, each designed to meet its own set of objectives.

Roadmap Considerations

When defining your roadmap, you must be mindful of your program's overall impact and time demands on the security awareness team and the participants. Likewise, when you draw up your timelines, you must ensure that they reflect your campaign objectives and are realistic based on your resources.

> *Tip:* Avoid launching your campaign during the same time frame as an organization-wide event or any other activity that could affect participation rates.

Once you have finalized your roadmap, present it to your program sponsor and any decision makers whose approval and support you need for your security awareness program.

As you set your timelines, keep in mind the following:

- Program announcement
- Program duration
- Campaign frequency
- Campaign duration

- User awareness maturity level
- Quiz duration
- Course duration
- Phishing campaign duration
- Blackout periods
- Prelaunch testing

Program Announcement

Allocate time before you launch your first activity to properly introduce your program to your audience:

- Describe program and upcoming activities.
- Explain employee participation expectations.
- Demonstrate management and executive support of the program.

You should send an announcement three to five days before the first activity.

In addition, don't forget your new hires. You must coordinate with your Human Resources department to include specific communications and steps in the new employee onboarding process to include information on security awareness campaigns.

Program Duration

When deciding on the overall duration of your security awareness program, you must consider several variables including:

- Is training mandatory or optional? If compulsory, you can impose deadlines. If optional, you may provide a more extended time frame to increase participation.

- How many participants must complete the same program? If the number is high, you may want to release the training in stages over an extended period so you do not overwhelm your email system or internal IT network.

- Do you have to track and report on participation? We recommend launching bite-size content so that users can more easily retain the information. If releasing one module per month is too much for your resources, consider delivering modules less frequently to a larger group of people.

- Does your program contain all the activities, themes, and topics for a certain period (typically twelve months)?
  - Online training
  - Quizzes and surveys
  - Phishing simulations
  - Reinforcement activities
  - Communication plan
  - Other reach-out activities (e.g., bulletins, Lunch and Learns, kiosks, etc.)

Ultimately, your program duration is determined by logistics—by your needs, goals, the reach of your program, and the resources available to help you deploy it successfully.

Campaign Frequency

- How often will you carry out online awareness training?
- How often will you launch phishing simulations?

- How often will you launch knowledge, behavior, and culture quizzes or surveys?
  - Yearly?
  - Biannually?
  - Quarterly?
  - Monthly?

When deciding, consider that increasing campaign frequency has many benefits as it:

- Keeps security top of mind
- Relieves the pressure of trying to cover everything at once
- Keeps the attention on the importance of information security in your organization (through repetition, you are letting your audiences know that information security is vital for your organization and that they have a role to play)

However, you should also know that increasing campaign frequency has some drawbacks and may:

- Place a strain on your security awareness team and resources
- Risk oversoliciting participants, which will cause them to lose interest
- Require more time between campaigns for making adjustments following pilot testing
- Be too rigid; you may not be able to adapt your strategy between campaigns

Campaign Duration

Depending on the campaign frequency, you will decide how long each campaign should last. For example, let's say you have chosen a frequency of one campaign per month or every two months.

In this scenario, your campaign should last between four to eight weeks:

- One to two weeks to complete knowledge quiz, behavior quiz, and culture quiz
- Two to four weeks for participants to complete the online training
- Two to four weeks for communications, before and after the training period
- Phishing campaign: one week (simulation, just-in-time training, results)
- Awareness week: one week (security booth, daily Lunch and Learns, games, etc.)
- Awareness month: one month (posters, videos, games, newsletters, microlearning)

User Awareness Maturity Level

Earlier in the book, I introduced security awareness program maturity, which referred to the thoroughness of developing your security awareness program. You must also consider user awareness maturity, meaning the level of knowledge, experience, and motivation of the people in your organization and on your security awareness team.

Questions to ask:

- Have participants completed information security awareness training in the past?

- Has the current security awareness team ever planned, prepared, and developed a security awareness campaign?
- How much time do you need to prepare and make adjustments between campaigns?
- To determine the maturity level, you may consult the results of:
  - User knowledge quiz
  - User behavior quiz
  - Culture or motivation survey

Depending on your team's awareness maturity and the security culture within your organization, we usually recommend starting with smaller campaigns and adjusting the duration and frequency of future campaigns based on campaign results and participant motivation and feedback.

Quiz Duration

Quizzes should be short and be composed of 10 to 15 questions. Users should be able to complete the questionnaires in about ten minutes.

Course Duration

Consider four factors when determining your roadmap:

1. How many hours do you want each user to allocate for training per year?
2. Is there a limit to the maximum duration of each course?
3. Is there a maximum number of awareness courses you can roll out each year? (Do not include reinforcement activities such as newsletter, micro- and nano-learning, etc.)
4. How many of the available topics do you want to deploy each year?

You must determine at least three out of the four above parameters to determine how you will plan your deployment.

Also consider how many modules you will include in your course. Depending on the frequency of the campaign, the number of topics, and your participants, you may decide to launch:

- One or two critical topics per month totaling three to five minutes
- Three to six critical topics per quarter totaling fifteen to thirty minutes
- Microlearning modules that last two to three minutes (we often recommend these for millennials and people on the move)

Phishing Campaign Duration

Phishing campaigns should remain active for at least seven days and span two weeks to allow for maximum exposure.

Blackout Periods

Are there times when you should not plan awareness activities? Yes. There are times when it may be challenging to reach your target audience.

Standard blackout periods include:

- Annual winter and summer vacation periods
- Time blocked out for other organization-wide campaigns
- Statutory holidays
- Year-end cycles

On the other hand, it would be clever to plan extra campaigns to coincide with Cyber Security Awareness Month, Safer Internet Day, or Data Privacy Day.

Prelaunch Testing

Before you launch your program and individual campaigns, you must conduct pretesting to ensure everything will run smoothly on launch day.

Factor in time for content review, compatibility, accessibility, and performance testing of your IT systems and a general pilot test of your actual campaign. (We will look at these in more detail in Step 3—Deploy.)

You must also give yourself enough time to measure campaign success and implement an action plan to meet objectives and goals. (There is much more to come on these aspects in Step 4—Measure and Step 5—Optimize later in this book.)

Finally, leave enough time in your project plan to conduct your testing and make necessary adjustments.

EXERCISE

DEFINING YOUR ROADMAP: CONSIDERATIONS

Planning a security awareness program can be complex and may take a long time. Doing the proper groundwork and asking all the right questions will allow you to plan your roadmap and timelines.

Referring to the previous pages for guidance, make as many notes as possible to keep track of any variables that could affect scheduling. Your notes will give you a good overview of the time you will need to allocate.

Then consider these questions:

Program Announcement

Consider who will draft, who will send, and who will sign the announcement message. When will the message be sent and what medium will be used to have maximum visibility?

continued...

EXERCISE

Program Duration
How long should your program last before you need to review your strategy and priorities?

Campaign Frequency
How often will you carry out online training? For instance, you might choose biannually, quarterly, or monthly.

Campaign Duration
How long should each program campaign last (period to cover a specific theme)?

How much time will be allotted for participants to complete the training? (This question is especially relevant for compliance training.)

Course Duration
How many topics will you include in your course?

Quiz Duration
How long will you allocate for the quiz and at what point will you issue a reminder?

Phishing Duration
For how long you will collect data related to the phishing exercise?

Awareness Maturity
Have participants ever completed security awareness training in the past?

- If yes, will you repeat any previous activities or leverage only new topics?

Has the current security awareness team ever planned, prepared, and developed a security awareness campaign?

- Either way, consider giving them a copy of this book.

How much time do you need to prepare and make adjustments between campaigns?

continued...

EXERCISE

Blackout Periods

Are there times when you should not plan awareness activities?

- If yes, what are they?

Prelaunch Testing

How much time will you allocate for:

- Content review
- Testing
- Compatibility and performance testing of your platforms
- Pilot testing
- Adjustments before launch

Tip: When defining your roadmap, you need to be mindful of the overall impact and time demands your prelaunch testing will have on your security awareness team.

Selecting Your Content and Platforms

So now the questions are, What content will you include in your program in general and in each of your campaigns? Will you purchase products already on the market or develop your own?

In the next section, I will walk you through all the considerations you need to keep in mind when selecting content and measurement tools for your campaigns, and I will showcase some of the ways you can customize them.

Selecting and Customizing Your Content

- Online training courses
- Live presentations
- Reinforcement tools

Selecting and Customizing Your Measurement Tools

- LMS (learning management system) training reports and dashboards
- Phishing simulation reports and dashboards
- Vulnerability assessments
- Survey and quiz reports and dashboards
- Security Awareness Index
- Culture Index

The Importance of Diverse, High-Quality Content

A security awareness program is only as good as its content. To ensure that end users retain core concepts and knowledge, it's important to contextualize topics and keep users engaged during the entire training process. To change behaviors, the content must be fun and fit into users' schedules. This result is achieved in a few different ways.

Engaging Content

Content must be designed by education professionals who understand adult learning. Break up lessons into bite-size morsels and carefully divide them by topics. Keep the interface simple and include an interactive component in each lesson, such as a short quiz that can gauge user understanding and also create a fun learning atmosphere.

Finally, tailor content to the user's specific role within the organization. You might show someone in a manager role, for example, content that helps them coach their team members and supervise any

existing cyber security awareness processes. Similarly, cyber security awareness is a vastly different subject for different departments or disciplines, like marketing versus software development, so you will want to take a custom approach to each.

Varied Formats

Additionally, vary the media you use to deliver your content and personalize it to your organization's needs, or your users will never relate to it and take it seriously.

For example, you can use newsletters and desktop images as reference material and reminders of best practices. Deploy them after the learning activities or use them to promote key topics that you did not have the opportunity to cover during your program.

You can also promote your message with short, engaging online learning activities throughout the year, such as microlearning, nanolearning, videos, and gamified Cyber Challenge modules.

Accessibility

To ensure that your training is digested and internalized by all team members, make it practical for the user to complete it. In other words, successful security awareness training must be available to *all* users and must meet minimum accessibility standards, if not exceed them.

Responsive Design

With users increasingly working outside the office, for instance, it has become crucial to have mobile-ready content that can be viewed on any device. Similarly, it's essential to ensure the content is available in various formats compatible with all the different computer systems your organization offers to the workers.

Gamification

Gamification is an excellent complement to cyber security awareness training. Training delivered in game form, with point accumulation and completion badges, motivates users to acquire new cyber security knowledge. If rolled out correctly, these measures can even turn your users into ambassadors within the organization.

Quality Content

Finally, content quality is also integral to your organization's cyber security because it's directly tied to the completion levels of your training. When you provide quality content, your employees understand that this is a subject you're serious about, and they are more likely to stick with their cyber security habits; by doing so, you strengthen your data security.

Your next round of planning decisions must be about the content you want to include in each program campaign. To make your selection, you must consider many variables, including the risks, the behavior you want to change, your participants' motivation, your organization's culture, your training budget, and your capacity to implement and distribute the content in various forms.

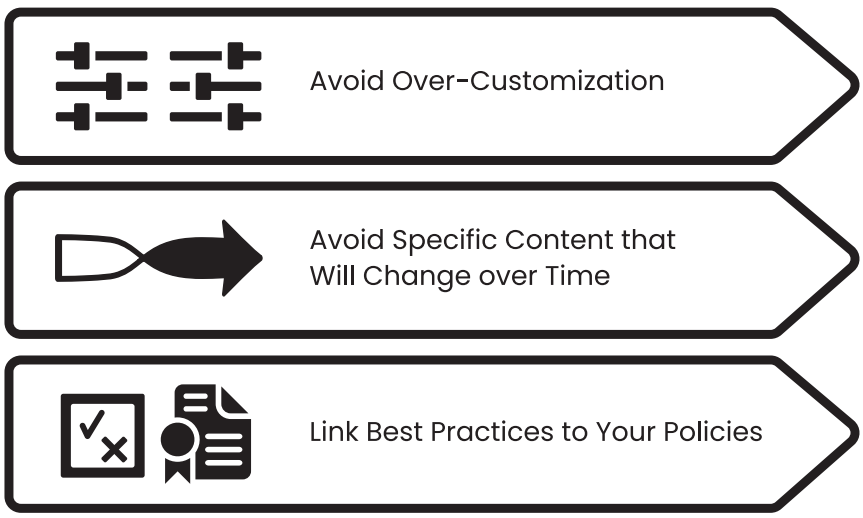
EXERCISE

IDENTIFY FORMAT REQUIREMENTS FOR ACTIVITIES

What are the minimum requirements for your awareness program format?

- Must meet accessibility standards
- Must include responsive design for mobile users
- Must include gamification for user engagement
- Leverage existing or acquire a learning management system

Customizing Your Content



Customizing your communications compels people to be more motivated to participate. You can tailor your content by working with a template and adding elements that make your content more engaging and relatable.

Course customizations can include:

- Your logo, brand colors, etc.
- Links to your organization's policies
- Real-life examples and stories
- Photos, videos, graphs, and other visuals relevant to your organization

Course Customization Considerations

When customizing your program content, keep the following in mind:

1. Avoid Overcustomization

When you build a program for the first time, ensure that your SMEs do not cover too much information in a single course.

Your goal is to turn participants into security advocates, not experts, so provide them with the exact knowledge they need to adopt security best practices and behaviors.

2. Customize with "Evergreen" Information

Evergreen information is information that is not likely to change over time. For example, rather than providing the email address and extension number of a particular contact person at your organization—information that almost certainly *will* change over time—provide a general point of contact that remains stable, such as your helpdesk. You can also create a generic INFOSEC inbox to collect and consolidate all participant feedback, questions, and concerns.

3. Link Best Practices Training to Your Policies

Reinforce acceptable uses of technology by including your organization's policy statements in the best practices section of your course. You might also add links to the location of your internal policies to highlight their importance.

Note: A link should only be provided once—at the end of the activity or a module—to reduce distraction and the risk of participants leaving the course before reaching the end.

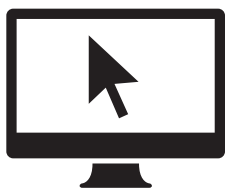
Content Comes in All Shapes and Sizes

Everyone responds to messaging differently. Fortunately, you have an assortment of awareness tools available to use depending on the context and the target audience.

Ways to communicate your security awareness message and content:

- Online training courses
- Live presentations
- Reinforcement tools

Online Training Courses



Laird's sensory theory (1985) states that learning occurs when the five senses of sight, hearing, touch, smell, and taste are stimulated. Laird's theory suggests that if multisenses are stimulated, greater learning takes place. That's one reason interactive online training courses and games succeed—they provide visual, auditory, and tactile feedback.[2]

These types of tools can help you communicate knowledge and best practices and change human behavior. There are plenty of options to choose from as well. Courses are available in various forms and lengths, ranging from three-minute microlearning to twenty-minute courses. Explore all the ways you can enhance the learning experience, from interactive instructional exercises to games, quizzes, and evaluations.

Advantages.

- Reach a broad audience quickly
- Address specific learning objectives
- Higher retention due to interactivity of online training

2 Dugan Laird, *Approaches to Training and Development*: *New Perspectives in Organizational Learning, Performance, and Change, 3rd ed.*, ed. Sharon S. Naquin and Elwood F. Holton III (New York: Basic Books, 2003).

Target Audiences for Online Content. When selecting online modules or courses for your security awareness program, you need to keep in mind the target audiences you identified in Step 1—Analyze so that the level of training content is appropriate for each member's role and responsibilities. When you put the topics into context by providing specific examples, risks, and potential impacts in the role, the learner can better relate to the training activity and understand the importance of security best practices.

In-House Target Audiences.

- Executives[3]
- Managers[3]
- End users (general staff)
- IT staff
- Specialized roles (internal)

3 Depending on your corporate culture, executives and senior managers might opt for a live awareness presentation rather than doing an online course.

Third Parties (Additional Specialized Roles).

- Contractors
- Business partners
- Clients
- Suppliers

Online Training Considerations

As you plan and prepare to roll out your online training, you will have to make decisions about certain functional aspects of the training:

- Mandatory versus voluntary participation
- Evaluation and grading
- Course duration and frequency

Mandatory versus Voluntary Participation. Should you opt for mandatory or voluntary participation? Although both options have merit, mandatory participation will:

- Reinforce the importance of training
- Ensure a higher participation rate
- Vary based on the applied consequences for nonparticipation as defined by each organization
- Begin with new hires
- Include mandatory training follow-ups and escalations performed by Human Resources and employee supervisors
- Set limits to certain resources or the internet until courses have been completed
- Increase the likelihood of meeting compliance obligations

If there are challenges with achieving desired participation rates, consider taking the following actions:

- Create shorter modules and use varied formats.
- Send continuous notifications and reminders.
- Associate completion with yearly performance evaluation.
- Include messages and best practices that help in the personal life.
- Send reminders from supervisors and managers.
- Implement competition and rewards.
- Recognize top departments.
- Present department performance to executive leadership team.
- Organize Lunch and Learn sessions to increase interest.
- Assign local or department ambassadors to promote awareness activities.

In general, set participation objectives and monitor them over time. If participation falls short, you may need to adjust your campaign midstream or alter your next program activities.

Finally, ensure no union or labor contracts would prevent your training from being mandatory. Depending on the situation, you may consider having a mix of compulsory and voluntary topics.

Evaluation and Passing Grade. You decide whether to add an evaluation at the end of your online training. If you do, you must also set a passing grade. Such decisions must be in keeping with the culture of your organization. Also, ensure there are no union or labor contracts preventing individual scores from being compiled.

Once you have decided on the passing grade, you must determine what happens when someone fails. Will they have to redo the whole

course or retake the test? Will a customized learning path be set up for each user who failed the training and the phishing simulations or according to their Security Culture Index?

You can show users their progress in terms of percentage of program completed, results of activities, and their own Security Awareness Index. Doing so can help to develop the culture of security in the organization and encourage users to self-identify if they need to do more. Organizations are also encouraged to set up individual learning paths per end user based on their Index-related data.

Track and provide scoring and progress reports on all your activities such as quizzes, courses, games, simulations, phish reporting, and so forth. In addition to informing your training efforts, this record of improvements over time will help demonstrate the value of your program.

Course Duration and Frequency. When rolling out an online course, it is important not to include too much content simultaneously. You might end up overwhelming the participants, and they may be unable to absorb the critical knowledge, acquire new skills, and adopt desired behaviors.

The duration of the modules within a campaign must align with your organization's culture and operations. For example, let's say you are a retail company and need to train your sales associates. These employees typically work on the sales floor, interacting directly with customers, not on a dedicated computer. Therefore, you may have to approach their training differently than you would office workers.

You could ask them to leave the sales floor for a brief period to do the training in the back office. In this case, short quick modules offered once a month might be the right solution. On the other hand,

if you already train your remote salesforce and have a semiannual sales meeting scheduled, that might be the right time for them to do a more extended training session as part of their sales meeting agenda.

Ideally, a campaign should not cover more than three to four key topics in fifteen to thirty minutes, with each topic lasting approximately six to eight minutes.

You could also launch:

- One topic per month
- Three topics per quarter
- One course per year

Course Completion Criteria. What must the participant accomplish to obtain a course completed status? Is it sufficient to simply complete the course and evaluation, or do participants need to obtain a certain score in the evaluation to receive a completed status? View certain videos? Play certain games? Complete a challenge?

It's up to you, but we do suggest you allow users to redo the evaluation step for a course if needed. This approach ensures users have adequate time to follow the course, do the reading, and adequately respond to the evaluation questions, which is also part of the learning process.

> *Tip:* As you plan and prepare to roll out your online awareness training, you will have to make decisions about certain functional aspects of the training.

Organization Structure. Organizations operating in a decentralized model, where cyber security is managed independently at each local entity, must decide how they will plan and deploy awareness programs.

Although each entity likely has some discretion over the topics, format, and schedule they use, parent organizations may provide some criteria for the design of the program and expectations such as:

- The need for an awareness program
- Participation expectations
- The need for a phishing simulation program
- Performance expectations
- A common framework (this book)

Employee Workload and Sentiment. Other essential elements to consider when planning your program are employee workload and sentiment toward the organization regarding security awareness training. When we ask employees to complete security awareness training, we ask them to complete activities beyond their core responsibilities. They may be reluctant to dedicate the required time away from their day-to-day tasks. Based on your organization and target audience, consider the following examples:

- An educational facility asking faculty to complete the training during pedagogical days
- A manufacturing company asking shift workers to complete the training at the start or end of their shift
- An organization with a fully remote workforce allowing employees to complete the training from anywhere, on any device at any time
- A firm granting their employees one or two free hours per quarter provided they complete the quarterly training (which is typically thirty minutes)

EXERCISE

ONLINE TRAINING CONSIDERATIONS

Complete this worksheet to ensure you do not overlook any critical factors that may affect the logistics of your program, campaign, or courses.

Is participation in the training mandatory?

- Note any special considerations such as company policies and union stipulations that will affect whether participation is mandatory.

Will you impose a passing grade?

- If yes, please specify and note any special considerations.

Do all your different target audiences have a dedicated computer?

- If no, which ones do not? Note any special measures you may take in light of this situation.

How long should your courses be, and how often will you distribute them?

- One campaign per quarter: training from twenty to thirty minutes each
- One campaign per month: training from three to ten minutes each
- Note any special considerations.

What about training for new employees? Will they:

- Start with a course or campaign that is currently underway?
- Start your program from the beginning?
- Receive a custom program for new hires that includes all the security essentials?
- Note any role-based training.

- A financial institution associating program completion with yearly bonuses

Whatever your situation, you must consider your target audience's workload, availability, perception, and overall satisfaction with their work environment before you ask them to invest time in security awareness training.

TIPS FOR EFFECTIVE SECURITY AWARENESS CONTENT

- The topics must be relevant to the individual.
- The topics should be relevant to their day-to-day activities.
- You need to use language they can relate to and understand.
- The format you use to deliver your message should be friendly, engaging, and interesting.
- You should deliver the information in segments that are easy to absorb and retain.
- Communications should be short, concise, and consistent.
- Remember to provide compelling reasons to participate ("What's in it for them?").

Live Presentations

As useful as online courses are, this should not be your only approach. Live presentations are a better option in some cases, especially if you need to get buy-in on the importance of your security awareness initiatives. Live presentations are the ideal format to share valuable security-related information with executives.

Live presentations should be used to:

- Present a high-level overview of your organization's information security strategy
- Introduce your organization's information security team
- Demonstrate that information security risks are business risks
- Inform them of common threats and best practices (both organizational and individual)
- Provide them with the essentials for future discussions and commitments

Advantages.

- They are short (15–20 minutes) but long enough to cover the specific awareness concerns of this audience (e.g., threats and relevant news stories).
- Executives, who tend to be very busy, are likelier to make a short presentation than complete online awareness training.
- You can add your presentation to the agenda of a meeting.

Target Audiences.

- Executives
- Senior managers

Live presentations can also be used for the general audience and allow them to ask questions and hear from their peers.

Reinforcement Tools

After launching a campaign, use reinforcement tools to repeat the key messages covered in the awareness training so participants don't

forget best practices. Videos, newsletters, desktop images, web banners, games, and posters are just a few ways to increase retention, keep security top of mind, and ultimately achieve your campaign objectives.

Target Audiences.

- Executives
- Managers
- End users (general staff)
- IT staff
- Specialized roles

Advantages.

- Reinforcement tools send the message home and keep security awareness top of mind so that the people at your organization change their behaviors and prioritize information security.

- With so many media channels at your disposal, you can reach your target audiences in a variety of ways over many channels.

- You can be creative and impactful when conveying your message. For example, use reinforcement tools to showcase desired behaviors in videos or share "breach-averted" stories in your newsletter.

- Tools such as micromodules are effective for highlighting and reinforcing best practices related to a specific risk or threat.

Selecting and Customizing Your Measurement Tools

What are measurement tools, exactly? They are any of a variety of mechanisms that provide you with information to assess the effectiveness of your campaigns. It is essential to have these tools in place because they can give you insights and precise data on a vast array of performance indicators—from participation rates to knowledge retention to participant satisfaction—which you can then use to tweak subsequent campaigns to achieve even better results.

Powerful measurement tools we recommend for every security awareness campaign:

- LMS training reports and dashboards
- Phishing simulation reports and dashboards
- Vulnerability assessments
- Survey and quiz reports and dashboards

Learning Management System

The security awareness platform or learning management system (LMS) you use in your campaigns will allow you to measure online training

participation rates and determine the percentage of successful users who have completed the courses.

As I have discussed throughout this book, you have to define objectives and metrics and produce reports on your program's performance to ensure you are reaching your campaign objectives and strategic program goals. You can create actual reports using the security awareness platform or LMS by configuring it to collect data related to user participation.

You then have tangible data that you can compare against other security awareness initiatives and present to decision makers as needed.

Phishing Simulations

Phishing simulations are a great tool to measure your organization's ability to recognize and deal with cyber security threats. *Note: Phishing simulations should not include third-party target audiences without their approval.*

Target Audiences

- Executives
- Managers
- End users (general staff)
- IT staff
- Specialized roles (internal)

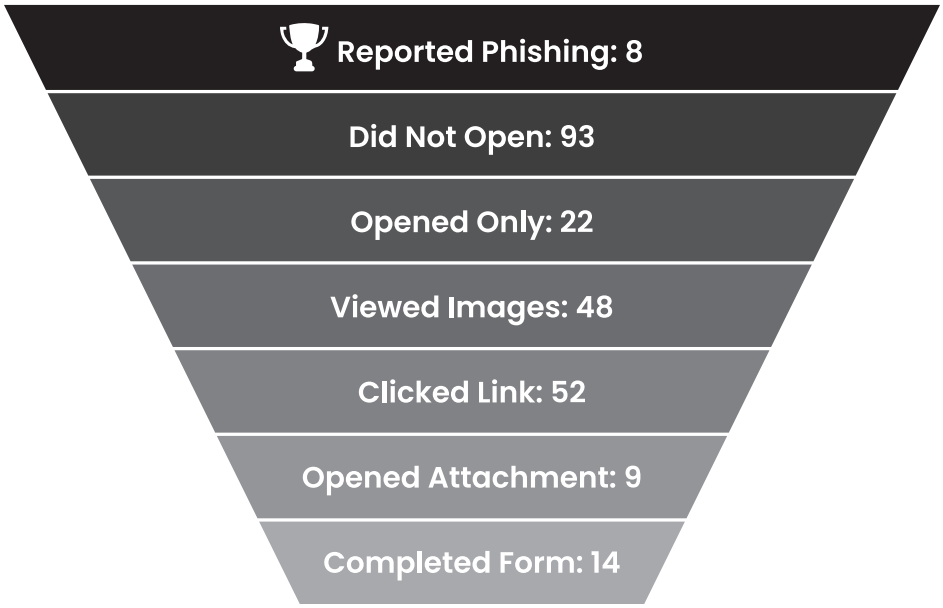
Advantages

- They provide quantitative insight into your organization's vulnerability to phishing and other email-based attacks.
- You can use them before and after awareness training to determine training effectiveness.

- They can be enhanced with just-in-time training to build a comprehensive phishing awareness program.
- You can use them with real-time reporting and dashboards (when used with a phishing platform).

Phishing Simulation Considerations

Total Actions Performed



When preparing a phishing simulation, it is vital to do the following:

- Clearly define the strategy as well as the lines of communication before launching.
- Inform all stakeholders concerned that they will know when you conduct a phishing test.

- Avoid sending messages alphabetically if you opt for a gradual deployment. Participants may realize it is a test if they seem to be in some sort of order.
- Perform validation and cleanup of email addresses before the simulation.
- Establish a response mechanism for the security team because participants who detect phishing may report it as real.
- Report the results to management and participants.
- Take the time to teach participants who fail to recognize phishing what they should do. We do not recommend reprimands.
- Deliver just-in-time training for users who fail to detect the threat.
- Consider local laws and regulations related to phishing users.

Vulnerability Assessments

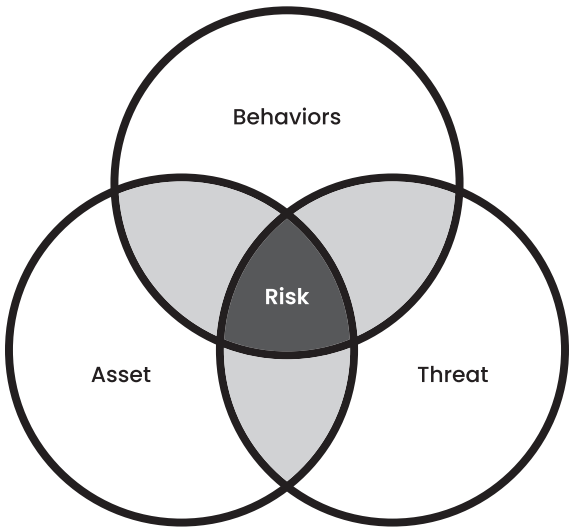
Assess your organization's level of information security knowledge using social engineering techniques such as:

- USB key drop
- Vishing simulations
- Smishing simulations
- Tailgating exercises
- Clean-desk spot checks

Target Audiences

- Executives
- Managers

- End users (general staff)
- IT staff
- Specialized roles (internal)



Advantages

- They provide insights into cyber criminals' additional tactics in the physical world.
- They illustrate that not all security breaches occur online.

Surveys and Quizzes

Surveys, assessments, and quizzes are useful measurement tools to use before and after your security awareness program.

When using a quiz, please keep these recommendations in mind:

- Keep quizzes short (10–15 questions).
- Provide feedback with each question answered when you use quizzes as awareness tools.
- Withhold feedback when quizzes are used as evaluations to assess the awareness levels of your organization.
- Determine desired sample size based on your population size and aim for at least 95 percent confidence level with a margin of error of 5 percent in the responses.

Target Audiences

- Managers
- End users (general staff)
- IT staff
- Specialized roles (internal)
- Contractors
- Business partners
- Clients
- Suppliers

Quiz Example

Question 1/125

Which of the following characteristics make mobile devices vulnerable to loss or theft? *Select one or more answers.*

- ☑ Their portability
- ☐ Their connectivity
- ☑ Their size
- ☑ Their resale value

✓ The portability, small size, and resale value of mobile devices make them vulnerable to loss and theft. Connectivity is also one of their characteristics, but it does not make mobile devices vulnerable to loss or theft.

Advantages

- They provide a means to measure current levels of awareness, behavior tendencies, culture integration, program satisfaction, and so forth.
- They allow you to prioritize awareness topics.

- You can give participants a choice to opt out of online training if they pass the pretraining evaluation.
- You can measure overall gains and knowledge retention (a pre- and post-training assessment).
- They help you determine culture and motivation.

Defining Your KPIs

Once you have selected your content and campaign objectives in your planning phase, the next task is to express your KPIs and metrics.

Data gathering is an essential part of your security awareness program. The metrics you define and collect allow you to measure your program's progress and performance, providing you with crucial insights into its effectiveness. (This subject is discussed further in Step 4—Measure section of this book.)

Your metrics must align with your program goals and campaign objectives. For example, you might track course enrollment, course completion details, phishing simulation results, and other indicators to determine whether the target audience meets the goals and objectives you have identified.

As you decide on your security awareness metrics, you need to check that:

- These metrics are readily available
- Somebody can capture these metrics
- These metrics are understandable by those to whom you will present your findings
- Your security team agrees with the publishing frequency of your metrics

Common Metrics

When you deploy security awareness campaigns, you have a unique opportunity to collect information that lets you know how well your security awareness program is progressing.

Awareness measures fall into five different categories, each providing specific insights into your program or campaign:

- Training statistics
- Participant satisfaction
- Training effectiveness
- ROI
- Subjective indicators

Training Statistics

Metrics in this category are mainly related to online training:

- Percentage of participants who have completed training
- Percentage of participants who have yet to complete training
- Pass/fail distribution
- Course completion rates of the various organizational units/departments

Participant Satisfaction

Metrics in this category are related to participant and stakeholder satisfaction with security awareness campaigns:

- Ease of accessibility
- Appeal of content
- Relevance of content to day-to-day activities
- Percentage of overall satisfaction

Training Effectiveness

Metrics in this category are related to determining which resources reduce cost and maintain quality standards:

- Most popular awareness activities, sorted by cost
- Number of attendees per event, sorted by the average cost per attendee
- Most popular newsletter article, based on analytics
- Participant engagement with reinforcement tools

ROI

Metrics in this category are related to the benefits of investing in positive behavioral changes:

- Reduction in password reset tickets
- Reduction in the numbers of computers that must be reinstalled because of infections
- Reduction in stolen or lost computer devices
- Reduction in computer fraud-related costs to the organization
- Reduction in computer downtime linked to risky behavior

Subjective Indicators

- Office chatter arises about aspects of the security awareness program
- Champions start to surface
- Informal discussions are occurring about topics within security awareness
- Funding of security awareness programs is easier to obtain
- Executive Awareness Program Topics

EXERCISE

DEFINING YOUR METRICS

For each awareness campaign, identify 2 to 3 objectives. For each objective identify 1 to 3 measures:

- Objective name
- Supporting metrics
- Collection method and source
- Expected results
- Effectiveness indicator
- Follow-up action if objective is met or not met

When you deploy security awareness campaigns, you have a unique opportunity to collect information that lets you know how well your security awareness program is progressing.

Creating Your Communication Plan

To keep your security awareness campaign top of mind, your communications must strategically advertise your campaign to target audiences. A planned yet flexible timeline of communications helps to mobilize your audiences throughout the campaign to help realize your campaign objectives such as:

- Achieving high participation rates
- Increasing security visibility
- Keeping security awareness top of mind
- Developing a security culture

Consistency is also essential, as it will help brand your campaign and establish a relationship with your target audiences. A communication plan has two components:

- Communication strategy
- Communication calendar

Tip: We strongly recommend asking your organization's communications, marketing, and change management department(s) to contribute to your communication strategy and plan. Their expertise and experience in previous organization-wide campaigns as well as their knowledge of the upcoming organizational events will prove very beneficial.

Communication Strategy

Your communication strategy must identify the following:

- Who is responsible for drafting and/or signing memos, emails, and so forth
- Best times to communicate to maintain the momentum
- Key messages
- Languages that will be used
- Preferred communication channels (e.g., meetings, email, security portal)

Effective Communications

What will you say about your security awareness program and why? Is your message clear? Will people interpret what you are saying the

way you intended? What do you want your target audiences to do? Will they act?

Effective communications require facts, knowledge, and understanding of your organization's culture. You should look back to Step 1—Analyze to remind yourself of your target audiences, their motivation levels, and get inspiration on ways to talk to them (i.e., tone, level of language, topics).

Involve your security awareness team and coworkers in the communications component to be sure you are in line with your target audience and that you are on track for a successful campaign.

Do what works!

Go ahead and get creative. Grab attention and make an impact.

Creating Your Communication Plan

- Choose a variety of communication tools: posters, banners, emails, intranet, and so forth.
- Brand and market your campaign for increased visibility.
- Use the security awareness platform as a communication channel, not simply for course delivery or phishing attempts.
- Make it fun!

Communication Calendar

Your communication calendar should include details about every communication activity included in each of your campaigns, even if the communication strategy is the same for all. Recording activities at this level of detail helps you anticipate any challenges you might encounter with multiple sites, remote users, multiple languages, and so forth.

EXERCISE

CREATING YOUR COMMUNICATION PLAN

Questions to answer:

- Who is responsible for drafting and/or signing memos, emails, and so forth?
- What are the best times to communicate to keep up the momentum?
- What are the key messages?
- Which languages will be used?
- What are the preferred communication channels (e.g., email, security portal, internal collaboration tools)?

Tip: You may work in the field of information security, but if you want your security awareness program to be impactful, you also have to think like a marketing or communications expert so your target audiences respond positively to your "call to action," which is: *Be part of the solution. Let's prevent security breaches. Participate in our organization's awareness training today!*

Each Communication Calendar Must Include:

- Date
- Sender
- Recipients
- Communication channel used
- Key messages
- Potential blackout periods

Date	Type of Communication	Audience	Sender	Key Messages	Channel
	ISA Program kick-off	All employees		Inform user of Roadmap and upcoming campaign (FOCUS on Program and why)	Email
	ISA Campaign kick-off			Inform user of upcoming campaign (FOCUS on online training)	Email
	ISA End User campaign kick-off			Course now online + login credentials	LMS
	Reminder email #1			Remind of deadline and importance	LMS
	Reminder email #2			Remind of deadline and importance	LMS
	Reminder email #3			Remind of deadline and importance	LMS
	Course completion thank you email			Thank you for completing the training	LMS
	End of awareness campaign and results			Thank you with metrics and upcoming events	Email
	Launch video and newsletter			Reinforcement	Email
	Phishing simulation results			Inform about phishing simulation and results	Email
	Launch awareness level survey			How to access and why	Email

Times to Communicate

- Pre-
- Campaign launch
- During
- Post-

Pre-campaign.

- Announce the upcoming program/campaign
- Mobilize participants
- Inform them of their responsibilities

I usually suggest sending out the program announcement once (or yearly). It should be signed by your security awareness sponsor. Subsequently, send a campaign announcement for each separate campaign.

Tip: You may want to send one or two separate communications, as you may have different key messages for managers than for other participants.

Campaign Launch Communications.

- Use to officially launch the security awareness campaign
- Send on the day the online training course goes live. These communications must be concise and clear, explaining:
  - How to access online training (including LMS credentials)
  - Whether training is mandatory or voluntary
  - Required training completion dates
- Announce how phishing simulation will be part of the awareness program and how users should report suspicious events

- Announce and encourage users to participate in quizzes and surveys and how their responses will help develop the program

During Campaign: Online Training Communications. People frequently make the mistake of launching a campaign but not following up with additional communications. To keep the momentum going after the campaign launch, you can use online training communications to boost participation.

During the online training period, use communications to:

- Mobilize and motivate your target audiences
- Send reminders to those who have not yet completed their training
- Send thank-you messages to those who did complete their training
- Send certificates of completion to those who passed the training
- Share updates and progress reports with participants

During the post-training period, use communications to:

- Officially inform your target audiences that the campaign has ended
- Publish campaign results
- Continue follow-ups with anyone who did not complete the training during the allotted time frame
- Inform new hires of past campaigns that may be required
- Announce the next campaign

Keep your target audiences informed and engaged with creative, strategic, well-designed communications at different critical moments of your security awareness campaign or program.

After the campaign, communicate the results by:

- Sending dashboard results to department managers
- Sending results to users on their own dashboard
- Including competition results if you integrated a competition
- Sending each user their overall Security Awareness Score
- Telling them what will come next

Creative, Impactful Communication Tips

The keys to your success are communicating at strategic moments and keeping your messaging engaging. The campaign's communications should:

- Inform participants about accessing the online training, the completion deadline, and who to contact for support.
- Provide information about why security is essential and why you are implementing a security awareness program.
- Present the online training topics in a separate communication before the campaign launch.
- Provide consistency, flow, and branding across your communications. For example, each message should build on previous communications. Consider adding an awareness slogan and logo.
- Provide an email address for participant feedback.
- Choose your signatories according to the purpose and content of the messages. For example, consider an executive or program sponsor to announce your program or campaign.

- For messages on how to access training, it may be better to feature the unit that will support the signatory.
- Once you have compiled the quiz results, identify strong and weak areas and deliver key messages based on the results.
- After a phishing simulation, provide high-level results and remind employees of best practices. Share the scenario used and show them the indicators so even those who did not participate have an opportunity to learn.

If your communications are creative, impactful, and attention grabbing, you are more likely to reach your desired participation rates.

Selecting and Customizing Your Communication Materials

Give your security awareness campaigns a boost using different communication reinforcement tools, such as posters, videos, newsletters, emails, and web banners to:

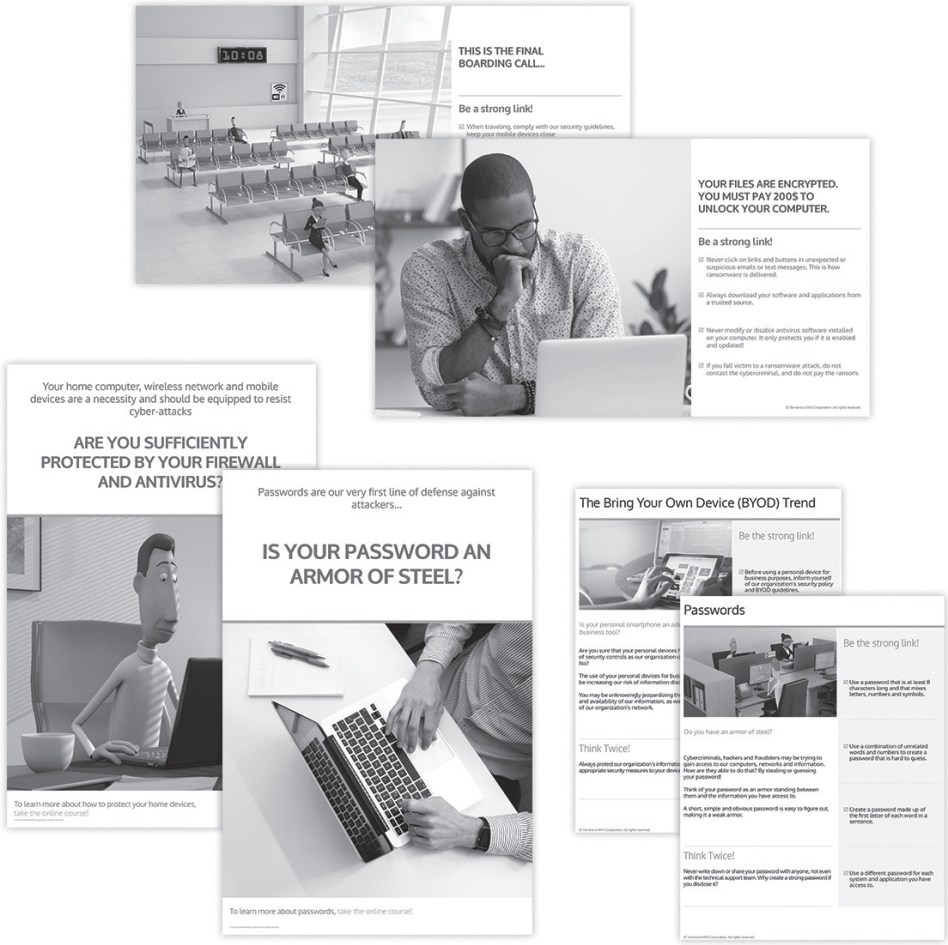
- Highlight security best practices
- Reinforce your overall messaging
- Maximize the visibility of your security awareness program

Target Audiences

- Executives
- Managers
- End users (general staff)
- IT staff
- Specialized roles (internal)

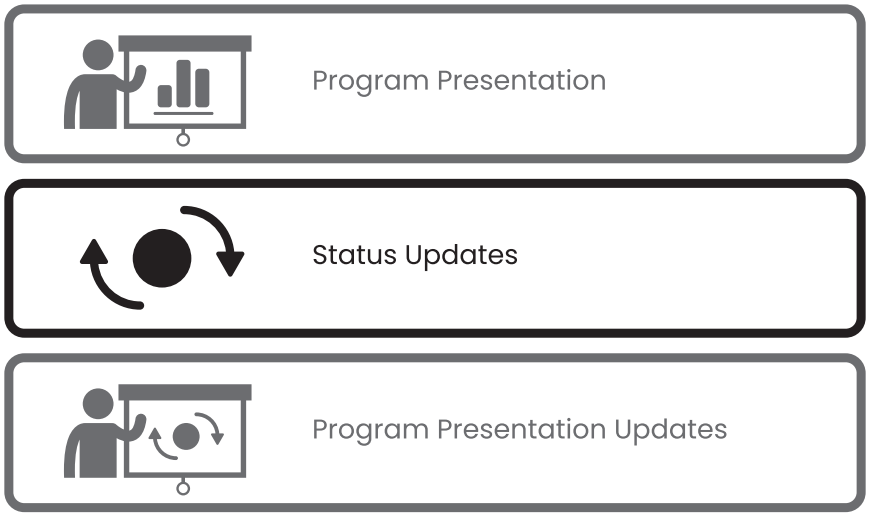
Advantages

- Publicize and market your upcoming security awareness program (e.g., posters)
- Emphasize your message (e.g., teaser video)
- Recap necessary knowledge (e.g., newsletters)
- Reinforce knowledge (e.g., microlearning) about a specific risk, threat, or best practice



Presenting Your Security Awareness Program

Now that you've defined and planned all the program components, it is time to consolidate everything into a presentation highlighting the main elements of your security awareness program and communication strategies.



Tip: Present your program as an answer to a business problem that you want to solve.

Your target audience for this presentation could be a security governance committee, security awareness team members, and other stakeholders.

If you need to add supporting arguments for your program to your presentation, see the Preface of this book, where I thoroughly discuss why it is important to design and implement a security awareness program.

Tip: Once it is completed, use key slides from the security awareness program presentation to create an executive summary.

Program Presentation Considerations

A good presentation tells a compelling story and is easy to understand as well as visually appealing. At a minimum, you should include the following in your security awareness program presentation:

- General introduction to the state of information security and your organization's current level of awareness (e.g., results of assessments, phishing, etc.)
- Legal and regulatory awareness training obligations of your organization
- Security awareness program scope (topics), objectives, audience, content, and KPIs
- Campaign deployment roadmap and program milestones
- Security awareness team members and additional contributors

Status Updates

If decision makers require regular status updates, consider including the following information:

- Project milestones, time frames, and current status
- Campaign results, lessons learned, and an action plan to deal with shortcomings

Program Presentation Updates

You should update your program presentation at least once a year, preferably after each major security awareness campaign and before each stakeholder meeting.

Since the program presentation is a strategic document, limit the information you include to the leading strategies and milestones. Using graphics to illustrate your points is very helpful.

If needed, more in-depth details, such as your communication plan, can be provided as supporting documents.

Executive Awareness Program Topics

Cyber security awareness programs are large-scale projects that have the potential to influence an entire organization. That's why getting buy-in from executives in various departments is a crucial step. Directors in operations and finance will be the two who first come to mind, but it might be helpful to reach out to HR, communications, and specific business groups to cover all fronts.

Although each department will have its questions and issues regarding the program, you should present it and what you expect from them in the same way to everyone. This meeting should be led by the CISO in person and structured in the following manner:

1. Introduce organization's information security function.
2. Demonstrate that information risks are business risks.
3. Provide executives with the foundation for future discussions and engagement.
4. Present at a high level the information security strategy.
5. Inform about common threats and best practices (both corporate and individual).

It might be helpful to close this presentation by sharing a few common concerns and favorable outcomes regarding cyber security programs within companies such as:

1. Cyber security is now a core product and value-chain issue, not just an IT concern, since it can dramatically improve the delivery and stability of products and services.
2. Attackers will always have more time on their hands to develop new attacks. That's why awareness programs are so crucial; awareness is the only proactive cyber security tool in an organization's arsenal.
3. Except for a few heavily regulated sectors, many industries lack a standard approach to cyber security in their product offering.

Include cyber security in the design of business ventures, products, systems, processes, services, and so forth from the start to make them more robust and appealing to specific fields.

Creating and Running a Security Awareness Ambassador Program

Once executive approval has been secured, budgets have been approved, and the direct managers have been briefed on the programs, it's time to get buy-in from the employees themselves. The best way to achieve this is by building an ambassador program.

Building an ambassador program starts with identifying a few cyber security champions within the workforce who will advocate for you by communicating with their coworkers. Their advocacy tasks can range from reminding coworkers about training to bringing up cyber

security awareness in team meetings. They might even act as the first line of defense by speaking up when they see their coworkers behaving dangerously.

Five Steps

Here are the five steps to building a security awareness ambassador program:

Step 1—Apply or Nominate the First Ambassadors

Once you have identified the time commitment and other program expectations, the program benefits or incentives that can be offered, and the program's specific responsibilities, send out a call for applications or nominations.

Start by introducing and communicating what the Security Awareness Ambassador Program entails. Explain how employees and team members can apply to the program and encourage them to get approval from their direct supervisor first.

Ambassadors should not be members of the information security team or hold leadership roles. The culture of security is more likely to permeate through the organization via ambassadors from the field team, rather than management, because the guidance is communicated peer to peer versus top down.

Step 2—Review and Select Applicants

When reviewing the applications and nominations that come in, select your initial ambassadors to represent a cross-section of locations, roles, and service lines within your organizations.

Instead of technical knowledge, look for an attitude and a desire to learn and take responsibility. Ideally, candidates will understand

the region where they work, their specific department, and their colleagues' challenges.

Step 3—Launch a Training and Mentorship Program

Ambassadors will require a training and mentoring program. Position your organization well by planning at least a three-month period to prepare your initial group of ambassadors.

Before awarding the internal accreditation to your ambassadors, consider requiring each to complete all security awareness training modules already offered by your organization and attend security monitoring workshops led by Security Team members. Also, have them complete any reading assignments and deliver a security awareness presentation to their business unit as practice for becoming their team's cyber security voice.

Eventually, the ambassadors in the program will be able to train the next wave of ambassadors.

Step 4—Host a Certification and Induction Ceremony

It's important to publicly acknowledge not only your first group of ambassadors but each one that follows.

Consider hosting a ceremony or asking the executive team to publicly acknowledge the ambassadors. The executives are now, after all, the point of contact within their teams for enhanced cyber security awareness.

Step 5—Manage and Measure the Ambassador Program

Once you're off and running, be sure your information security team continues to provide ongoing communication and resources to the ambassadors. Consider creating a forum for ambassadors to

exchange ideas. And if some ambassadors need to leave the program over time, be sure to develop a way to cycle new ambassadors into the program.

In addition to managing the program, measure its effectiveness, too. Track the number and types of inquiries or incidents submitted or reported by users to the ambassadors. Look at the number of inquiries submitted from ambassadors to the information security team.

And finally, look to see, after a predetermined period, if behavior improvements are made as a result of the program. One way to achieve this is by hosting a phishing simulation or quiz before the launch of the Security Awareness Ambassador Program and then again several months into the program.

Gamification

Completion of content is the name of the game. Any tool that can lead to higher completion rates should be deployed since it has a direct impact on the effectiveness of the program. Gamification can be a powerful solution in that regard. Before implementing gamification, consider your industry, the culture of your organization, your audience, and their region. Gamified content may not be perceived as serious, not accepted in certain organizations, or confuse the learner. Be prepared to address these challenges by selecting gamified content that is suitable for your environment and audience.

Gamification allows users to have increased engagement while they learn, offers a variety of ways to provide feedback to the participant and improve knowledge retention.

Gamification is inspired by systems used in video games to reward users for accomplishing virtual tasks. These features can take on many different forms, and each has a very specific goal and usage.

Points

Points are used to track desired behavior, keep score, and provide feedback. Points awarded at the end of each section of a program act as a soft reward and a way for the user to gauge their progress.

Badges

Used to proudly present an achievement, these badges are awarded upon completion of a program section or to the best performing employees. It's important to display them in a public way such as including them in email signatures or announcing them within the company intranet.

Levels

Awarding levels to employees recognizes their expertise on a specific subject to their coworkers and becomes a point of pride.

Leaderboards

An internally accessible leaderboard promotes friendly competition among employees and can be another way to showcase points, levels, and badges awarded.

Rewards

Rewards that tie in the real-world nature of the cyber security program might include physical prizes such as company swag, gift cards, or even snacks.

Motivation, Consequences, and Escalation

Security awareness programs are mostly accomplished via the content itself, but you will probably have a few stragglers and less attentive

individuals in the process—it's human nature. It's crucial to have a robust and well-defined escalation process for people who don't seem to be getting the message (e.g., repeat clickers in phishing simulations) or policy violators.

Here is a sample escalation process that should be appropriate for companies of all sizes:

- 1 fail/violation—Message from IT Security
- 2 fails/violations—Message from IT Security and CISO/CIO in cc
- 3 fails/violations—Message from IT Security, and Supervisor and CISO/CIO in cc
- 4+ fails/violations—Message from IT Security, and Supervisor, Department VP, and CISO/CIO in cc

In smaller organizations, the CEO may be involved at the individual level. In larger organizations, the CEO may be informed on which department has the most repeat clickers so the CEO can put pressure on the Department VP.

The purpose of escalations is to:

1. Notify management that they have a high-risk user
2. Educate the clicker/violator and provide best practices
3. Help management understand the circumstances that caused the user to click or not follow policy guidelines

It is important to address both desired and undesired behaviors to effectively ingrain security awareness into your company culture.

Desired Behaviors

- 0 failed attempts after X (at least 3+) simulations—Select two or three individuals at random and, with their permission, recognize them within the organization as phish detection experts.
- 3+ reported phishing attempts—Select two or three individuals at random and, with their permission, recognize them within the organization as superstars contributing to the protection of the organization and their colleagues.
- The employee noticed a situation or event and, by alerting the proper channel, prevented a data breach or other information security incident.

Undesired Behaviors (Phishing)

- 2 failed phishing simulations or real attacks—Note from IT. Assign additional training.
- 3 fails—Message from a supervisor with CIO copied. The message should include how stolen credentials or stolen data can affect the organization based on the specific role of the user. Assign additional training.
- 4+ fails—Message from a supervisor with VP and CIO on copy. Explain how any further failures may result in the temporary loss of internet access. Invite clickers to share their story with their coworkers during a staff meeting or other gathering. Assign additional training.

Other Options

Below are some additional actions you can include as part of follow-up procedures. The more opportunities you leverage to communicate with your users, the more chances you provide for them to learn.

User Profiles. You can also set up user profiles based on click rates and awareness and address them with a custom learning journey:

- New hires: Never phished, never trained
- Champions: Never clicked
- Clicked once: Clicked last simulation
- Frequent clickers: Clicked in X out of the last Y simulations

Simulation Follow-ups.

- Each phishing simulation you conduct gives you the opportunity to reach out to the participants and feedback and learning activities:
- Deployment of surveys to assess knowledge and behaviors at the time of the event
- Exposure to phishing scenarios for information purposes and awareness
- More frequent deployment of mandatory reinforcement activities such a micro- or nano-learning

Follow-through with Impact of Simulation. For those who fell victim to a simulation, you may want to imitate the negative impact of a phishing attack. Use the following examples as an exercise to encourage users to experience the negative consequences of a phishing attack:

- Credential harvesting: Your password was compromised and now you must change it. Identify all the systems and data a hacker would access with your accounts.

- Malware/ransomware: Your PC is not available for two hours while we remove the malware. You need to explain to your manager why you cannot be productive.

- Identity theft: Your personal information was stolen, and you need to protect yourself. Identify the steps required to protect yourself against fraud and identity theft through the use of your personal information.

CONGRATULATIONS!

You have just completed Step 2 of the Terranova Security Awareness 5-Step Framework—Plan.

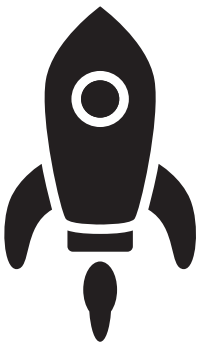
You have compiled some very important data, information, and insights that will guide your decisions in Step 3—Deploy.

Plan Categories:

- Team
- Roadmap
- Product
- KPIs and Metrics
- Communication
- Program Presentation

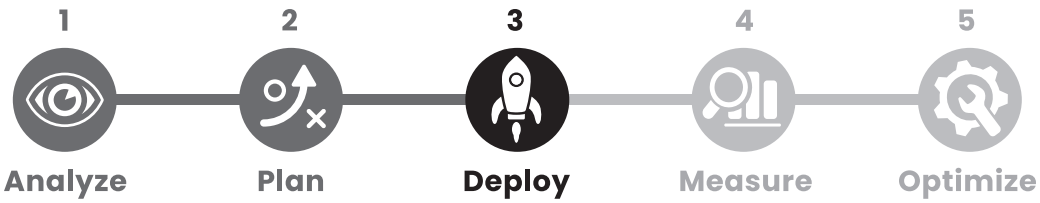
Ready for Step 3—Deploy? Let's do it!

EVERYTHING YOU HAVE COMPLETED SO FAR IS PREPARING YOU FOR AN **EFFECTIVE LAUNCH.**



THREE

STEP 3: DEPLOY



Welcome to Step 3 of the Terranova Security Awareness 5-Step Framework—Deploy.

All your hard work—all your analysis and planning—has led to this moment. You are now ready to deploy your security awareness campaigns.

Preparing for Deployment

You should always deploy your campaigns in three phases:

- Test
  - Before you launch each campaign, test the technical functionality of your campaign, your content, and the user interface to make sure there are no glitches and everything will run smoothly on deployment day.
- Launch
  - Launch the campaign and communicate with employees.
- Remind
  - Reinforce your security awareness messages using various communication tools (e.g., posters, newsletters, e-blasts and web banners, videos, etc.) to remind everyone of the importance of participating.

Testing 1, 2, 3

Before your kickoff, you must pretest to ensure the campaign runs smoothly. You will need to follow up with reminder messages during and after your deployment to promote the activities and better position you to reach your security awareness campaign objectives.

Make your launch day as stress-free as possible by testing beforehand!

Why Do a Test?

- To validate that your technical environment (i.e., operating systems, computer models, bandwidth) will support the program

- To minimize unforeseen deployment glitches by documenting and correcting any issues discovered during the testing phase
- To give yourself added peace of mind that you have not overlooked any crucial deployment details
- To validate the flow and customization of content
- To improve your probability of success

Making Time for Testing

To give yourself enough time to correct any issues that may arise during the testing phase, remember to factor a buffer into your planned rollout schedule. Testing only one week before rolling out a campaign, for example, may not give you the time you need to correct any problems. Instead, plan at least one whole week of testing along with one to two additional weeks to make any adjustments that might be necessary.

Make sure testing is in your communication calendar as a predeployment activity.

There are three main types of prelaunch testing:

- Content review
- Compatibility and performance testing
- Pilot testing

Content Review

In Step 2—Plan, you selected your program content and divided it into a series of campaigns. Before deployment, you should have the content and activities of your campaigns reviewed by key people to ensure they align with your organization's needs, objectives, and compliance obligations.

Ideally, you should have all the content of your first year of campaigns reviewed at once so you are always ready to launch a new campaign.

Consider asking the following people to be involved in the review process:

- SMEs, to review the course and quiz content and customization
- Your security awareness champions or ambassadors, to review the courses and quizzes and give their feedback on the content and its relevance to their day-to-day activities
- Native speakers, to review any translations to ensure that the terminology is correct and culturally appropriate
- Departments with a stake in the program, to review its content and associated messaging (e.g., audit, compliance, legal, HR)
- Internal departments, if they are used in the phishing simulation scenarios
- Communication or HR departments, if conducting a survey. (Note that some organizations may have restrictions on collecting employee opinions.)

Tip: Do your content review as early as you can so it doesn't impact your scheduled launch date.

Tip: Remember to leave enough time in your overall deployment schedule to conduct the content review and make any necessary adjustments.

EXERCISE

YOUR CONTENT REVIEW

List every person who should review your content to align it with your organization's needs, objectives, and obligations.

Identify individuals in the following areas:

- Security subject matter experts
- Experts on internal policies
- Native speakers of selected languages
- Change management team
- Human resources

Compatibility and Performance Testing

You put so much time and thought into your campaign; the last thing you want to discover on launch day is that a technical issue is sabotaging your rollout schedule. Therefore, it is essential to conduct several compatibility and performance tests with assistance from your IT and/or HR department(s) to ensure everything is ready for your deployment.

Integration. Ensure the online course SCORM (Sharable Content Object Reference Model) packages are compatible with your organization's LMS, if applicable. This will not be an issue if you use the SCORM vendor's platform.

Browser Compatibility Testing. Verify that the various web browsers and devices your participants will use to access the online training are compatible with the awareness platform. Make a note of incompatible web browsers and specify the system requirements when you send out your launch email.

Form Factor Testing. Make sure to test the SCORM package using the various form factors in your organization (e.g., smartphones, tablets, laptops, desktops). If access is allowed from personal devices, additional technical testing will be needed. Make a note of any incompatible device types and specify the system requirements when doing the training and when you send out your launch email.

Performance Stress Testing. Ensure your platform and network can support the number of users who may be accessing the course material simultaneously, especially at the initial launch or near the campaign deadline. If you are using the SCORM vendor's platform over the internet, ensure that your internet bandwidth is sufficient for the volume and location of concurrent trainees scheduled for the launch.

Security Testing for LMS Web Application. If your LMS is public facing, ensure it is tested for vulnerabilities and patched accordingly.

Remote Location Performance Testing. At remote locations (such as stores), network bandwidth might be much more limited than at your corporate headquarters. If this is the case, stagger the number of concurrent trainees from that remote location to reduce simultaneous demand on the bandwidth.

Remote Access Performance Testing (e.g., VPN). Security perimeter access mechanisms may affect how online training is accessed or delivered. Running a course over a VPN, for example, may slow down the animations in the course.

Firewall and Anti-spam Settings. If you use an external platform to send your launch and reminder emails, you will probably have to "spoof" your email address so it looks like an internal email. You need to notify your network team not to block these emails by your firewalls or anti-spam mechanisms.

User Synchronization. Verify that the user list is in the platform or that the synchronization process with the platform produces an accurate trainee database.

Learning Activity Testing. Verify the following elements for each of your training activities:

- Course description, title, and icon
- Completion/success criteria
- Course duration
- Email notifications and certificates
- Course access

Phishing Simulation Testing. Verify the following elements for each of your phishing simulations:

- Email templates and links
- Landing page text and browser tab titles
- Feedback page and linked training
- Email delivery and web page accessibility

Also verify reports for false positives and leverage the IP exclusion list.

Quiz/Survey Testing. Verify the following elements for each of your questionnaires:

- Access link and password
- Access permissions
- Welcome message and thank-you note
- Question-answer format
- Text (e.g., when referencing internal policies, departments, procedures, etc.)

Platform/Single Sign-On and User Provisioning Integration. If you are using SSO or SCIM functionalities to set up your trainees, you should ensure that their enrollment, deregistration, authentication, and authorization all work as you intended.

User Support Procedures. Establish procedures for your support staff and helpdesk, and then test those procedures. Support staff must be informed on how to handle calls related to issues with the learning and phishing activities.

Phish Reporting. Establish a mechanism for users to report suspected phishing attempts. Your mechanism should be able to filter simulations so the support team does not have to triage simulations. The support team should also be informed on how to respond to direct calls from users reporting phishing simulation emails. For example, you may not want to inform the caller that a simulation is in progress and simply thank them for reporting the event.

Browser Settings. Determine whether the awareness content requires a specific browser setting (e.g., pop-ups) and ensure compatibility with the standard settings in your organization.

Verify Reporting. After loading the trainee database, verify that platform reporting capabilities will satisfy your metrics and compliance requirements and that participant groupings are adequate. Leverage existing filters or create custom ones to allow for more granular reporting.

User Synchronization. After loading the initial trainee database, ensure you have an automated or manual process to keep the trainee list up to date. If the process is manual, validate before each training activity, phishing simulation, or quiz.

Pilot Testing

A pilot test is a real-life deployment of your complete campaign, including related emails, but it is presented to a minimal audience. This test allows you to troubleshoot any remaining issues before your actual full-scale deployment.

Who to Include in Your Pilot Project. Test your campaign on a small cross-section of the audiences you are targeting in your upcoming campaign. If possible, select pilot participants from various access points (e.g., corporate HQ, remote locations, remote dial-up or VPN)—preferably choosing those you determined to be "intrinsically motivated" in Step 1—Analyze.

In your pilot, be sure to include:

EXERCISE

YOUR COMPATIBILITY AND PERFORMANCE TESTING

Create your list of contacts assigned to do the various types of testing. This will help prevent technical glitches that can negatively impact launch day.

Required Technical Test	Contact(s)	Date Test Completed
Integration		
Browser compatibility testing		
Form factor testing		
Performance stress testing		
Security testing for platform web application		
Remote location performance testing		
Remote access performance testing (e.g., VPN)		
Firewall and anti-spam settings		
User synchronization		
Platform/Single Sign-On integration		
Test production deployment monitoring procedures		
Pop-ups		
Verify reporting		
Activity testing from start to end		
Other:		

Remember to leave enough time in your overall deployment schedule to conduct your compatibility and performance testing and make any necessary adjustments.

- Security awareness ambassadors or champions that you selected in Step 1—Analyze
- Additional contributors you selected in Step 2—Plan
- Members of your IT team—as many of them as possible since they will provide you with actionable observations
- Native speakers from each region if you are deploying in multiple languages

Reporting Issues. Establish a precise feedback mechanism so participants in your pilot test can quickly and efficiently report any issues they uncover. The report should include:

- A short description of the problem
- What action led to the problem
- A screenshot of the problem, if possible
- The contact information of the person reporting the problem

False-Positive Trapping. During the testing phase, it's also crucial to ensure your phishing simulation data will be accurate and not laden with false positives (i.e., simulation results that are incorrectly reported as an undesired end user action). If a phishing simulation's results come back at 100 percent or a similarly suspicious number before it's launched to all employees, your awareness training administrative team must follow up. Perhaps IP addresses need to be added to an exclusion list or other technical optimizations are required.

The False-Positive Trap function in the Terranova Security Awareness Platform makes the process of avoiding false positives quick and easy and adds the possibility of automating certain tasks.

What to Evaluate during the Pilot Project.

- Access to online training
- Course content
- Course content screen flows
- Course audio quality at different access bandwidths
- Communications delivery (e.g., email, videos, web banners)
- Language and localization

When you conduct your pilot project, advise your IT staff to give you feedback on any pilot technical issues.

EXERCISE

YOUR PILOT TEST

List different people in the various departments whom you want to be involved in your pilot testing. Remember, your list should include security awareness ambassadors or champions you selected in Step 1—Analyze, additional contributors you selected in Step 2—Plan, and members of your IT team.

Identify individuals in the following areas:

- IT operations
- Security operations
- Help desk
- Security ambassadors
- Business representatives

Remember to leave enough time in your overall deployment schedule to conduct your pilot test and make any necessary adjustments.

Launching Your Campaign

Communicate, Communicate, Communicate

Now that your testing is complete and you've completed all the necessary adjustments or corrections, it's time to use the communication plan you developed in Step 2—Plan. You can now begin sending out the various pre-deployment communications that you identified in your communication strategy and calendar.

For an excellent kickoff, have your security awareness program sponsor send out email or video content stressing the importance of the program or campaign to your organization. Another good way to get the hype started is to host "teasers" about the upcoming campaign on your internal intranet. Also try hanging posters that hint that a special program is coming.

Use your imagination and find ways to make your target audience curious about what is in the pipeline.

Launch Day Has Arrived

> You've crossed every *t* and dotted every *i*. Now you're ready to launch!

Today is launch day, and you intend to make security a hot topic of conversation.

At this point, you should have already sent out your pretraining communications outlining why the campaign is necessary and other important details such as the topics you will cover and whether the training is mandatory (see Step 2—Plan).

The *Musts* of Your Campaign Launch Communications

When you launch, you want to be sure your messages—whether communicated via email, posters, videos, or general assembly—clearly tell your target audiences:

- How to access the online training (if by email, include login instructions and the URL to access the training)
- Expected completion date
- Whom to contact for support
- If leveraging an awareness partner, inform your audience that communications may originate from an external source

This is your time to shine. Be prepared, be visible, and keep up the momentum!

You're Ready for Deployment!

The deployment phase requires you to:

- Be prepared
- Be visible
- Keep up the momentum

Be Prepared

It's easy to get so caught up in taking care of the last-minute details that we overlook basic things like ensuring everyone is ready for action.

To prevent a last-minute panic, plan to check in with your team a day or two before your launch. Double-check with everyone who plays a role in the deployment phase. Schedule a quick call or send an email with a strong subject line. If your email platform does not allow you to see who opened your message, create an email with "Please confirm that you are ready" in the title email.

What you need to know:

- Are the team members aware of their responsibilities?
- Are the platform support personnel on standby?
- Have you alerted the helpdesk? (They may experience an increase in support calls.)

Expect the unexpected! Making sure you are well prepared will reduce the risk of snafus.

EXERCISE

LAST-MINUTE TOUCH BASE

List all the people in various departments who play a role in your campaign deployment to ensure they are all ready for action!

Identify individuals in the following areas:

- Help desk
- Human resources
- Communications team
- Management team
- Platform support team

This list is golden. Keep it handy and make sure you contact everyone on it a day or two before your launch to make certain they are all ready for action on launch day.

Be Visible

You want your target audiences to be enthusiastic and participate in your campaigns. Fortunately, information security is a pretty cool topic, especially in today's evolving cyber crime landscape, so it's not hard to develop engaging ways to create hype around your campaign, make it exciting, and get everyone talking about it. For example, you might:

- Create an event for the launch such as an assembly with refreshments.
- Put up eye-catching posters in common areas such as the cafeteria or restrooms.
- Set up a booth in the lobby to welcome employees and give training demonstrations.
- Promote branded giveaways (e.g., branded mugs or screen wipes).
- Offer your participants a unique email address to contact you with any comments, suggestions, or critiques regarding their training experiences.
- Add a prize drawing for participants who have passed the course in the required time.
- Organize a competition with a cyber game.

Tip: Get people talking about security, increase participation rates, and make your campaign a monumental success.

Leverage Cyber Security Awareness Month

October has become synonymous with cyber security, so we recommend providing some additional activities that are aligned with the international campaign or the one provided by the government in your region.

Leverage this time to discuss specific topics and tie them to being a responsible and secure digital citizen. Other periods to consider:

- Safer Internet Day (every February, date varies)
- Data Privacy Day (every January 28)
- World Password Day (first Thursday every May)

EXERCISE

BUZZ-BUILDING BRAINSTORM

Brainstorm ideas with your security awareness team. Explore creative ways to get people at your organization to talk about your security awareness activities. Examples:

- Mind maps
- SWOT analysis
- Whiteboard brainstorming
- Brainwriting
- Why analysis

Brainstorming can be a great team-building activity. Keep the mood fun and positive by encouraging everyone on your security awareness team to share their ideas.

Keep Up the Momentum

You want to get as many people as possible to start their training on day one. However, you may have to reach out to a significant percentage of your target audiences multiple times before they take part.

Some may have valid reasons such as juggling a full workload or being on vacation; they may simply need a friendly reminder. Others may be lukewarm to the idea, so you might have to find incentives to win them over.

If your participation rates are low in the beginning, stay positive and keep in mind the "rule of 7," a marketing precept that says people need to see or hear a message as many as seven times before they will act or respond.

Tip: You will have to reinforce your message to keep your campaign top of mind and get optimal results.

Stay Top of Mind

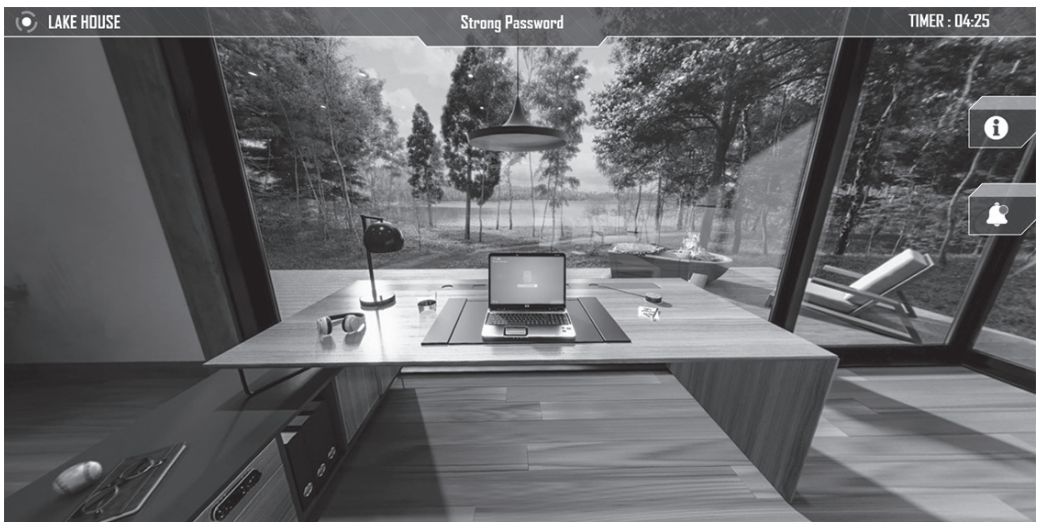
Too many people launch a campaign with great fanfare and then go silent. Instead, keep everyone engaged and motivated to participate by communicating with them at strategic moments throughout the campaign. For example:

- Go beyond email to get your message out there.
  - Podcasts
  - TV screens
  - Blogs
  - Infographics
  - Web banners and screen savers
  - Screens in common areas
  - Announcement during staff meeting
  - Internal social channels
  - Handouts and pamphlets

- Send out reminders emphasizing the deadline for participation and encouraging nonparticipants to join this new cyber security culture you are creating in your organization.

- Try a little gamification. Set up competitions among different departments, divisions, or locations by routinely publishing completion rates on your intranet.

- Use engaging reinforcement tools such as serious games, cyber security challenges, interactive videos, infographics, and so forth.



Make Your Activities Mandatory

You may need to make some of the awareness activities mandatory. This can encourage those who aren't intrinsically motivated to follow the training. Consider the following:

- When courses are presented as mandatory, the completion rates tend to be higher.
- Mandatory is defined differently by each organization and will vary based on the applied consequences for nonparticipation.
- It is common for organizations to introduce a mandatory program for new hires.
- Mandatory training follow-ups and escalations are performed by HR/LR and employee supervisors.
- Some organizations may limit access to certain resources or the internet until courses have been completed.

Increase Course Completion Rates

Increase your course completion rates with these practices:

1. Use short modules and varied formats.
2. Leverage continuous notifications and reminders.
3. Associate completion with yearly performance evaluation.
4. Include messages and best practices that help participants in their personal lives.
5. Send reminders from supervisors and managers.
6. Implement competition and rewards.
7. Provide recognition for top departments.
8. Present the department performance metrics to the executive leadership team.
9. Schedule Lunch and Learn sessions to increase interest.
10. Establish local or department ambassadors to promote awareness activities.
11. Provide each user their results and how they compare to the department, organization, etc.

Reinforce Your Message

You want your security awareness program or campaign to be a great success. Emails and memos, however, can generate only so much interest. Drive your message home with some additional engaging reinforcement tools.

Reinforcement tools are, in essence, marketing tools that grab attention, raise awareness, and ultimately trigger shifts in behavior. They include posters, newsletters, comic strips, videos, web banners, cyber games, and so forth. Using them in different combinations is compelling—people are more likely to remember a message delivered in a variety of formats.

Reinforcements can be used:

- To keep the importance of security awareness top of mind
- To reinforce your messaging so that participants retain what they have learned and actually correct their risky behaviors

Tip: Using reinforcement tools keeps security awareness fresh in their minds and makes your campaigns much more impactful.

Types of Reinforcement Tools

Our clients find these reinforcement tools especially useful.

Videos

Video content is extremely versatile and can be used at all stages of a training program. It's an

especially useful way to give context to some of the cyber security dangers you mention to your users, dangers that might seem abstract to them until they see the potential breaches playing out in a familiar day-to-day setting. After that, they might realize they really do need to change some behaviors.

Posters, Screensavers, Web Banners, Comic Strips, and Wallpapers

Reminders users encounter every day in the workplace are especially powerful. If your workforce is still in the office, place physical posters around cubicles and workstations. In a hybrid or fully remote environment, you'll have to get creative. Cyber security-focused wallpapers and screensavers are effective because users see them several times a day. If your company uses an intranet, web banners can also be an excellent way to display cyber security tips and reminders.

Newsletters

A security awareness training newsletter can serve multiple purposes. It might contain detailed promotional tools, a rundown of key cyber security tips and tricks, a preview of new learning opportunities, or even a combination of all three. Just make sure you set specific goals to focus your newsletter's intent.

Reinforcement Events and Activities

Although organizing events and activities requires more resources than the other items on this list, they can be the most beneficial. When you organize a Lunch and Learn, whether in person or virtual, for example, it allows users to ask questions and get answers in real time, and it also allows you to get a feel for what your users do and don't understand. You might also uncover issues that weren't brought up during user testing.

Important: You can complement communication and reinforcement tools with internal resources and communication channels such as your intranet, security portals, security FAQs, news feeds, internal security blogs, and articles in your organization's newsletter.

EXERCISE

REINFORCEMENT IDEAS

Think about exciting ideas that will keep your target audiences engaged after deployment. You may need to reach out to other departments, such as marketing and administration, to determine the budgets and logistics involved in implementing those ideas.

Consider which of the following you have the capacity deploy and at what frequency:

- Videos
- Posters
- Screensavers
- Web banners
- Comic strips
- Wallpapers
- Newsletters

For each one identify:

- What is the topic
- What is the purpose (e.g., promote awareness program or share best practices)
- Who creates
- Who deploys
- Where it is hosted
- Duration
- Consumption metrics

CONGRATULATIONS!

You have just completed Step 3 of the Terranova Security Awareness 5-Step Framework—Deploy.

When you deploy a campaign, it's a big day. All your hard work goes into action, and you have a lot of details to oversee. Remember to test, deploy, and then follow through with well-chosen reinforcement tools to make your campaign a great success.

Summary of Deployment Actions

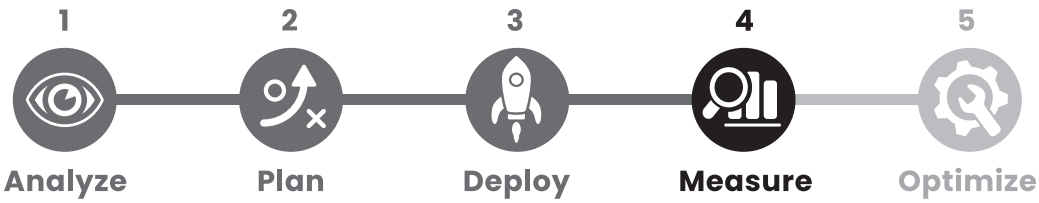
- Test
- Deploy
- Reinforce

Ready for Step 4—Measure? Let's do it!

THE SUCCESS OF YOUR SECURITY AWARENESS PROGRAM OFTEN DEPENDS ON **HOW YOUR METRICS ARE MEASURED, INTERPRETED, REPORTED, AND ACTED ON.**

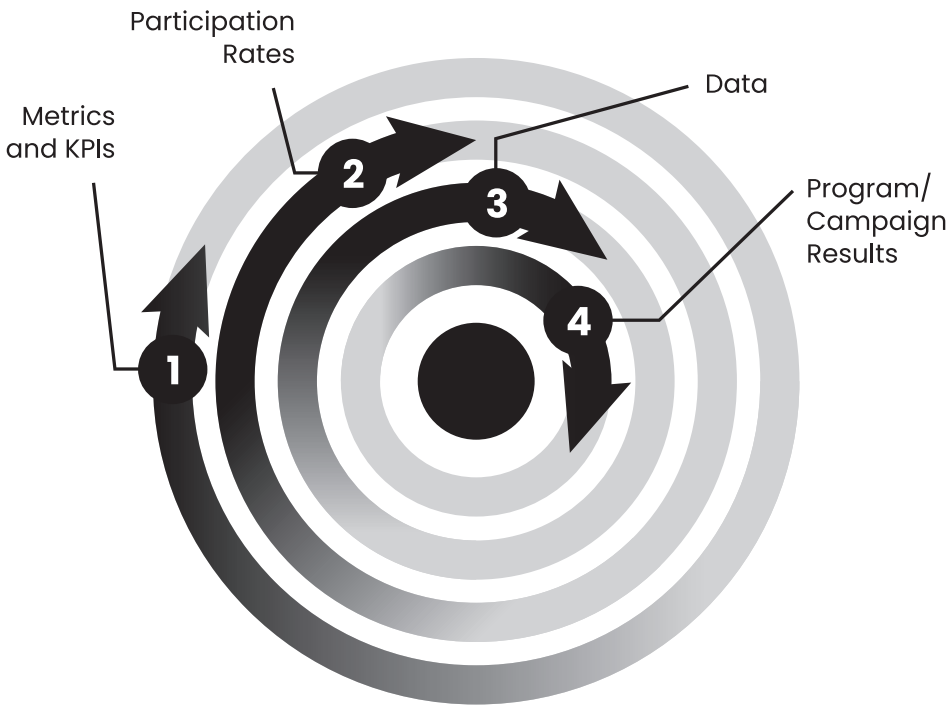
FOUR

STEP 4: MEASURE



Welcome to Step 4 of the Terranova Security Awareness 5-Step Framework—Measure.

Deployment of your security awareness campaign has begun, and you are sharing information on overall performance. In Step 4—Measure, you will use the metrics identified in Step 2—Plan to evaluate the success of your program and campaigns and determine if they are meeting your objectives.



These metrics will give you essential insights that you will use in Step 5—Optimize. You will compare your initial program goals with measurable results and identify new campaign objectives so you can tweak your next activities to make them even more impactful.

You've launched your campaign, and now you want to have a clear indication of how it's performing. Measuring performance, participant satisfaction, and compliance will allow you to identify areas where your program needs to be improved.

In this phase, you will:

- **Define and gather data:** Measure your progress according to your predefined metrics

- **Track progress:** Effectively manage and monitor your campaign/program
- **Report:** Communicate information about campaign performance to departments across your organization and demonstrate performance against your objectives

Define and Gather Data

In Step 2—Plan, I outlined what you should be tracking once you launch your security awareness program or campaign. Below is a recap of the different categories of metrics, followed by a review of the tools and indicators you can use to measure them.

Use the following sources as starting points to define metrics and gather data:

- Security awareness platform reports, knowledge retention surveys, and quizzes
- Helpdesk (ticketing) and incident reports
- Post-campaign satisfaction surveys
- Feedback obtained from the dedicated campaign email address (if any)

KPIs

In Step 2—Plan, you defined the objectives associated with your KPIs. These are the KPIs that you are tracking to monitor the effectiveness of your security awareness campaign. Assessing your KPIs will tell you if your participants learn and apply their new knowledge. For example, a reduction in security incidents would indicate that your campaigns are helping to change risky behaviors.

Measures are identified in three areas: Compliance, Behavior, and Culture.

- Compliance: Report on how many users have assisted in awareness activities. These metrics can be used to demonstrate that the program is being followed by the users and that management has a program in place (following best practices) to inform its users

- Behavior/Knowledge: Report on what knowledge the users have retained because of awareness activities and what helpful behaviors have been adopted

- Culture: Report on whether users are applying what they learned in the awareness activities. Are they going beyond the minimum required to ensure a cyber safe working environment?

When metrics are not available in a system, you can still collect data using surveys, quizzes, phishing simulations, social engineering exercises, or audits. User perception data, such as content appreciation or employee engagement, can be collected this way.

Questionnaires tailored to a specific role or employee segment can offer a more detailed analysis. You can capture statistics from those who are involved in a specific process, activity, or business process.

Other data collection techniques include one-on-one interviews where SMEs collect information and explain the risks in an area or subject (e.g., interviews with executives, key stakeholders, etc.).

Remember to also ask your information security professionals to record and communicate their observations to the awareness program manager. Their input can help you understand how the behaviors that

are communicated in the awareness program are actually being used in a job setting.

Clear and defined goals are essential to plan strategically and to develop an awareness program that is focused on producing tangible results. If you use the SMART approach, set goals that are S for Specific and focused on what you trying to achieve. Your goals should be M for Measurable, and that measure will come next when we discuss metrics and KPIs. Select goals that are A for Attainable for your organization or industry. Make sure that your goals are R for Relevant to your business environment and realities. And finally, set a Time-limit for achieving your goals with periodic reviews and adjustments.

1. Training Statistics

A mainstay of compliance reporting, training statistics such as participation rates can also provide information on behavioral and cultural changes. Most learning management systems allow you to track real-time training statistics (e.g., participation rates, time taken to complete training, pass/fail statistics, etc.).

For each online training campaign, monitor:

- **Success of outreach**, particularly campaign launch communications and access instructions (e.g., Did the email invitation reach all intended recipients?)

- **Participation rates**. Track these early and often. Although participation is often high for a few days after initial announcement, it tends to slow down in the following days. Knowing how this plays out will help you determine how soon to issue a reminder. For example, a low participation rate to

a voluntary pretraining survey is an indication that frequent reminders will be required.

- **Completion rates.** It is also important to track completion rates. Users may start the course but not complete it, either because they were interrupted or there were technical issues.

- **Time spent on course.** When a user completes a forty-five-minute course in under ten minutes, it may indicate a click-through behavior, where the training was not fully followed.

KPI	Metric	Effectiveness Indicator
Users are aware of information security risks and controls	Percentage of participants who have completed training	Increase in attendance
	Percentage of participants who have not completed training	Reduction in the number of employees who missed training without a valid reason
	Number of end users in various departments or units who have completed specialized training (e.g., IT staff, HR, Finance)	Increase in attendance
Increase the number of users who follow the complete course without skipping content	Time spent following online courses	Time spent equals or exceeds expectations
Users understand security threats and best practices	Results from quiz or survey	Higher scores in post-training quizzes and assessments

2. Phishing Statistics

Your analysis should leverage the data from each simulation to produce detailed reports and track trends over time.

Whether you are conducting a phishing simulation via email, text message, or live phone call, the first step is to identify the objectives of your simulation.

Objective 1: Malicious Links

Malicious links are often used by cyber attackers to mount various cyber attacks including spamming, credential theft, financial fraud, and malware delivery. The ability to detect when a message or a link is malicious is critical to thwarting these attacks.

Malicious links may be delivered via email, text messages, and phone. Users may even receive a phone call directing them to visit a malicious website. Even a simple action such as clicking on a link is enough to compromise a system with an unpatched zero-day vulnerability.

These scenarios lure users to click on a link. These scenarios may be used in combination with the other objectives listed below.

Objective 2: Data Theft

Data theft is one of the most dangerous threats an organization can face. Depending on the data they collect, cyber criminals can use that stolen information to conduct sophisticated attacks or commit financial theft or fraud.

These scenarios can be used to harvest credentials, credit card numbers, personal information, or any other sensitive information that the cyber criminal can use. The scenario typically lures users to click on a link that directs them to supply data on a web form or a social engineer may request this data over the phone.

Objective 3: Infected Attachment

One of the most common threats to a system is a virus. Viruses are often embedded in files, delivered via email, or downloaded from the internet. Once opened, they can infect a system to corrupt data, steal information, make systems operational, and search for and infect other systems on the network. Users must be cautious and should seldom open attachments from unknown or untrusted sources.

These scenarios attempt to convince users to open an attachment included in the email message or direct them to download it from the internet.

Simulation Results

Consider the following when preparing your analysis and reports:

1. Number and selection of users
2. Groups or filters for granular reporting
3. Objectives and complexity of the simulation

Not all phishing scenarios are created equal, and not all scenarios are relevant to all organizations and all users.

When collecting data from each simulation, consider the following data points in your analysis:

- Messages sent
- Images viewed (number/percentage of users who viewed the images)
- Link clicked
- Information submitted on the website among all recipients
- Information submitted on the website among clickers

- Attachment opened
- Reported phishing
- Filtered by department, role, or another parameter
- Repeat clickers
- Superstars (those who have never clicked)

Although most of the above data points are self-explanatory, let's expand on certain topics that often raise questions and provide a challenge when attempting to interpret them.

Images viewed. Although this behavior poses a relatively low risk of infection or compromise, the act of downloading the images provides to the attacker an indicator that the recipient of the phishing message is valid and was curious enough to consciously download the images. The level of risk may vary depending on whether users automatically download the images when previewing the message or opening the email from a mobile device.

Information submitted on the website among clickers. The latest data shows that if users trust the phishing email message, they are likely to trust the phishing website linked in that message. That is why it is so important to know the percentage of users who submitted their password or other sensitive information on a phishing website. It is even more important to collect the same statistic based on those who clicked. What percentage of clickers failed to recognize the phishing website? Getting this information will help you identify where you need to focus your awareness efforts—on informing your users how to detect a phishing email, a phishing website, or both.

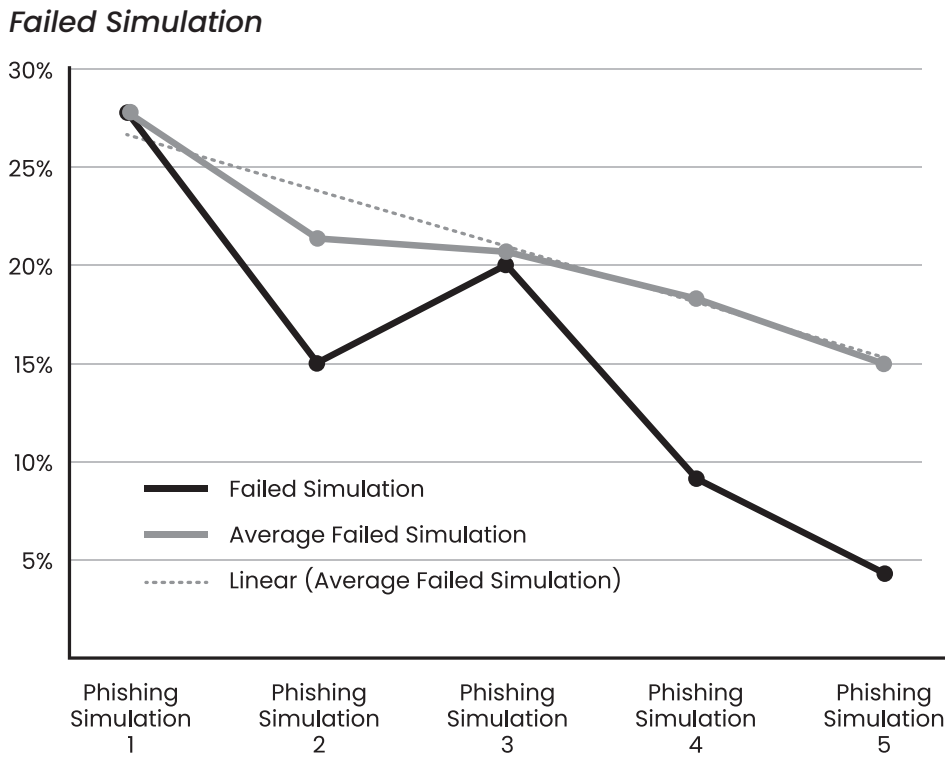
Reported phishing. When looking at data related to users who reported the phishing event, it is important to determine at what stage of the exercise they did the reporting. Was it the moment they saw the email message that their suspicions were raised and took the effort to report the event, or was it after they took an action such as clicking on a link, attachment, or submitting data on the fictitious form? When users report before taking any other action, this indicates a good understanding of phish detection mechanisms. When users report after taking a risky action, this indicates that more training is required to inform them on phish detection mechanisms; but on the positive side, users are not afraid to report when they did something wrong and that the organization is moving toward a positive security culture. Either way, users should be thanked for reporting similar events and encouraged to report, even if after they have done something wrong.

Interpreting Results

Note that the results of each simulation are the results for that specific scenario and do not indicate that these numbers will be the same for all future simulations or even real attacks.

The average of multiple simulations will need to be collected and the trend over time must be monitored for indicators of improvement. For example, see the chart on the following page.

The collection and processing of end user actions during a simulation must be transparent and comply with data protection laws in the organization's jurisdiction or where the users are located. Care must be taken to limit the type of data collected. For example, a scenario luring your users to submit their password should not collect the actual password.



	Compliance	Behavior	Culture
KPI	All employees have received training on the phishing attack method	Reduction in the number of incidents that result from an email attack	Increase in number of employees reporting phishing activity to the Service Desk
Metric	Training participation rates	Recorded malware infections or other incidents from phishing	Reported phishing attacks (e.g., simulations)
Effectiveness Indicator	Increase in the number of users who participate in online training	Reduction in the number of users who opened attachments in real or simulated phishing attempts	Increase in the number of users who reported real or simulated phishing attempts

When communicating the results internally, consider your click rates extremely confidential and secure them accordingly.

The table of the previous page is an example of how you may position metrics around phishing.

3. Participant Satisfaction

Use "satisfaction and content appreciation" surveys or quizzes to gather insights into your participants' perception of the importance of security and the knowledge they have acquired from the training. Consider having an email address dedicated to your security awareness program for employee feedback. This feedback will make it possible to improve the current campaign and upcoming awareness activities.

KPI	Metric	Effectiveness Indicator
Content is easily accessible	Number of users reporting issues accessing the course	Reduction in reported issues
Relevance of campaign to daily activities	Number of users reporting they can apply what they learned	80 percent of users reporting they can apply what they learned
Participant satisfaction	Percentage of overall satisfaction	80 percent of users are satisfied with the content
Training material is efficient	Time is taken to complete the course	Number of participants completing the course in the allotted or desired time
Ensure appropriate degree of difficulty	Number of users reporting the material is too complex or not relevant	Less than 20 percent of users say that material is too challenging or not relevant
Ensure accuracy of the translation, if applicable	Reported translation issues	Reduction in translation mistakes

4. Training Effectiveness

Helpdesk tickets, security incident reports, awareness assessments, and phishing simulations are good starting points for determining program effectiveness and whether employees are applying the desired behaviors.

KPI	Metric	Effectiveness Indicator
Information is handled according to its classification level	Number of data breaches as a result of improper handling	Reduction in the number of data leakage incidents that result from the inappropriate handling of information
Accounts and passwords are protected	Number of business email compromises or business account takeovers	Reduction of stolen account credentials due to insecure user behaviors
Handling and protection of personal information in accordance with privacy principles, laws, and regulations	Number of personal information breaches as a result of improper handling	Reduction in the number of personal data disclosures; reduction in the number of disclosed records
Secure and proper use of corporate internet services	Number of policy violations related to unacceptable use of your organization's internet service	Fewer instances of access to prohibited content/sites
Users are able to detect and know how to respond to phishing attacks	Percentage of users who click on malicious links	Decrease in percentage of users who click in simulations
	Percentage of users who report phishing attempts	Increase in percentage of users who report phishing attempts

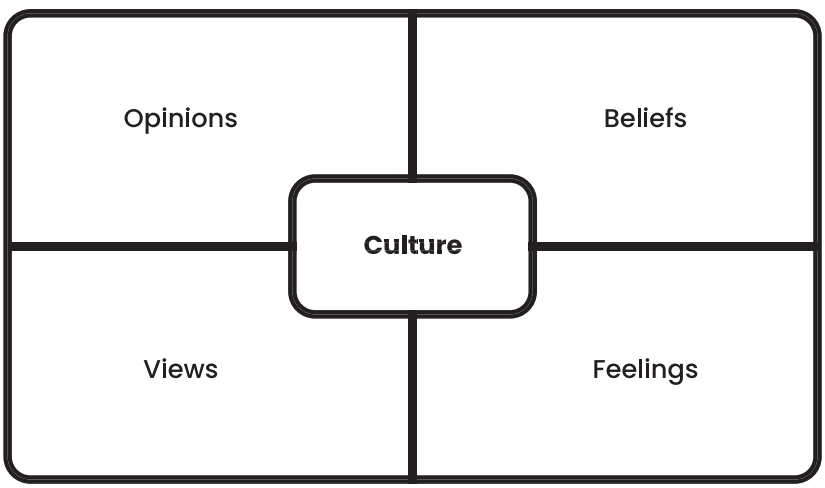
5. Overall Metrics: Security Awareness Index and Security Culture Index

Let's look at security culture. A security-aware organizational culture is one where the cyber security best practices and protecting sensitive

information from cyber threats is always top of mind. We implement an awareness program because we want to create a secure culture. We want to:

- Demonstrate the importance of information security for the organization and the individual
- Leverage managers to become security and awareness ambassadors as every awareness program needs support from the top and a top-down approach
- Change attitudes about security that may have been formed without fact or knowledge
- Help people understand the security implications of their actions or inactions. What is the impact on them, their colleagues, your organization, and your clients?

Culture is about the opinions, beliefs, views, and feelings of individuals or groups about cyber security.



Changing these and measuring this change is difficult and it takes time. But it's important to do because culture change:

- Reduces risk, minimizes incidents
- Saves time and money, boosts productivity
- Ensures compliance
- Promotes employee empowerment, growth

The Security Culture Index

The Security Culture Index available in the Terranova Security Awareness Platform gives organizations the power to go beyond one-dimensional security awareness assessments and assign unique risk-based ratings to employees. Ratings are based on existing security awareness knowledge, access to sensitive information, role requirements, and other crucial data points specific to the individual.

By combining tailored risk scoring with automated risk-based campaigns, organizations can:

- Quickly identify risk levels based on role, function, region, and more
- Confidently reduce human risk through actionable behavior change
- Build a cyber-aware organizational culture across all departments and teams

The two elements of this Index are the Security Awareness Index and the risk level.

In the first step, we need to understand the current and desired level of awareness, what we call the Security Awareness Index. This will be determined based on activities completed, the progress, the results, and information gathered on the simulation performance. Other inputs include quizzes and surveys that will allow you to evaluate individuals' current level of knowledge of best practices, their ability to recognize cyber threats, and their likely reaction when facing a situation that requires proper security measures. The question you are answering is this: Do users know what the best practices are and are they motivated to apply them?

An individual's Security Culture Index draws from multiple factors to facilitate the creation of risk-based campaigns that respond and adapt to changes in behavior.

These data points include a person's:

- Role and function within the organization
- Access permissions to sensitive information
- Number of emails received on a daily or weekly basis
- Involvement in or proximity to previous data breaches

- Awareness training course participation and completion
- Phishing simulation results
- Behavior change performance over time

Later when you define the risk level for each audience, you will be able to define the learning path users can take to achieve the desired level of Security Culture Index. The risk level will be based on the role of the user, their work environment, the type of data they have access to, and other elements that cannot be influenced via awareness.

We want to use data-driven insights that are unique to each employee. These elements will allow you to measure culture change over time and be ready to join the forefront of targeted risk-based security awareness training.

You know your program is working when your security awareness program influences motivation (participants want to learn and apply what they've learned). You will also notice that your course completion rates increase steadily over time, with less effort chasing users to complete activities or escalating for noncompliance.

Ultimately, you will see a rise in best practice adoption and more users will report suspicious messages and inform their colleagues. Doing the right thing will become second nature.

6. ROI

The metrics related to ROI are straightforward.

You'll notice that when you record a reduction in password reset tickets, lost or stolen devices, fraud-related costs, and downtime incidents caused by risky behaviors, your ROI increases. In other words, your security awareness campaign starts to pay for itself.

This happens because the financial impact of a security compromise is far reaching and results in staggering costs that may not be immediately apparent:

- Time spent by the service desk or security operations to resolve the problem
- Time required to recover from an infected computer after a malware infection, and the time spent by IT to repair and recover the computer
- Time required to recover an infected server
- Productivity impact and revenue loss if a critical server is infected
- Time required to restore an encrypted file share
- Tarnished reputation and decrease in client confidence

A security awareness program will not reduce the costs associated with an incident, but it will significantly reduce the likelihood of an occurrence and make future detection faster. As an interesting exercise, review your budget and cost estimates. Then investigate the costs associated with a typical security incident at your organization. Inquire as to how many occur annually and make a comparison.

This is an excellent exercise to do when presenting the results of your program to decision makers and senior management.

7. Subjective Indicators

Some of the top indicators that risky behavior is decreasing are not objective statistics; they are much more subjective, so you should also be observant of the following:

KPI	Metric	Effectiveness Indicator
Create a security-aware culture	Office "chatter" about aspects of the security awareness program	An indicator that enthusiasm and excitement are spreading
Create interest in information security	Champions start to surface within different workgroups	An indicator that awareness sponsorship and leadership is crystallizing
Encourage users to inquire and discuss information security	Informal discussions are occurring about topics within the security awareness program	An indicator of curiosity and awareness about the topic is becoming a "state of mind"
The tone at the top supports security awareness	Funding for security awareness programs is much easier to obtain	Executives request updates and reports on the performance of the security awareness program

Tracking Progress

As you gather and analyze your metrics data, keep the following in mind:

- Track metrics and KPIs before program/campaign deployment to set a baseline against which future results will be compared. For example, use a phishing simulation or quiz to establish a baseline.

- Monitor participation rates as soon as you launch the online training and on an ongoing basis to track progress and trends. This will allow you to gauge whether you are on track to meet your objectives. If not on track, you will be able to take corrective actions.

Document Your Metrics

Type of metric based on the previous categories:

- Associated KPIs
- Objective of the KPI
- Data source
- Responsible for producing data
- Audience
- Reporting frequency
- Targets
- Indicators
- Dashboard location and format
- Trends and presentation breakdown (e.g., by department, by region, by role)
- Positive performance actions
- Negative performance actions

Reporting

There are several benefits of proper and timely reporting. It allows you to:

Improve Communication

An effective reporting mechanism will allow you to communicate information about your program's performance at all levels of your organization. Keep in mind that the details you are providing in the report must be appropriate for your audience—the higher the audience level, the more macro the report must be. For example:

- Senior management: program progression and success stories
- Department heads: participation rates and department progress
- Participants:
  - Observed best behaviors and campaign success
  - Winners of prize drawings or contests to highlight users who demonstrated good behaviors and prevented an incident
  - Statistics on campaign participation to show that the whole organization is committed to information security
  - Gamification and leaderboards to promote healthy competition. This allows the user to evaluate himself in comparison with peers or the whole organization.

Improve Efficiency

The staff responsible for managing your security awareness program will be able to respond quickly to events and requests from the participants and to oversee the program more efficiently:

- To diagnose technical issues
- To allow for targeted follow-ups and reminders
- To link events and observed behaviors to internal policies and training

Increase Value

The success of any planning, forecasting, and budgeting you do to implement and manage your programs largely depends on accurate and complete data. These include:

- Areas of vulnerability to determine priorities
- Content appreciation by the audience
- Resource allocation requirements

Demonstrate Compliance

Use metrics to demonstrate proper communication of internal policies and procedures. Examples include:

- Compliance requirements by auditors
- Compliance requirements by regulatory agencies
- Benchmarking and comparison with industry peers

Validate Your Program

Share reports and results with decision makers who are key to your security awareness program. They would be especially interested in your ROI report.

Report

Metrics begin life as raw data that must ultimately be analyzed, interpreted, and presented in a simple and visually appealing format that helps ensure the information is quickly processed and understood—a report. Remember that a picture is worth a thousand words, so include graphics in your reports whenever possible.

Consider granting managers access to reports or a dashboard so they can be directly involved in the program and intervene earlier if additional user support and encouragement is required. Opening up managers' access to their department's performance will increase participation and will engage all levels of the organization in the success of your program.

When preparing your reports, consider the following:

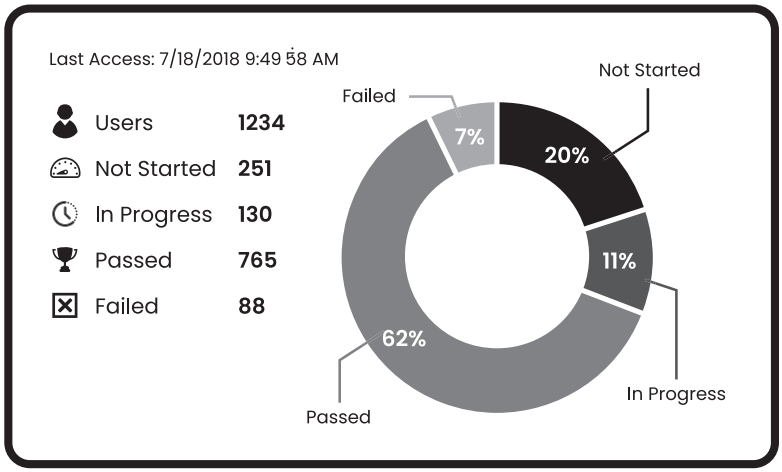
- Why is this report relevant to the viewer?
- Is the information organized in a format that provides value?
- Can the data in the report be cross-referenced with data from other sources to identify trends or symptoms (e.g., if there is a SIEM, merge campaign data with other data)?
- Are any decisions to be made based on unfavorable or favorable results?
- Do you have any recommendations for improvements based on the reported metrics?

Report examples:

- Phishing Summary Report over Time
- Phishing Results by Template Difficulty
- Course Results by Topic
- Course Completion Status versus Phishing Results
- Knowledge Quiz
- Behavior Quiz
- Culture Quiz
- Quiz Completion over Time
- User Scorecard
- User Scorecard by Filter

Tip: Present your findings in a concise, targeted, and well-organized report.

Report Data Example



Overview Dashboard

Course Dashboard

Simulation Dashboard

Quiz Dashboard

User Dashboard

Including a variety of dashboards and widgets can greatly increase the visibility of program performance and allow security leaders to quickly report and adjust their program to meet desired objectives.

Reporting Examples

Example—Report 1

Title: Security Awareness Program Participation by Department
Audience: Department leads/security awareness program manager/auditors and regulators
Source: Participation in current campaign by department, as reported in the LMS
Data: Number or percentage of users and their status (not started/in progress/passed)
Frequency: Every two weeks during a campaign and yearly afterward
Format: Reports delivered via email or accessible via LMS dashboards
Decision: If participation is not at the expected levels, the department lead or program manager must issue a reminder. This report can also demonstrate employee participation in security awareness activities to auditors and regulators.

Example—Report 2

Title: Security Awareness Campaign Online Training Feedback
Audience: Security awareness program manager
Source: Employee satisfaction survey
Data: Percentage of users reporting satisfaction with the relevance of online awareness training to their jobs
Frequency: After the first campaign and ideally after each campaign

Format: PowerPoint presentation, survey results analysis

Decision: According to feedback received, adjust the content, format, length, or target audience for the training. Feedback should be gathered early in a program to allow for timely adjustments before the launch of subsequent campaigns.

Example—Report 3

Title: User-Reported Incidents

Audience: Security awareness program manager

Source: Helpdesk incident data/information security incident data/evaluation quiz

Data: Number and type of incidents affecting users (e.g., vectors of virus infection, social engineering victims, policy violations, stolen devices, password misuse, etc.), areas of user vulnerability

Frequency: Monthly/yearly

Format: PowerPoint presentation, event dashboard

Decision: If you can't obtain this data quickly within the organization, public reports from researchers and security service providers can identify how most security breaches occur. Use this data to tailor content based on the most common vulnerabilities and prioritize topics based on the frequency and the potential impact of harmful events.

Example—Report 4

Title: User Dashboard

Audience: End users

Source: LMS

Data: Number and type of activities completed, results of learning activities, games, simulations, quizzes, Security Awareness and Culture Index, peer benchmarking

Frequency: Dynamic

Format: Online dashboard

Decision: When users can track their performance, they will be motivated to participate, complete more activities, and learn.

CONGRATULATIONS!

You have just completed Step 4 of the Terranova Security Awareness 5-Step Framework—Measure.

Taking the time to assess the performance of your security awareness activities provides valuable information you can use to make improvements to your program. It also allows you to illustrate to decision makers the effectiveness of your security awareness initiatives.

Summary of Measure Actions

- Define and gather data
- Track progress
- Report

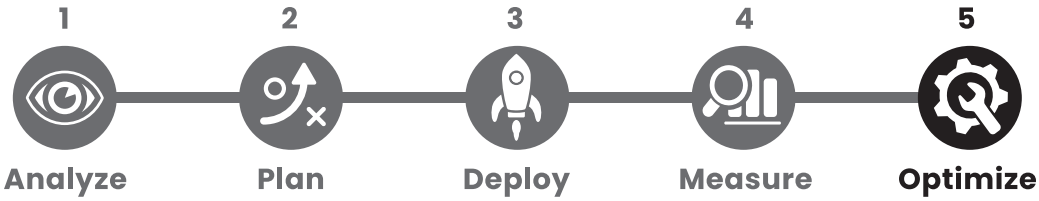
Ready for Step 5—Optimize? Let's do it!

INSANITY: DOING THE SAME THING OVER AND OVER AGAIN AND EXPECTING DIFFERENT RESULTS.

—ALBERT EINSTEIN

FIVE

STEP 5: OPTIMIZE



Welcome to Step 5 of the Terranova Security Awareness 5-Step Framework—Optimize.

This is the fifth and final step of the Terranova Security Awareness 5-Step Framework. In Step 4—Measure, I touched briefly on monitoring your campaign or program performance by gathering and analyzing data so that you can identify areas for improvement and start developing an optimization plan.

It is essential to act on your findings. Keep updating and improving your security awareness program and campaigns to meet your objectives and keep security top of mind across your organization over the long term.

You want to instill a culture of security.

The most significant benefits of gathering and analyzing data are that you can now identify areas for improvement and develop an action plan to address them.

For a given campaign, you may need to take action to meet your goals and objectives if they are not completed. For example, if participation is low, you could review your communication strategy and send out a more engaging reminder, perhaps using a different medium than you did previously.

For your overall program, we recommend reviewing and updating (as needed) your program goals, campaign objectives, priorities, and strategies after each deployment. That way, you can decide if the lessons learned can be applied to subsequent campaigns. For example, while reviewing your roadmap, you may realize that changing priorities and scheduling future campaigns is necessary.

In Step 5, we will explore these five steps:

- Analyze your resulting metrics from Step 4—Measure
  - Investigate statistics, interpret data, validate assumptions, and take necessary corrective measures.

- Compare your results with your campaign objectives and program goals
  - Assess the current situation and gaps in your security awareness program.

    - Compare with peers in your industry or their priorities and approach.

- Identify improvement opportunities
    - Optimize your campaigns based on your KPIs and metrics.

- Identify new objectives
    - Determine changes in training and behavioral objectives for a follow-up campaign.

- Conduct a postmortem meeting
    - Once you have gathered and compiled your observations and the gaps you discovered, you need to share your learnings with your security awareness team to identify areas for improvement.

Tip: If you decide to make extensive changes in order to optimize your program, consider going back to Step 1—Analyze and Step 2—Plan to see how your program and campaigns should be reviewed.

Analyze Your Resulting Metrics

Time to crunch some numbers! This is the moment when you roll up your sleeves to review your metrics and interpret your results. By completing this process, you will learn where your campaign is vital and where it is weak so you can zero in on the suitable corrective measures and optimize your program.

Optimizing your security awareness program is an ongoing process, a part of your long-term strategy. Each campaign will take you a little further along the learning curve, revealing new insights that will allow you to build an even more vigorous campaign the next time.

Focus your efforts and resources on activities aligned with your goals and objectives. Work with the KPIs and metrics you defined in Step 2—Plan and collected in Step 4—Measure.

Compare Your Results with Your Campaign Objectives and Program Goals

This part of the process takes several steps and time to analyze results.

First, you must review your program goals and campaign objectives identified in Step 1—Analyze.

Divide your awareness goals into three categories:

- Risks and behaviors
  - To reduce risk and foster behavioral change
- Security culture
  - To instill or reinforce a culture of security
- Compliance obligations
  - To ensure compliance with your organization's security or regulatory obligations

Then compare your objectives to the results of your actual campaign.

Assess the current situation and identify any gaps in your security awareness program. Your team can compare your objectives with the results after each campaign or yearly. After a significant activity,

schedule some time with key players on your security awareness team to do this review.

To compare your objectives with results, first list the program goals you identified in Step 1—Analyze under these related categories: risks and behaviors, security culture, and compliance obligations.

Next, transcribe the campaign objectives that you identified in Step 2—Plan onto the first column. Make a note of the results in the second column, and then identify any deficiencies or shortcomings in the third column.

Identify Improvement Opportunities

Once your campaign is underway, you may encounter any number of issues. Remember, your security awareness program is not a project; it is ongoing. Every issue arising is an opportunity to improve your overall program and fine-tune your upcoming campaigns.

After helping thousands of clients build and deploy their security awareness programs worldwide, we have observed that the issues that create improvement opportunities fall into three specific categories.

Improvement opportunities:

- Overproduction
- Technical issues
- Logistical issues

Overproduction—Too Much Is Too Much

Sometimes less is better. Avoid information overload caused by bombarding end users with:

- Online training modules that are too long and time consuming
- Content that is irrelevant to them or their job function

In your platform, note the time it takes participants to complete the different modules. Are they starting but not finishing them? If this is the case, compare them to the lengths recommended in Step 2—Plan and make sure you have selected the right content for each of your target audiences.

Keep this issue in mind when planning your subsequent campaign and focus more on content selection. Then, the next time you deploy a campaign, monitor your training metrics and measure any improvements—the result: higher participation rates and, by extension, more tremendous success which will be demonstrated via your phishing simulation and quiz results.

Technical Issues: Troubleshooting after the Fact

In the prelaunch phase of Step 3—Deploy, I described the need for prelaunch testing, including running a pilot test. Suppose there are technical issues while your campaign is already underway. In that case, the downtime you experience while your IT department is working out the bugs will throw your program off course, create delays, and interfere with your success.

Some of the common technical issues may include:

- Content not appropriately displayed on target form factors (e.g., tablets, laptops, smartphones, etc.), making it impossible to complete a module
- Difficult access and a complicated platform authentication process cause users to abandon training

- Bandwidth issues slowing down the content or disrupting the audio of the training
- Blocked pop-ups, if they are required for the training to run correctly
- Incompatible browser security settings
- Accessibility issues for users with impairments

Should a technical issue arise during a campaign, alert the assigned support team members to resolve it as quickly as possible. Then revisit your Compatibility and Performance Testing worksheet from Step 3—Deploy to ensure that you include more testing and troubleshooting in your next campaign and that you schedule this testing well before your launch date.

Logistical Issues: Keeping the Plates Spinning

Keeping all the plates spinning when running a security awareness program is not an easy feat, especially if your security awareness team members have other responsibilities or work in a different department.

An oversight like failing to send out the login credentials for a new module is a human error that can bring your campaign to a complete standstill.

Whatever the circumstances, you have to keep your security awareness team members in the loop at all times, giving them clearly defined tasks with expected delivery dates. You also have to follow up to ensure they are ready for action on deployment day (see Step 3—Deploy).

Logistical challenges take many forms. Ask yourself what you would do if:

- Your organization is holding an important event that requires extensive coordination, and your training gets pushed to the bottom of the list of priorities?
- It's peak season at your organization, and everyone is focused on meeting your client's expectations, not on your campaign?
- You discover you did not set realistic timelines for developing and delivering the communication material?

All of these situations are logistical nightmares, but the important takeaway is this: How you deal with these situations now and how you prevent them from happening in the future directly impacts your ongoing success.

Instead, what if you approached it from a different angle—reframing problems as opportunities to do it differently next time—by asking yourself these questions:

- Did this happen because a security awareness team member dropped the ball?
- Was it a scheduling issue? Was I realistic?
- When creating my campaign calendar in Step 2—Plan, did I consider everything? Did I overlook something that I now see?

For your next campaign, you may want to speak with your security awareness team members and their managers to confirm their commitment and consider making necessary changes.

Finally, you must be more realistic and thorough when creating your communication calendar (see Step 2—Plan). Use your updated checklist to keep track of everything required to succeed in your campaign.

Being realistic about logistics means coming to terms with this truth: running an effective security awareness program requires all hands on deck. So, what if the issue is that your organization cannot provide you with the team members you need in-house?

To determine if this is the case, verify that all your scheduled activities were deployed and completed on time. If there were any issues, investigate further to see if they occurred because you do not have sufficient in-house resources to manage your awareness activities. If so, you may want to hire an outside source to help out.

Taking the helm of a security awareness program you didn't design requires strong project management skills. Many organizations opt to retain the services of a permanent or temporary outside resource dedicated exclusively to their security awareness program, depending on its magnitude and the effort required to oversee it.

Identify New Objectives—Updating Your Program

In addition to applying all of your lessons learned, you need to revisit the goals and objectives you identified in Steps 1 and 2 to see if they have changed at all and then adjust them accordingly.

Factors of Change

Remember that refining your security awareness program is an ongoing process, and you must therefore consider several factors to identify any new security objectives for your campaign:

- Compliance
- Evolving risk landscape
- Action plan
- Industry benchmarks

Compliance

Changing your organization's mission, key operational activities, geographical location, or implementing a new regulation may affect your compliance ecosystem. Ensure you are up to date on all contractual and regulatory compliance obligations affecting your organization. If any new compliance obligations have been put in place since you first completed Step 1—Analyze, go back and update your goals.

Evolving Risk Landscape

As we have discussed throughout this book, the cyber security threat landscape is changing daily, so you may have to develop an entirely new security awareness campaign. You have to be alert to all the latest morphing and mutations of malware, cyber scams, and social engineering so that you include the latest, most potent training modules and phishing templates in your program.

Another factor that affects your risk posture is a change in your organization's critical operational activities or the implementation of new business processes or technologies. Consult your IT, HR, security, finance, administration, and other relevant departments to discover if they have introduced any new systems that cyber attacks may target.

Action Plan

An action plan is a list of work priorities you draft concerning your program and its requirements, with the essential items at the top so your team knows what to deliver first. Establish priorities with your teams and ensure everyone shares the same mindset about the program.

Once you draft the action plan, it is important to maintain and update it on an ongoing basis to keep pace with the program. It will almost certainly evolve over time; be prepared for your organization's

decision makers to challenge priorities, compelling you to make adjustments as you go.

Industry Benchmarks

Accurate comparative data is not always readily available to an organization due to differences in size, sophistication, and business sector. Therefore, many organizations rely on industry or trade association reports to gather best practices data. Other sources include conferences, magazines, and the internet. These sources may shed light on new trends, updated statistics, or new breeds of cyber crime.

You need to be agile and responsive when you discover new industry information that could affect your organization. Change your programs to make your people aware of new threats so they can help you fend off the latest type of cyber attack.

Conducting Your Postmortem Meeting

Bring your security awareness team together after a campaign or on a yearly basis to compare notes and brainstorm fresh ideas.

Everyone has had a different experience developing and delivering your program and campaigns. They all have suggestions that will take your program to the next level of effectiveness. Sharing insights into what worked and didn't work with your security awareness team is a powerful exercise.

Postmortem Meeting Tips

- After a major activity, schedule a meeting with key players to discuss what worked and what went wrong.

- Make a whiteboard available to capture comments; it is easier to decide on priorities when everyone is looking at the same list. Take photos of the whiteboard entries to record what was said so you can document it after the meeting. Record what you have learned to ensure it is not lost or forgotten and that errors don't happen again.

- Pick the top three items to address as your priorities rather than trying to resolve all the issues simultaneously. You can always schedule additional postmortem meetings to work through the remaining issues.

Your Optimization Plan for Continuous Improvement

The whole purpose of leveraging the Terranova Security Awareness 5-Step Framework is to produce more effective results—to succeed in the adoption of protective security behaviors among your audiences. The key to accomplishing this is to keep improving and upgrading your program by bringing together your security awareness team to assess the success of your activities and plan your next steps.

Review Feedback

Before the postmortem meeting, send out a survey to all team members, support staff, champions, sponsors, SMEs, and critical clients so that you have a preview of their perceptions and thoughts about your program.

You should also review any direct feedback and comments sent to your security awareness team during the campaign from the participants.

Identify Best Practices and Lessons Learned

Based on your metrics developed in Step 4—Measure, prepare a handout for your meeting that outlines what worked well and areas where you can make improvements in terms of:

- Program management, including content
- Budgeting and procurement
- Time management and scheduling
- Management of finances, human resources, marketing and change management, as well as legal and external contractors

Select Priorities

When you and your security awareness team meet, plan and prioritize your upcoming improvement activities. Think of ways to optimize your program to achieve better results with each wave. Your optimization plan should specify:

- Optimization priority
- Current organizational situation/context
- Recommended initiatives
- Expected benefits of the optimization initiative
- Expected completion date

Assign Responsibility

Identify which department is responsible for delivering the selected optimization activities and allocate the appropriate resources (i.e.,

budget and staff). Remember to report all findings and plans to your security awareness program sponsor.

Conduct a Follow-up

Once all the optimization activities have been assigned and delivery dates set, incorporate them into your program schedule and update your security awareness team. Allocate time in your schedule for follow-up and collecting progress reports from those responsible.

EXERCISE

EVALUATING YOUR SECURITY AWARENESS PROGRAM

When evaluating your security awareness program, you must answer these most important questions:

- Did your security awareness program meet your strategic goals and campaign objectives?
- Did it change the risk behaviors that could compromise your organization's security?
- Did it improve the overall company security culture?
- Did the general risk level of departments or users increase or decrease?
- Did the overall Security Awareness Index of departments or users increase or decrease?
- Did the overall Security Culture Index of the organization, departments, or users increase or decrease?

Use the evaluation questions below to guide the type of questions your security awareness team should answer individually or in a postmortem focus group discussion.

Process Evaluation

- Did the program target the right audiences with suitable topics?
- Do you need to consider adding another target audience?
- Did the program take into consideration the needs of all target audiences?
- Did the target audiences react favorably to the program? Which communication channels worked best?
- Which communication channels did not work and why?
- Do you need to consider different methods for delivering your messages?
- Were you able to deploy all your planned security awareness activities and communications in time?

Outcome Evaluation

- Were any assumptions made at the start of the program incorrect? Refer to your Analyze Cheat Sheet.
- Were any actions taken to compensate for unforeseen events?
- Were any workarounds developed to compensate for technical issues?
- Were your security awareness program goals met?
- Did any of the awareness team members receive direct feedback on the program?
- Were the campaign activities beneficial to the target audiences?
- To what extent can behavior changes be attributed to your security awareness program?
- Which activities in the program made a positive difference in participant behaviors?
- Did any activities in the program have any adverse effects?

- Is your security awareness program aligned with your organization's current policies?
- What else can you do to improve your security awareness program?

Resources Evaluation

- Does everyone on the security awareness team understand their roles and responsibilities?
- Does your security awareness program team need any additional resources?
- Are the costs of the program's activities reasonable in relation to the benefits?
- Does your security awareness program have the required budget to continue its activities?

EXERCISE

OPTIMIZATION PLAN

When you conduct your postmortem with your team, come to a consensus on the top three optimization priorities you want to implement to optimize the program's level of success.

For each of the priorities you identify, answer the following questions and document you responses and plans:

- What will be optimized?
- Why? Describe the current situation at your organization that made you decide on this optimization priority.
- What are the expected benefits of this optimization initiative?
- How? What are the recommended steps to address this optimization priority?
- Who is assigned to work on this optimization initiative? Completion date?

CONGRATULATIONS!

You have completed Step 5 of the Terranova Security Awareness 5-Step Framework—Optimize.

You have now created a cycle of ongoing optimization. Keep aiming higher. Probe your findings and look for ways to use what you have learned to enhance your campaigns so that cyber security stays top of mind across your organization over the long term!

Summary of Optimized Actions

1. Analyze your resulting metrics.
2. Compare objectives with results.
3. Identify areas for improvement.
4. Identify new objectives.
5. Conduct a postmortem.

This is the fifth and final step in the Terranova Security Awareness 5-Step Framework.

In writing this book, I aim to empower you with the knowledge you need to implement a security awareness program that addresses and changes human risk behaviors in your organization. I hope I was successful.

Ready to get to work on masterminding your security awareness program?

Remember, the experts on my Terranova Security Awareness Team are happy to support you and help ensure your success.

Let's do it!

CONCLUSION

I've dedicated the last two decades of my career to training, IT, and security awareness, and I feel a great sense of responsibility to share what my team and I have learned to help you design and deploy a successful security awareness program. When I say "successful," I specifically mean one that creates behavioral change, dramatically reduces the likelihood of a breach at your organization, and instills a security culture.

This book is your go-to manual for masterminding your organization's ideal security awareness program. Beyond that, it's also a call to action. You might even say it is a call to arms, urging you to implement a security awareness program that effectively confronts the surging levels of cyber attacks aimed at organizations like yours.

Having a cyber security awareness policy has never been more crucial. Recent years have completely flipped the script on cyber security awareness training. The global move to remote work introduced new challenges and forced cyber security professionals to update many of their practices. Cyber criminals have and will continue to capitalize on this period of uncertainty to steal your data.

Today, it is not enough to rely on security technology or maintain a "tick the box" mentality and merely go through the motions to say,

"security awareness training completed." We need to employ a human fix to address the human risk factors.

As you know, cyber criminals target the people at your organization with phishing scams, social engineering, and other cyber threats to gain access to sensitive information. In response, you have to engage the people at your organization with the proper security awareness training that is relevant, interactive, engaging, ongoing, and repetitive to change their risky behaviors and keep information security top of mind. You have to provide them with the knowledge they need to become your human firewall and help you fight the cyber war.

Therefore, it is incumbent on us to teach them to detect the threats, not just the same day, week, or month of their training—but over the long term so all of the sensitive information your company handles and produces stays protected.

One breach is one too many. Your users are the first line of defense. They need to be accountable as active participants to protect their organization and themselves against cyber crime.

To keep cyber threats at bay, you have to be proactive and strategic. You have to mastermind a plan customized to your organization's specific realities and needs. A one-size-fits-all approach cannot effectively reduce human risk. This book provides a starting point and a proven methodology for masterminding a security awareness program that will drastically minimize risky behavior from your ranks and create a security culture in your organization.

My team and I have drawn on our vast expertise in professional training, behavioral change, IT, and security awareness to develop the Terranova Security Awareness 5-Step Framework. It is an innovative, robust, and highly effective process that has helped thousands of companies implement effective security awareness programs worldwide.

Time after time, we have seen organizations implement security awareness initiatives that do not adequately reduce the risk of security breaches. There are different reasons why this happens. For example, they:

- View security awareness as a project, not as an ongoing process
- Start at the deploy phase, releasing online courses and/or videos without proper analysis and planning
- Only want to check the box of compliance
- Don't set goals and objectives for the program and campaigns
- Don't establish KPIs or measure results
- Don't make the campaigns exciting and interactive for participants
- Don't customize content to reflect the reality of the organization or audience

The Terranova Security Awareness 5-Step Framework addresses all of these shortcomings based on five essential steps that give you greater assurance that your security awareness program will be successful:

- **Step 1—Analyze**
- **Step 2—Plan**
- **Step 3—Deploy**
- **Step 4—Measure**
- **Step 5—Optimize**

Tip: Without a framework, it's just trial and error—you are leaving it to chance.

While my team and I were planning and writing this book, we focused on some key points that I want to highlight here for you. When

you deploy your security awareness program, you must consider the many factors directly impacting how readily people absorb and retain information.

Specifically, for your security awareness program to be effective, it has to be:

- Relevant to the people taking the training and their function
- Engaging, interactive, and fun
- Delivered in segments that are not too long. Snackable content is most effective
- Tailored to their learning capacity and motivation level
- Ongoing, repetitive, and reinforced
- Individualized for each user based on their role in the organization, their risk level, and Security Awareness and Culture Index

Moving Forward

As you work with this book, I hope you begin to identify what makes your organization and its security awareness needs different from any other organization. More importantly, I hope you get a clearer view of the path you need to take, everything you need to consider, the tasks and activities you need to complete, and the resources you need to secure to design and deploy the ultimate security awareness program. I want you to create a program that will make you proud. A program that reduces risk and increases certain behaviors among the people at your organization. Create a real security culture!

ACKNOWLEDGMENTS

To say that this book is "by Lise Lapointe" is an overstatement. I would never have been able to bring this project to life without the incredible contribution of my team.

I have so many people to thank. At the top of the list are the CISOs who developed and evolved the Terranova Security Awareness 5-Step Framework and methodology over the past years. They have shown such commitment to helping me grow Terranova Security and help our clients build successful security awareness programs.

I want to take this opportunity to personally thank each member of the Raising Security Awareness team for their dedication, contribution, and support:

- Theo Zafirakos, CISO
- Jamal Elachqar, CINO
- Anick Charland, CISO
- Client advisory board members

ABOUT THE AUTHOR

Lise Lapointe is a visionary entrepreneur who has dedicated the last two decades of her career to cyber security awareness. Her company, Terranova Security, has been delivering industry-leading security awareness training for more than twenty years. By supporting and working with security leaders globally, Lise spearheaded the development of personalized security awareness programs that change end user behavior and grow security-aware organizational cultures worldwide.

Lise and her team first published *The Human Fix to Human Risk: 5 Steps to Masterminding an Effective Security Awareness Program*™ as a way to share lessons from her experience in cyber security and help organizations secure their sensitive information through a people-centric approach to learning. Security leaders agree that a personalized approach that takes into consideration the objectives of the organization, the maturity level in security of its users, the role of the employee, and language will deliver the greatest results by drastically reducing the human risk factor.

Making her home in Laval, Quebec, Canada, Lise was named one of Canada's Top 20 Women in Cyber Security by IT World Canada. In

2021, she was a recipient of Canada's Most Powerful Women: Top 100 in the BMO Entrepreneurs category, recognizing women who own and operate thriving businesses.