THE HUMAN FIX TO HUMAN RISK™

5-steps to masterminding an effective security awareness program™

Lise Lapointe

& the Dedicated Terranova Cyber Security Savvy Team

THE HUMAN FIX TO HUMAN RISK™

The Human Fix to Human Risk
5 Steps to Masterminding an Effective Security Awareness Program™

Published by Terranova Worldwide Corporation Inc., Quebec, Canada
www.terranovacorporation.com

Printed in Canada by Mardigrafe

Legal deposit
Bibliothèque nationale du Québec – 2018
National Library of Canada – 2018

ISBN 978-1-9994206-0-4

THE HUMAN FIX TO HUMAN RISK™

5 steps to masterminding an effective security awareness program™

Lise Lapointe
& the Dedicated Terranova Cyber Security Savvy Team

TERRANOVA WORLDWIDE CORPORATION

TABLE OF CONTENTS

This book is dedicated to my team, for whom I have such a deep appreciation, as well as to Jamal, Stéphanie and Mathieu for their contribution and their unconditional support for more than a decade in helping make Terranova a global company.

ACKNOWLEDGEMENTS

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 worked to develop and evolve the ***Terranova Security Awareness 5-Step Framework*** and methodology over the past five years. They have shown such commitment—to help me grow Terranova, and to help our clients build successful security awareness campaigns.

I would like to take this opportunity to personally thank each member of the Raising Security Awareness team for their dedication, contribution and support:

- Anick Charland, CISO
- Theo Zafirakos, CISO
- Mathieu Joel Gervais, Ph.D. Change Management
- Laraine A. Weglarz, CISO

I would also like to thank the members of our Client Advisory Board for their invaluable feedback.

Lise Lapointe

FOREWORD

Those of us who are CISOs and have been conducting awareness programs for years realize that “the devil is in the details” when building a successful program. Our initial attempts on getting an awareness program started are usually done by trial and error. That hit-and-miss approach is often ineffective or frustrating, making funding for new programs hard to get.

I am very impressed by the new ***Terranova Security Awareness 5-Step Framework*** for effectively raising security awareness. It walks you through every detail you need to consider in order to plan and deliver a successful awareness program with checklists, templates and other takeaways to simplify your efforts. Built on five essential steps (Analyse, Plan, Deploy, Measure and Optimize), the framework incorporates several tried-and-true techniques for changing human behavior—the ultimate goal of any security awareness program.

A successful security awareness program must be well-defined and have measurable objectives, a strong knowledge of your target audiences, and topics that are chosen based on assessments of your organization’s risks. Everything in your program feeds from those foundational points. By following the recommendations in ***Terranova Security Awareness 5-Step Framework,*** you’ll accomplish those key success factors and produce a security awareness program with measurable impact. Most importantly, your organization, clients and customers will be better protected.

Laraine A. Weglarz, CISSP
Former CISO of a €15 Billion
multinational conglomerate

The only mistake in life is the lesson not learned.

— Albert Einstein

PREFACE

> Training is my passion and so is information technology, for that matter. Why?
> Because training is such a positive thing—it creates real change in people's everyday lives.
> Plus, technology keeps evolving, and that's what makes the field so interesting.

I am very honored that you have decided to read my book, ***The Human Fix to Human Risk. 5 steps to masterminding an effective security awareness program***.™

It means you are probably concerned about the staggering proliferation of cyberattacks that prey on human weakness. It also means you know that your strongest line of defense is your people—people who are well trained in security awareness, people who are always alert to social engineering, phishing scams and all the other evolving cyber threats. Most importantly, it means you want to make security awareness training a priority at your organization in order to reduce the human risk factors that could compromise your information security.

In this book, my team and I show you how to ***mastermind*** your own security awareness program with our easy-to-follow ***Terranova Security Awareness 5-Step Framework***. Working in the ***security awareness*** industry for close to ***two decades***, we share our lessons learned from helping clients all over the world design and deliver thousands of successful security awareness programs to millions of users.

We guide you through the entire process, outlining everything you need to consider and do to create a security awareness program that is adapted to the needs of your organization—a program that effectively raises security awareness and keeps best practices top of mind across your organization ***by changing human behavior***.

At Terranova, we are a team of passionate people who take a very human approach to security awareness. What is cybercrime after all? It is humans (cyber criminals) targeting humans (the people at your organization, as well as you and me) in order to access sensitive information such as personal information, intellectual property, proprietary information and other assets. The best way to fix this situation and fend off attacks is to change the risk behavior of those being targeted within your organization.

Once you figure out how to change behaviors, you can create an organizational culture of security awareness, which ultimately results in dramatically fewer human-related security incidents.

Whether you are an experienced security professional or completely new to the field, I hope you enjoy reading ***The Human Fix to Human Risk*** and that you discover new, valuable information, insights and strategies that you can apply to your information security program.

WHEN YOU IMPLEMENT THE RIGHT SECURITY AWARENESS PROGRAM FOR YOUR ORGANIZATION…

YOUR PEOPLE BECOME AWARE OF SECURITY BEST PRACTICES

↓

YOUR PEOPLE ADOPT DESIRED SECURITY BEHAVIORS

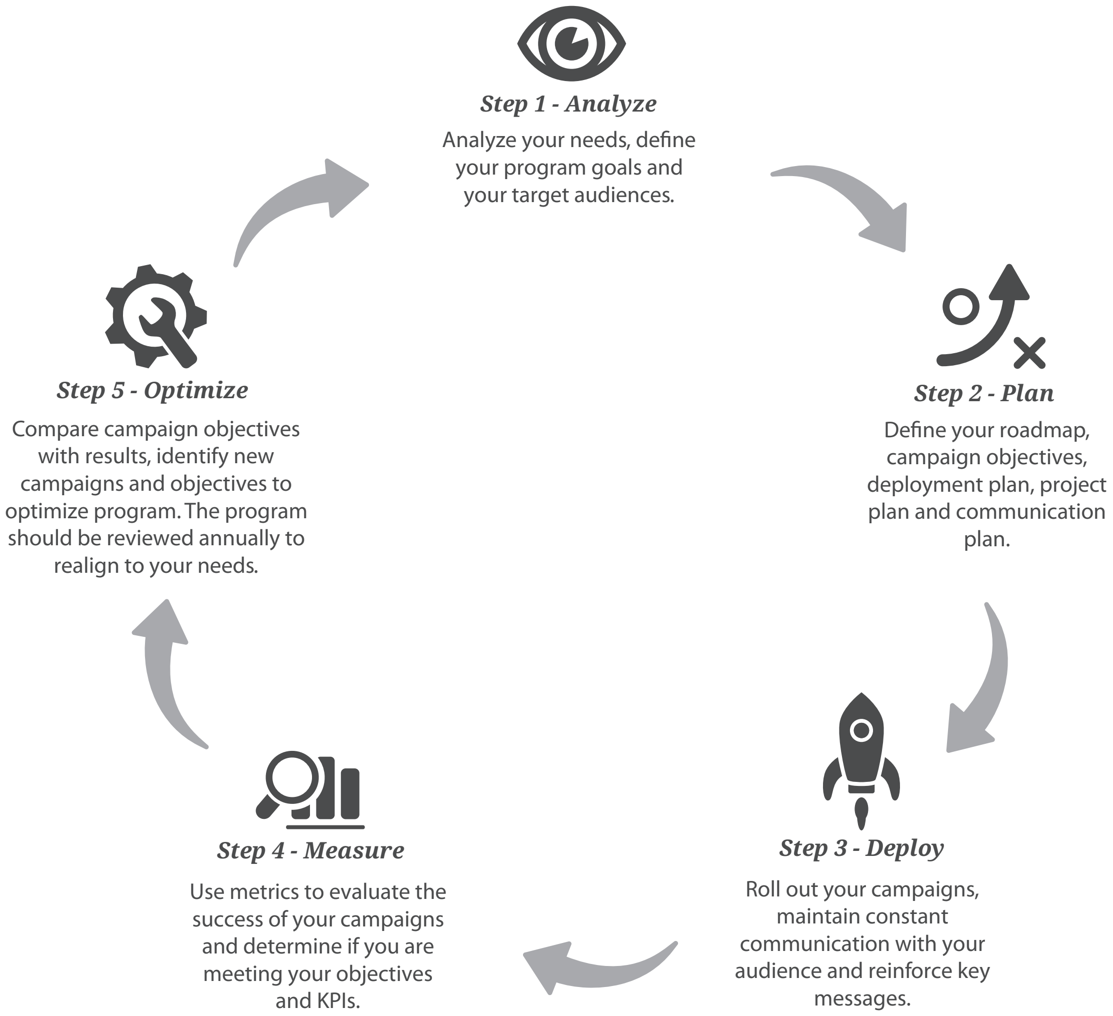
↓

YOUR ORGANIZATION CREATES A STRONGER SECURITY AWARENESS CULTURE

↓

YOU EXPERIENCE A REDUCTION IN HUMAN-RELATED SECURITY INCIDENTS

THE TERRANOVA SECURITY AWARENESS 5-STEP FRAMEWORK AT A GLANCE



Step 1 - Analyze

Analyze your needs, define your program goals and your target audiences.

Step 2 - Plan

Define your roadmap, campaign objectives, deployment plan, project plan and communication plan.

Step 3 - Deploy

Roll out your campaigns, maintain constant communication with your audience and reinforce key messages.

Step 4 - Measure

Use metrics to evaluate the success of your campaigns and determine if you are meeting your objectives and KPIs.

Step 5 - Optimize

Compare campaign objectives with results, identify new campaigns and objectives to optimize program. The program should be reviewed annually to realign to your needs.

The ***Terranova Security Awareness 5-Step Framework*** is a smart, powerful and extremely effective method that has helped thousands of companies around the world successfully change the behavior of their employees and reduce the human risk within their organizations.

WHO IS THIS BOOK FOR?

If you are…

- a CISO
- a privacy officer
- a security manager
- a training manager
- a change management professional
- an information security professional
- a small business owner
- or any person responsible for part of the security awareness program in your organization

I wrote this book for you, even if you…

- have never deployed a security awareness program and don't know where to start
- have deployed a security awareness program, but have lingering concerns about its effectiveness
- have deployed a successful security awareness program, but are interested in learning about other methodologies and frameworks to help reduce human risk

WHY IMPLEMENT A SECURITY AWARENESS PROGRAM?

Security awareness is key to becoming more responsible and secure in the digital world. Implementing training in your organization is a critical component of your global information security plan because it allows you to:

- **Maintain compliance:** You need a security awareness program if you have to comply with any regulations pertaining to data protection, privacy or IT governance.
- **Remain operational:** Given that human error accounts for a significant percentage of data breaches which result in the reduced availability of your operations, you need a security awareness program to help ensure that your people are not vulnerable to attacks.
- **Reduce expenses:** A security awareness program can help you minimize costs associated with incidents and breaches that could result in loss of reputation, interruption of service, productivity loss, data leakage or stakeholder discontent.
- **Clarify responsibilities:** Information security is everyone's responsibility. A security awareness program can help you establish responsibilities for handling information and technology resources.

- **Maintain credibility and trust:** As an organization, you can use your security awareness program to reinforce your credibility and trust with customers, clients, internal and external stakeholders, and auditors.
- **Reduce risk:** The goal of a security awareness program is to make everyone at your organization alert to cyber threats and thus lower the overall risk of a breach.

HOW I BECAME A SECURITY AWARENESS ENTREPRENEUR

Genetics or the Environment

I come from a family of entrepreneurs, but my father always hoped his children would go to University and focus on a profession. He thought it would make life easier for us. As my father hoped, I became a teacher and my brothers chose other professions. However, whether it was the entrepreneurial environment we were raised in or simple genetics, all three of us ultimately became entrepreneurs.

The Journey to Terranova

As a young, new teacher in the early 1980s, my future seemed clear—teach for 30 years and retire with a pension. But deep inside, I knew there would be something more. What I didn't anticipate was that it would be my brother Michel, who would help me jumpstart my career as an entrepreneur.

Michel was selling computers for IBM, which had recently launched a new word processor, the Displaywriter, which stored data on 8-inch floppy discs! IBM wanted to introduce the Displaywriter into schools and colleges and my brother was working on a deal with one of the local colleges. He was hitting a roadblock because they wouldn't complete the transaction without a teacher to train employees. But he knew a teacher!

My brother hauled the big, clunky computer to my place one weekend to convince me to teach people how to use the IBM Displaywriter.

I was 23 years old and I had nothing to lose, so I agreed on the condition that IBM train me on their new computer so I could develop the course. The seeds of entrepreneurship had begun to sprout.

During the eighties, a ton of software packages was being developed for office use, and my brother came to me with another new idea: develop an accounting system on the IBM Displaywriter, which we would then sell to small businesses.

My brother, my husband and I spent all of our spare time on weekends and evenings programming our new accounting software, until we were ready to launch our business: Microcode.

I began selling our new accounting software full time. I worked with teams of IBM reps because our software provided their system with capabilities beyond word processing. This created a whole new market.

Within five years, I started a training department at Microcode, offering software training to large organizations. Business was good.

Over time, we decided to split up the company. My brother focused on the software and my husband and I kept the training.

Soon we were running 36 classrooms a day, and were recognized as one of the largest Microsoft Training Centers for Microsoft in North America. In 1998, we sold the training center to Canadian communications giant TELUS Business Solutions, and I stayed on as Vice President of Training for two years.

After a couple of years at TELUS, my entrepreneurial spirit began to reignite within me. I needed to create something new. I wanted to stay in training and also in IT, but I wanted a product-oriented company I could scale internationally. Terranova was launched in 2001!

I spent my first year doing research on e-learning and talking to clients about what was needed in the industry. Then, over coffee, one of my former employees pointed out that there was a lot of security training for IT people but none for company employees. ***That was exactly what I was looking for—a topic that could be taught to a lot of people worldwide.***

I teamed up with a security expert and e-learning developers, and Terranova's first security awareness course went to market in 2003!

My passion for training and business was reignited with the founding of Terranova, and the flame still burns today as we search for new ways to raise security awareness. This book is one of them!

Terranova Timeline in a Nutshell

- Nov. 2001 – created Terranova
- 2002 – conducted market analysis
- 2003 – developed the security awareness online course
- Sept. 2003 – sold security awareness training to first clients (grocery chain, pharmaceutical industry)
- 2003-2006 – Continued to grow the business (banks, ATVs, federal and provincial government agencies)
- 2006 – Terranova developed its own Learning Management System and assessment tool
- 2007 – Began to target U.S. market
- 2009 – Began to target Europe and offer services worldwide
- 2015 – Terranova was chosen by Gartner as an industry leader for its Magic Quadrant
- 2016 – Terranova developed its new phishing simulation platform
- 2017-2018 – Terranova developed its new integrated platform

Timing is everything

The timing couldn't have been better for me to start exploring this new reality and lay the foundations of my business. As the popularity of the Internet continued to grow, fraud and cybercrime were on the rise. Cybercrime was relatively new, but the threats were very real, and we had only seen the tip of the iceberg. Laws and regulations were beginning to emerge. In 2002, the first American regulation was the Sarbanes-Oxley Act and Canada followed with Bill 198 in 2005.

Companies and individuals alike were taking notice. We started to hear about identity theft and social engineering scams. It was becoming more and more urgent to train people with best practices so they could protect themselves and their organization. With every security awareness program we implemented, we recognized the need to create a comprehensive framework, not only to help CISOs be more efficient when developing their security awareness programs, but also to make their programs more effective.

Drawing from experience

My training background has given me first-hand insights into how people learn. When you deploy your security awareness program, you have to keep in mind a number of factors that have a direct impact on how readily people absorb and retain information.

Your security awareness program 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 is best)
- tailored to their learning capacity and motivation level
- ongoing, repetitive and reinforced

Think back to all the teachers or professors you have had over the years. Which of your classes actually held your interest? Which educators taught you the most?

If your experience is anything like mine, you probably had at least one teacher or professor who simply read from the textbook. Then, there were those incredible educators who engaged you, used creative teaching methods and sparked a love of learning. Years later, you still remember what you learned and use that knowledge in your day-to-day because the teacher made it relevant for you.

➔ ***The same principles need to apply to your security awareness program.***

Do it right

I am sure it is the teacher in me, the educator, the trainer—and the expert—that has compelled me to write this book. I really want people to stop ticking the box and start doing security awareness training right so they get the results they deserve. It is important they see that security awareness can really change behaviors and instill a culture of security.

I deeply believe in offering a product that brings results and solves a problem. I believe in offering true value to our clients. That is why my team and I developed the ***Terranova Security Awareness 5-Step Framework.***

Sometimes you don't know what you don't know

Before writing this book, we also developed an online course based on the ***Terranova Security Awareness 5-Step Framework*** to help our clients build their security awareness program more effectively. We pooled all the knowledge, questionnaires and templates that our professional services team uses to design security awareness programs for our clients and created one comprehensive course.

We then presented our course to a number of clients to get feedback before launching it. Our client said, "You know, Lise, I have been doing this for a long time and I didn't know I had to do all of this for my security awareness program to be successful. I really learned a lot."

To which I replied: "Now that you know, you can't go back. You have to do it the right way."

Let's get started

Creating a security awareness program can feel like a monumental challenge, especially when it comes to getting your people to understand the importance of information security, their individual role in protecting sensitive information, and how their actions—or inaction—may compromise your organization, customers, clients, coworkers or even themselves. It's an important responsibility and can be overwhelming when you think about all the planning, implementation and communication needed for an effective security awareness program.

Let me take some of that weight off your shoulders. In this book, I have laid out everything you need to think about and do based on the ***Terranova Security Awareness 5-step Framework***. It is an extremely effective method that has helped thousands of clients around the world design and deliver successful security awareness programs—and it can do the same for you.

HOW TO USE THIS BOOK

The Human Fix to Human Risk offers you a wealth of valuable information. Think of it as a manual or textbook. It contains a lot of exercises and worksheets that will help you zero in on the right strategies, content, schedules and other decisions you have to make to mastermind the best security awareness program for your organization.

Whether you read this book from cover to cover or jump between chapters, you will surely discover some valuable takeaways you can apply to your security awareness program.

Happy reading and learning!

INTRODUCTION

Without awareness, there is no security.
They're an inseparable pair.

As the number and shrewdness of cyberattacks continues to surge around the globe, there is more and more pressure placed squarely on the shoulders of people responsible for security in every sector of activity, from retail and finance to communications and manufacturing. It is clear that cybercrime is here to stay.

What's more, increasingly stringent regulations are being imposed worldwide, with hefty penalties for noncompliance, as cyber criminals are social engineering and phishing their way into our personal, professional and business lives.

Cybercrime is reaching epic levels and infiltrating security in more ways than we ever imagined. We are all concerned. We are all being targeted. We are all being affected, businesses and consumers alike.

➔ ***You absolutely have to heighten awareness of the human risk factors so the people in your organization recognize and are vigilant about the cyber threats they encounter. Otherwise, your data is simply not secure.***

THE IMPACT OF A SECURITY BREACH

Cyberattacks are not mere nuisances, they are full-blown threats. Their impact is so far reaching that we all need to become human firewalls.

Imagine you are responsible for information security at a complex global retailer that gathers and stores customer information in a database so it can give your customers the VIP treatment (such as VIP discounts or invitations to special sales and events) at any location in the world. Now imagine a hacker gets access to that database. The impact would be costly on so many levels—for your customers, for your company and for you.

Impact on the individual

Preoccupied with information security at the office, we may not always think of how a data breach can hurt actual people like consumers, your friends, neighbors, family and even you personally. **Personal data reflects real people.** When personal data like healthcare information, credit card information or banking records are hacked, mismanaged or mishandled, it can end up on the dark web and sold within minutes. This is especially alarming if you consider that some personal information, such as social security numbers and birthdays, cannot be changed. They can be used in perpetuity to commit crimes such as identity theft, which can disrupt lives and result in financial ruin. Shielding a person's confidential information is the same as protecting the individual.

Impact on your organization

A breach can have devastating financial and non-financial repercussions on your organization. Non-financial impacts could include loss of credibility, reduced consumer trust and even exposure of trade secrets, such as proprietary manufacturing practices or product R&D. From a financial standpoint, an organization could experience a drop in stock value or face regulatory penalties (like those being imposed by GDPR), legal or forensics fees, and the costs associated with a possible operational shutdown.

Impact on you in your professional role

Having the right technology, processes and awareness in place to prevent a breach are very important to any organization. If you are responsible for information security, safeguarding your organization from cyber threats will also positively impact your personal career.

➔ ***Security awareness is the most cost-effective way to prevent a breach!***

WHY ALL THE BREACHES? HOW DO HACKERS HACK?

It's very simple. Security comes down to three things: people, processes and technology.

Security processes and technology are typically well managed by an organization's senior management and IT department.

People, however, remain the greatest point of security vulnerability and are one of the leading causes of data breaches, with human error accounting for a significant percentage of all security incidents. You can set up all the powerful, cutting-edge security technology in the world, but if someone clicks on the link in a malicious email, lets a stranger into the building, uses their kid's birthday as a password, or leaves their mobile phone unlocked, they unwittingly swing the door wide open for hackers to saunter past your security technology and take all the data they want.

The human risk factor is very real. Cyber criminals know that people can be incredibly trusting, and that is why they would much rather take the easy way in—through your people—than try to penetrate your security technology. Human nature makes social engineering not only easy, but also very effective.

Hence, the need for effective security awareness training.

➔ ***And this is why we are sharing our knowledge and experience with you in this book!***

According to Bill Boni, VP and Corporate Information Security Officer of T-Mobile:

"It's rare that organizations have the practitioners, tools, and executive leadership required to understand and respond to security challenges," Boni says.

"Too many people still see information security as a principally technical problem and believe that simply buying the right software will cause the problem to go away.

Information security involves people, processes, and technologies—getting all three in the right measure is the real art of a successful security program."

Source: Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015

HOW DO WE ADDRESS HUMAN RISK?

It isn't enough for the people in your organization to go through the motions of security awareness training.

They actually have to turn their new knowledge into action. They have to stay alert to new threats and help keep data secure over the long term.

You understand the importance of protecting your organization, your customers and even yourself from the harmful effects of an information security breach, and that the human risk factor is the greatest point of vulnerability—the "weakest link."

You therefore need to make security awareness a mindset rather than a set of rules your people have to follow so that their awareness becomes alertness and attentiveness—it becomes second nature. That is how you turn them into the "strongest link" and make them part of your cybersecurity defense strategy.

➔ ***You need to apply a people-centric approach to fix this security problem so you can change human risk behaviors.***

TERRANOVA SECURITY AWARENESS 5-STEP FRAMEWORK INSTILLING SECURITY BEHAVIORS

> *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

Deploying an effective security awareness program across an organization is a complex effort that requires robust, yet simple enough tools and techniques to get the job done.

You also need to prepare and carefully plan—always making sure that you are doing tasks with intention. In other words, that you align your program with your goals and objectives.

I believe the ***framework*** I provide in this book will give you the tools and the structure to do it right the first time because it lays out a series of checkpoints to help ensure that you stay on track and that your program is successful. It forces you to analyze key factors before you start, to plan strategically, and to measure results so you can improve on your approach.

WHY A FRAMEWORK?

This question is best answered by asking why security awareness programs fail in the first place and why they do not effectively help reduce security breaches.

There are countless reasons, including:

1. Security awareness is regarded as project, not as an ongoing process.
2. We start at the deploy 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 set objectives for our program and campaigns.
5. We don't establish key performance indicators (KPIs) or measure results.
6. We don't make our campaigns interesting and interactive for participants.
7. We don't customize content to reflect the reality of our organization or audience.

➔ ***Without a framework, it's just trial and error—you are leaving it to chance.***

Think of awareness like a public service announcement

If you are responsible for security awareness, you are in the business of creating behavioral change and creating a culture of security in your organization. You are literally trying to get people to modify their habits so that they adopt secure behaviors.

If you want to change people's behaviors, you need to do more than ask them to do 15 minutes of intermittent, training or to sit down in front of their computers for an hour once a year. Security has to stay top of mind. To maintain that state of mind, you need a complete program that is made up of multiple smaller campaigns.

Look at seat belts 20 or 30 years ago… When I was a kid, there weren't even seat belts in the back seat of the family car. Then, one day, there was a complete shift in attitude and mindset. To save lives, the powers that began engraining the importance of buckling up. Suddenly the awareness ads were everywhere, citing statistics, laws and benefits. The public service announcements on television and radio were persistent, strong and frequent. There were billboards along the highways and posters at every post office, constantly reminding us to fasten our seat belts.

Now, the first thing we all do when we get in our car is buckle up.

Moreover, seat belt awareness campaigns continue today to reinforce the message, even though it has become second nature for most of us.

The seat belt example clearly illustrates why you need to talk about security awareness all the time.

➔ ***You have to use repetition and reinforcement to change behaviors.***

AN ONGOING METHODICAL APPROACH TO BEHAVIORAL CHANGE

To effectively change behaviors and build a security culture throughout your organization (which I hope I have convinced you is absolutely essential), you have to view security awareness not as a project, but as an ongoing process.

You need a comprehensive program that is carefully planned based on your organization's specific needs and objectives.

What an effective security awareness program involves:

- Your ***program should include multiple campaigns***, which you release over time.
- Your ***program*** should have ***long-term strategic goals*** and you should set ***specific objectives*** for ***each of your campaigns***.
- You should set ***baselines*** using pre-assessments and phishing simulations to ***measure the results*** of your program.

- Your planning phase should ***develop*** a ***deployment plan***, a ***communication plan*** and a ***project plan,*** which include ongoing deployment activities, such as training, communications and reinforcement, to keep security top of mind.
- You should also include a ***post-assessment*** to determine what needs to be improved for the next campaign.

The ***Terranova Security Awareness 5-Step Framework*** equips you to do all of the above, with clearly defined steps that are further broken down into smaller steps, so it's even easier to understand and follow.

I like to think of it as following a favorite recipe: you gather up all your ingredients and then carefully follow the instructions one step at a time, in the right order. The recipe is tested, tried and true—and you will get the same beautiful cake as the master chef who first created it if you simply stick to the recipe. Of course, once you get the hang of it, you will spend less time in the kitchen baking your perfect cake because you become more efficient and get consistent outcomes each time. In fact, you could say that I am sharing my secret recipe with you in this book.

THE CYCLE OF IMPLEMENTING BEHAVIORAL CHANGE

If you want to create change, you need an understanding of the people you are targeting, the context and a number of other factors outlined in the ***Terranova Security Awareness 5-Step Framework***. You will not be able to communicate the importance of security awareness to them and get them on board without a strategy.

You need to do some reconnaissance. You need to gather information at every stage: before, during, and after deployment of your security awareness program.

You need knowledge to create change

Before deployment

STEP 1 – ANALYZE: This is where you take a clear look at your organizational culture, level of security, maturity, target audiences, employee motivation, strategic goals, compliance obligations and other considerations.

➔ This information will enable you to complete ***STEP 2 – PLAN.*** In this step, you will make strategic decisions related to defining your campaigns—in particular, the objectives of each campaign, your deployment plan, project plan and communication plan.

During deployment

STEP 3 – DEPLOY: This is where you prepare and deploy all the learning and communication activities that you identified for the campaigns in your program. Just before kick-off, you do some pilot-testing to make sure the campaign runs smoothly and without any technical issues.

➔ This information will allow you to make any necessary adjustments so that your campaign will better reach the objectives you have set.

After deployment

STEP 4 – MEASURE: You use the metrics and KPIs that you identified in ***STEP 2 – PLAN*** to evaluate the success of your campaign and determine if it is meeting your objectives.

➔ This information will give you important insights that will allow you to complete ***STEP 5 – OPTIMIZE.*** This is where you compare campaign objectives with results and identify new objectives, so you can tweak subsequent campaigns to make them even more impactful.

A significant number of clients who come to us often have off-the-shelf courses in place but not a structured security awareness program. More often than not, they haven't done an **analysis** to know what they actually need. What's more, they have not clearly defined objectives and KPIs regarding what they want to achieve with their training. Typically, they buy training materials, launch their online courses and send an email to participants instructing them to complete the course. No metrics, no tracking, no reporting.

Consequently, there is little emphasis placed on the importance of the training, so it doesn't get the attention it deserves. Before you know it, participants forget the information they may have learned. Typically, it is those types of organizations that tend to suffer a breach. As a result of this shoot-from-the-hip approach, they don't achieve the benefits they were expecting.

Why go through all the bother?

We had a client who purchased some of our online training, but who felt comfortable opting out of implementing our ***5-Step Framework***—our method. "We just want the online training modules. We'll deploy them on our own."

That client suffered a data breach—and a very costly one at that. The client, a holding company, was the victim of social engineering of the shrewdest kind.

The company's Financial Comptroller, who had decades of experience and numerous financial responsibilities, received an email from the CEO (or so she thought), who happened to be out of the office that day. The email advised the Comptroller that the company was moving forward with a takeover bid in the amount of $5 million USD and she needed to make the transfer immediately. It also said the transaction was highly confidential and instructed her to contact a specific external lawyer to make all the necessary arrangements.

She followed the instructions to a tee and even spoke live on the phone with the "lawyer" who requested copies of previous transfer of funds documentation. She willingly complied and nonchalantly sent the requested documents, which included the signature of the other executive needed to finalize the transaction.

The scammers had everything they needed. Clearly, they knew the Comptroller was authorized to make such transfers, that the CEO was out of the office, and that a third signature was required.

The money was soon deposited into an account of a company headquartered in Hong Kong. The holding company was not able to recover the money. The insurance company refused to cover the loss.

This is the stuff of a Hollywood movie. You can almost picture the scammers trolling the CEO's social media profiles, lying in wait for the right moment to strike. Then, cut to the scene of these fraudsters on a turquoise beach with the sounds of the ocean, tropical music and clinking glasses.

Lesson learned

After this devastating experience, the holding company asked Terranova to build a comprehensive security awareness program. They are now implementing a culture of security to put all the chances on their side of not falling for another scam.

➔ ***The moral of the story? Even the savviest among us are always one click away from becoming a victim of a breach.***

Start by doing what's necessary; then do what's possible;
and suddenly you are doing the impossible.

— Francis of Assisi

SECURITY AWARENESS PROGRAM MATURITY

In the security awareness industry, you will certainly come across the term “security maturity.” At Terranova, we focus on ***security awareness program maturity*** and define it according to the following criteria.

Reactive

Almost every organization starts at this level of maturity. It may have some awareness activities, but it does not have a proactive security awareness program with clearly defined goals and continuity. Typically:

- Security awareness is focused on tactical steps to protect business activities or meet regulatory compliance mandates, with little concern for creating a global security awareness strategy.
- The organization generally recognizes the business risks related to human risk factors, but has not established security policies or procedures.
- Most security awareness activities are reactive and ad-hoc in response to incidents.
- Responsibility for security awareness is usually assigned to an IT security analyst, with little involvement or buy-in from senior executives.

Proactive

At this level of maturity, information security awareness is starting to be engrained in the organizational culture. An organization with medium maturity has a security awareness program, with solutions to increase awareness, but activities are not geared at optimizing effectiveness.

- Security policies and procedures are documented and reviewed, and adequate mechanisms are in place to create a culture of awareness and meet compliance obligations.
- Management of all awareness activities is usually centralized.
- There may be missed opportunities to instill long-term behavioral change, develop a security awareness culture and maintain ongoing executive support and buy-in for the program.
- Awareness activities are usually mandatory, closely monitored and promoted by management.

Optimized

At this level, security awareness is well managed, with opportunities to continue to adapt to the organization's risk landscape and optimize program results.

- The organization has control over its security awareness needs.
- It shows responsiveness to evolving threats, solid program monitoring and performance benchmarking.
- Security awareness program metrics are collected and the program is regularly reviewed and updated.
- Information security is firmly engrained in the organizational culture, with high participation rates, executive support and activities orchestrated across all levels of the organization.
- Security awareness is a joint responsibility of business and IT security, and the program is integrated with human resources, legal and communications.

No matter where you are on your security awareness journey, the ***Terranova Security Awareness 5-Step Framework*** is designed to help you mastermind a blueprint for a security awareness program that actually makes sense for your organization. It is designed to help you manage your program more easily, change risk behaviors, measure results and develop a security culture within your organization.

EXERCISE 0.1

WHAT IS YOUR ORGANIZATION'S LEVEL OF SECURITY AWARENESS PROGRAM MATURITY?

Check the box corresponding to the security awareness program maturity level that best describes your organization.

□ Reactive maturity

□ Proactive maturity

□ Optimized maturity

Identifying 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.

Our Professional Services team can perform a thorough maturity assessment and prepare your personalized report, complete with customized recommendations.

WE ARE FOCUSED ON YOUR SUCCESS

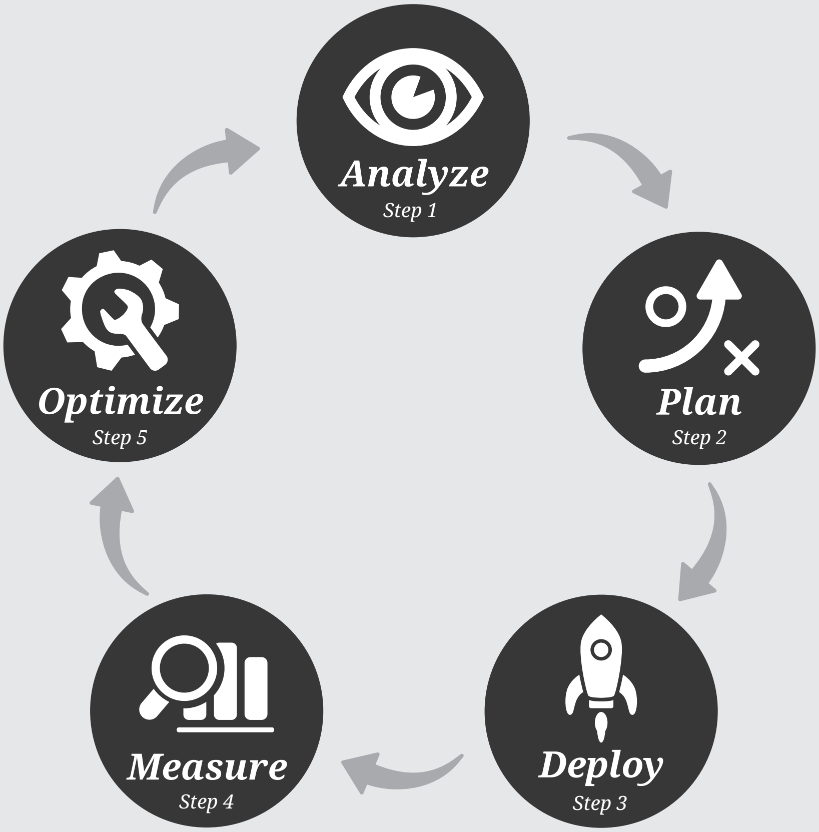
My objective in creating a security awareness framework is so you don't just go through the motions in order to tick the box saying, "There, I deployed online training so I am compliant." I want to give you all the tools to make it easy, do it right and get results.

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

We want you to succeed!

Ready to start *Step 1 – Analyze?*
Let's do it!

WELCOME TO THE TERRANOVA SECURITY AWARENESS 5-STEP FRAMEWORK



Raising security awareness effectively
requires an initial investment in resources
but generates long-term results!

STEP 1 – ANALYZE

1	2	3	4	5
Analyze	*Plan*	*Deploy*	*Measure*	*Optimize*
●	○	○	○	○

Laying a solid foundation is essential to the success of your security awareness program.

Welcome to *STEP 1 – ANALYZE* of the *Terranova Security Awareness 5-Step Framework.*

In this first step of the ***Terranova Security Awareness 5-Step Framework***, you will determine your ***strategic program goals***. These are broad, high-level goals, and are defined as the primary outcomes you intend to achieve through your security awareness program. I outline them in greater detail on page 46.

You will also take a closer look at the various factors relevant to your organization. You will identify risks, your target audiences and their motivation to participate in your program, your compliance obligations, the topics you need to cover and other key considerations. Furthermore, you will assess your organization's current level of security awareness and its capacity to deploy awareness activities, as well as the resources and budget you will need.

➔ ***The information you gather in* STEP 1 – ANALYZE *will give you all the information you need to build your plan in* STEP 2.**

ONE SIZE DOES NOT FIT ALL

I have never seen two organizations that need the same security awareness program, not even if they are in the same industry.

This would also hold true for your organization. Your situation is unique. Your organizational culture is different from the one down the street—and so are your risk factors, staff motivation levels, compliance obligations and ability to deploy a program.

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

How do you identify those strengths and weaknesses, and all of the other factors that will impact the effectiveness of your security awareness program?

… through analysis.

ANALYSIS IS CRUCIAL

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

It is very possible this may feel like a daunting task to you, especially if you are tackling building a security awareness program on your own for the first time, or if you do not have access to resources with the required skills or background to implement a program. Instead of doing your due diligence, you may simply end up taking the first quick-fix training package you find online, or worse, take no action at all. Neither scenario will do.

Let me put your mind at ease. Yes, 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. From there, 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.

PERFORMING YOUR ANALYSIS

Let's take a closer look at your organization and its culture.

Your analysis should focus on 9 primary data-gathering categories:

1. Strategic program goals
2. Compliance
3. Target audiences
4. Scope (topics)
5. Level of knowledge
6. Motivation and culture
7. Support resources
8. Globalization
9. Costs (resources)

EXERCISE 1.0

STARTING YOUR ANALYSIS

Take some time now to reflect on the following questions. You only need to give brief, high-level answers. We will go into a more in-depth discussion on each as we move forward. Consult with people in your organization, if necessary, to get as complete a picture as possible. Doing this exercise now will guide your thinking and the direction of your program will begin to emerge.

1. STRATEGIC GOALS

What are the strategic goals of your security awareness program?

2. COMPLIANCE

Does your organization have any contractual, industry-related or regulatory obligations? (Consult with your administration, if necessary.)

□ Yes □ No

If yes, what are they?

3. AUDIENCE

What audiences are you targeting with your security awareness program? In other words, what people in which departments? What about upper management, third parties, contractors, business partners or customers, etc.?

4. CURRENT KNOWLEDGE LEVELS

What is the current security awareness level of each target audience?

□ No knowledge

□ Little knowledge

□ High level of knowledge

Any risk behaviors that compromise information security? *(e.g. not securing devices or paperwork, visiting malicious websites, opening email attachments from unknown senders, sharing passwords).*

5. SCOPE (TOPICS)

What awareness training topics are required for each target audience based on their current level of awareness, as well as the current security threats affecting the people at your organization, contractors, business partners or customers, etc.? *(Consult with your administration, if necessary).*

6. MOTIVATION

What is the current organizational culture regarding security awareness? Are people on board, indifferent or resistant?

How motivated are they when it comes to information security?

□ Low

□ Medium

□ High

7. SUPPORT RESOURCES

Do you need to build a support team to help implement your security awareness program?

□ Yes □ No

If yes, who will you approach?

What departments or individuals would be able to help you address some of the challenges of putting together and deploying your security awareness program?

8. GLOBALIZATION

Do you need to offer your security awareness program in more than one language?

□ Yes □ No

If yes, what are they?

Will you have to customize content to reflect any geographic regions or cultures?

□ Yes □ No

If yes, specify.

Does your organization have the required resources, capabilities and capacities to deploy a security awareness program to all locations, business units and countries where you have operations?

□ Yes □ No

Specify what is needed or lacking

9. COSTS (RESOURCES)

What resources, time and budget are available to you to create and deploy an effective security awareness program?

Will a budget be available year after year for the current program, as well as for new initiatives?

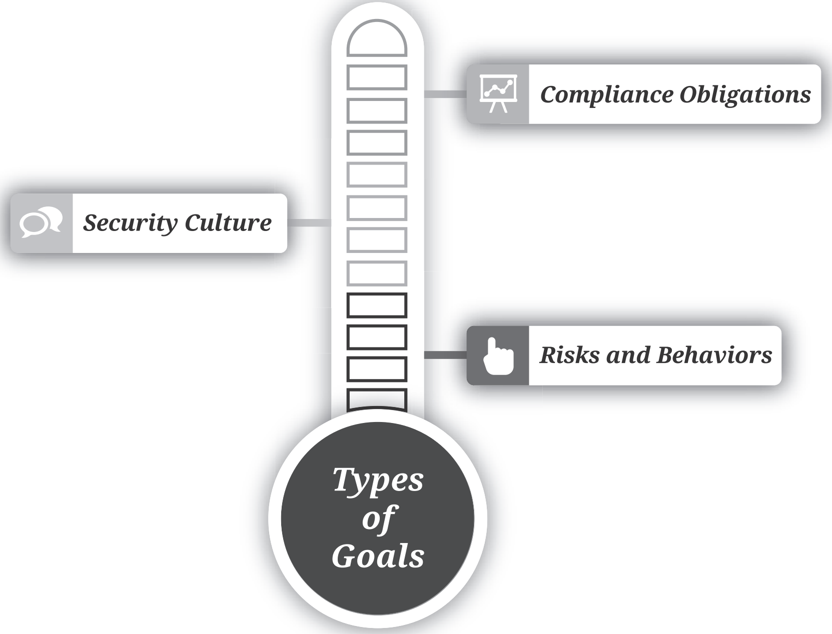
□ Yes □ No

Specify what is needed or lacking

Think of this exercise as your "cheat sheet." Once you have gone through all the other exercises in ***Step 1 – Analyze,*** you should come back to adjust your answers. Then, refer to it from time to time to make sure your actions are aligned with the critical factors that you need to take into account in ***Step 2 – Plan*** of your security awareness program.

9 PRIMARY DATA-GATHERING CATEGORIES

1. DEFINING YOUR STRATEGIC PROGRAM GOALS



Now, let's delve into the reasons why you are deploying a security awareness program. Your first response may be "because I have to" or "it's part of my responsibilities" or "that's what I was hired to do."

However, it is important to clearly identify *what you aim to achieve*. Although they are broad and high level, your ***strategic program goals*** have to be concrete and tangible, not vague and ambiguous. Once those goals are defined in ***Step 1 – Analyze***, you will be able to define specific objectives for your individual campaigns in ***Step 2 – Plan***.

As with any project or program—whether for security awareness, another facet of business or even in your personal life—*you have to identify your goals* so you can *plan all the steps* you need to get there. Otherwise, your program is just hit and miss, and it won't produce the results you want.

Outlining what you intend to achieve will also help you to 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.

CATEGORIES OF STRATEGIC PROGRAM GOALS

Your strategic security awareness program goals could be in any or all of these three categories:

1.Risks and behaviors

- to reduce risk and behavioral changes

2.Security culture

- to instill or reinforce a culture of security

3.Compliance obligations

- to ensure compliance with your organization's security obligations

EXERCISE 1.1.

DEFINING YOUR STRATEGIC PROGRAM GOALS

What are the strategic goals of your security awareness program? Check ALL the boxes that apply.

1. RISKS AND BEHAVIORS

□ Reduce human errors

□ Encourage everyone at your organization to adopt security best practices

□ Reduce human-related security incidents

□ Address the rapid changes in your organization's threat landscape

2. SECURITY CULTURE

□ Demonstrate the importance of information security

□ Mobilize managers to become security and awareness ambassadors

□ Change attitudes toward security within your organization

□ Get people to consider the security implications of their actions

□ Get people to understand their responsibilities in protecting information assets

3. COMPLIANCE OBLIGATIONS

□ Meet legal, regulatory or industry awareness compliance obligations

□ Fulfill contractual agreements regarding security and privacy awareness clauses

□ Enforce organizational security policies and standards

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.

2. IDENTIFYING YOUR COMPLIANCE OBLIGATIONS

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

Compiling ALL your organization's compliance obligations will allow you to make sure you design a laser-focused program that meets all requirements and avoids any oversights or omissions in the awareness training you deploy. What's more, it will help you identify the specific target audiences you will need to include in the different campaigns of your security awareness program. (*See page 51 on Identifying Your Target Audiences)*.

It is important to note whether your target audiences require ***both*** compliance ***and*** security awareness training:

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

KEY COMPLIANCE OBLIGATIONS

- Contractual obligations
- Financial processing obligations
- Governmental regulations (e.g. GDPR, HIPAA/HITECH)
- Industry-related obligations (e.g. PCI DSS)
- Privacy obligations

➔ ***If you have any doubts about your organization's compliance obligations, be sure to reach out to your legal, compliance or privacy teams to help you identify the obligations that must be addressed by your program.***

EXERCISE 1.2.

IDENTIFYING YOUR COMPLIANCE OBLIGATIONS

Check ALL the boxes that apply to your organization. Specify the name of the obligation and the key requirements you need to include when planning your security awareness program.

□ **Contractual obligations regarding security**

Obligation: ....

Key requirements: ....

....

Obligation: ....

Key requirements: ....

....

□ **Financial processing obligations**

Obligation: ....

Key requirements: ....

....

Obligation: ....

Key requirements: ....

....

□ **Governmental regulations**

Obligation: ....

Key requirements: ....

....

Obligation: ....

Key requirements: ....

....

□ **Industry-related obligations**

Obligation: ....

Key requirements: ....

....

Obligation: ....

Key requirements: ....

....

□ **Privacy obligations**

Obligation: ....

Key requirements: ....

....

Obligation: ....

Key requirements: ....

....

□ **Other obligations**

Obligation: ....

Key requirements: ....

....

Obligation: ....

Key requirements: ....

....

Obligation: ....

Key requirements: ....

....

Your organization's compliance obligations are usually very specific. To ensure that you fulfill those obligations, you need to have all those requirements at your fingertips so that you can target the right audiences with the right messages.

Mark this page and refer back to it regularly!

3. IDENTIFYING YOUR TARGET AUDIENCES

When you are implementing a security awareness program, you are essentially working in the field of communications. You are trying to engage people with an important message and get them to respond to it with your call to action. Specifically, you want them to recognize the importance of security awareness, understand their role and do the awareness training willingly. ***You want them to change their risky behaviors.***

Know who you are talking to

You may have to communicate with different groups of people—different target audiences—and will have to create a connection with each one. To do so, you need a very clear view of the different types of people you are talking to, who they are, their position or role in your organization, their motivation levels and any other relevant insights that will make them receptive to your message.

Changing behaviors is the name of the game

Like in all communications, you will have to adapt your language and message to the people you are talking to. You are, after all, convincing them to learn and retain information so that they change their behavior. Therefore, if you want everyone to be enthusiastic, it is important that you speak their language.

I go into greater detail on creating a strong communication plan on page 119 and selecting content for different target audiences on page 102 of ***Step 2 – Plan.***

Who are your target audiences?

Now, let's look at your target audiences.

Your target audiences are of course all those who belong to your organization, from your top executives and department heads to your IT staff and general staff. You might even want to extend your security awareness program to contractors who work with your organization and sometimes even to your clients.

You should also consider all of 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, such as a cashier with PCI DSS compliance duties or the receptionist who buzzes in visitors.

IMPORTANT:

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 the risks facing their organization in order to support and fund security awareness initiatives.

Managers

- Raising the awareness of managers about the risks facing their organization should mobilize them to act as ambassadors and security role models.

End users (general staff)

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

IT staff

- Raising 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 that exist in your environment.

Specialized 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 and the particular threats they face, or the regulations with which they must comply.

THIRD PARTIES – ADDITIONAL SPECIALIZED ROLES

Contractors

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

Business partners

- You may be taking all the necessary information security precautions, but are your partners or associates doing the same? To ensure that the information you share remains safe and confidential, business partners need to have the same level of security awareness.

Clients

- You may want to offer data security tips to your clients as an added value. A good example of this would be a bank offering suggestions to help protect clients from fraud and theft. This also would help reduce the number of incidents the bank 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, and therefore faculty, staff and students are required to take security awareness training.

Suppliers

- A business can be a very busy place. Suppliers are coming and going all day long and there may be certain security procedures you need them to be aware of and follow. Consider a photocopier technician who comes in regularly to service your machines or truck drivers who deliver products through your loading docks.

EXERCISE 1.3.

IDENTIFYING YOUR TARGET AUDIENCES

Review the target audiences outlined in the previous section and then check all those target audiences that are applicable to you. Think about your strategic program goals, which you identified on page 47, as well as your compliance obligations, which you listed on page 49.

GROUPS OF PEOPLE WHO WORK FOR YOUR ORGANIZATION

□ **Executives**

□ All

Specify: ....

....

□ **Managers**

□ All

Specify: ....

....

□ **End users (general staff)**

□ All

Specify: ....

....

□ **IT staff**

□ All

Specify: ....

....

□ **Specialized internal roles (people in various functions or departments of your organization)**

Specify: ....

....

ADDITIONAL SPECIALIZED ROLES — THIRD PARTIES

□ **Contractors**

Specify: ....

....

□ **Business partners**

Specify: ....

....

□ **Clients**

Specify: ....

....

□ **University professors and students**

Specify: ....

....

□ **Suppliers**

Specify: ....

....

When you deploy a security awareness program, you want everyone on board so that you have a high success rate.

To engage them and get them to act, you need to know who they are. You need to define ALL your target audiences.

4. DEFINING THE SCOPE OF YOUR PROGRAM (THE TOPICS)

Changing risky behaviors with the right topics

In this part of ***Step 1 – Analyze***, you will determine what topics should be covered in the awareness training you are developing for each of your target audiences.

Some of the topics will be common to all your target audiences, such as password protection or safe use of the Internet, while others will be very specific to a particular group (e.g. Privacy). Remember, if you want your communications to be impactful enough to actually instill new security behaviors, the topics you cover must be relevant to the target audiences you are addressing and presented in a language they understand.

ESSENTIALS OF EFFECTIVE AWARENESS

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

IMPORTANT: When determining the topics to include in your security awareness program, you also need to take into account all the requirements of the compliance obligations you identified in Exercise 1.2. on page 49.

To get a better idea of the topics you need to cover to meet these obligations, you could gather information from recent security incident reports. Such incidents are a clear indication of where you should be focusing your training priorities. I discuss this in more depth on page 42.

Scoping out your topics per audience

Over the course of the past two decades, the Terranova team and I have seen every imaginable scenario for security awareness. This experience has allowed us to zero in on the topics that are most 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 the risks facing your organization in order 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
- Common attacks and scams targeting executives
- Your organization's security and awareness compliance obligations

Managers

Raising the awareness of managers 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 aim to increase overall understanding of security threats and should communicate the best practices and behaviors that you want them 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 staff

Raising 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 that exist in your environment.

Topics to consider:

- Network security overview
- Application security overview
- Common network and application attacks
- System development lifecycle (SDLC) and secure coding
- Security framework
- Cryptography and key management
- Privacy by design/default

Specialized roles

Raising awareness about IT security for those in specialized roles will depend on your organizational structure, the particular threats they may encounter, the type of access to data they have or the regulations with which they must comply.

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)

EXERCISE 1.4.

DEFINING YOUR TOPICS PER TARGET AUDIENCE

Check the boxes of the target audiences you identified in Exercise 1.3. and, referring to the outline on the previous pages, specify the key topics ***you assume you need*** to address for each.

TARGET AUDIENCE KEY TOPICS FOR YOUR SECURITY AWARENESS PROGRAM

□ **Executives**

□ All

Topic(s): ....

....

□ **Managers**

□ All

Topic(s): ....

....

□ **End users (general staff)**

□ All

Topic(s): ....

....

□ **IT staff**

□ All

Topic(s): ....

....

□ **Specialized roles (both internal and third party)**

Specify role: ....

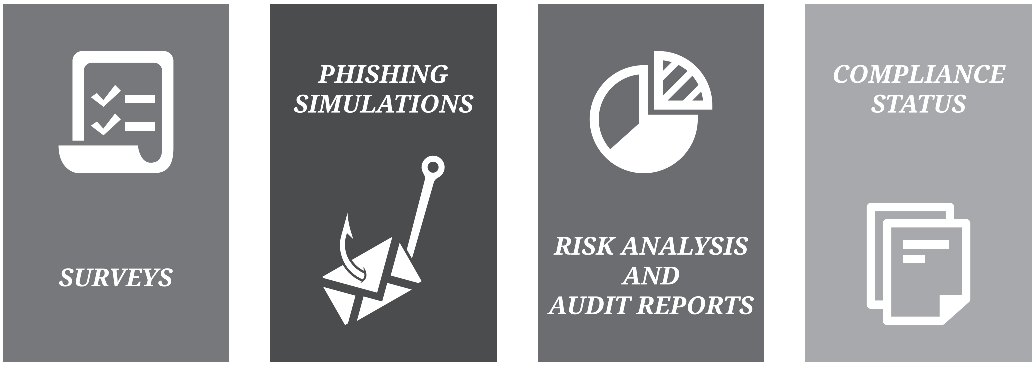
Specify role: ....

Specify role: ....

Review your answers above. Take note of any topics that are common to more than one target audience so you can streamline your program, whenever possible.

Remember: Tailoring your content to each group will make your overall security awareness campaign more impactful. You will be more successful at changing behaviors because you will be communicating information that is relevant to each person's day-to-day activities.

5. ASSESSING YOUR TARGET AUDIENCE'S LEVEL OF KNOWLEDGE



Getting a grasp of each target audience's level of knowledge and understanding of security is critical. Essentially, the ultimate and most effective course will be one that is designed to fill in the knowledge gaps of each target audience. You will be giving them new knowledge that will compel them to change their behaviors. After all, acquiring new knowledge is the foundation of change.

Think of it this way… You and a friend want to take a French class. You studied French in high school and even spent a summer backpacking in Provence, so you have good conversational skills. Your friend, on the other hand, has never studied any foreign languages. Obviously, you will not take the same class because you are not at the same level of comprehension. If your friend takes your class, he may be overwhelmed. If you take his class, you may be bored and disinterested. Neither of you will learn much of value.

➔ ***Remember, you need knowledge to create behavioral change.***

Your next task is to measure the level of knowledge and identify knowledge gaps for each target audience to make sure your choice of security awareness topics is aligned with the real-world needs of your organization. By doing so, you will design effective course content that will actually bring about changes in behavior.

To confirm your choice of topics and make a final decision on content, it is important to compare your assumptions to the reality in the field. Your "assumptions" are the topics you listed per target audience in Exercise 1.4.

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:

1. **Surveys**
2. **Phishing simulations**
3. **Risk analysis and audit reports**
4. **Compliance status reports**

SURVEYS

1. Surveys

An awareness assessment survey, which often takes the form of a short quiz or questionnaire, is useful for determining the strengths and weaknesses of your target audiences in terms of 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.

PHISHING SIMULATIONS

2. Phishing simulations

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

Phishing simulations are typically based on the most common security threats, including malicious website URLs, file attachments, ransomware, and business email compromises (BEC), to name a few.

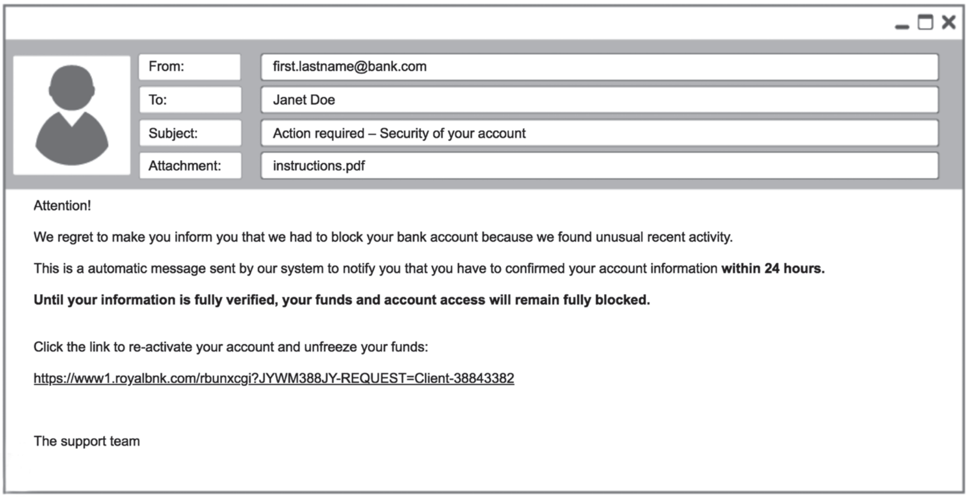
The advantage of using a phishing simulation package, such as the ones we have created at Terranova, is that it provides built-in detailed reporting so you can analyze the results and have tangible evidence of the weaknesses in your security. This analysis can be especially helpful when presenting your reports to upper management or decision makers about the importance of raising security awareness in your organization.

Creating a phishing baseline

We always recommend doing an initial simulation in ***Step 1 – Analyze*** in order to establish a baseline to use for comparison purposes following deployment of a security awareness campaign. For example, most organizations that perform phishing simulations experience a 20 to 30 percent simulation failure rate the first time (i.e. 20 to 30 percent of the target users are victims!). Following training, they administer another phishing simulation, hoping to see a lower failure rate.

➔ ***To be successful, it takes recurrent simulations to reduce rates to a desired level—a fact reinforcing our position that security awareness training is not a project, but rather an ongoing process.***

SAMPLE PHISHING SIMULATIONS USED TO ASSESS CURRENT SECURITY AWARENESS KNOWLEDGE



From:	first.lastname@bank.com
To:	Janet Doe
Subject:	Action required – Security of your account
Attachment:	instructions.pdf

Attention!

We regret to make you inform you that we had to block your bank account because we found unusual recent activity.

This is a automatic message sent by our system to notify you that you have to confirmed your account information **within 24 hours.**

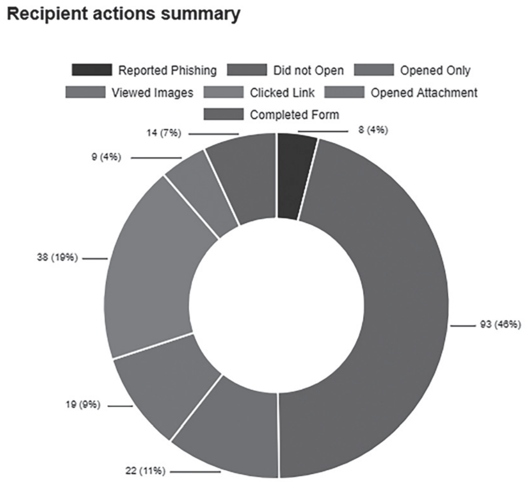
Until your information is fully verified, your funds and account access will remain fully blocked.

Click the link to re-activate your account and unfreeze your funds:

https://www1.royalbnk.com/rbunxcgi?JYWM388JY-REQUEST=Client-38843382

The support team

PHISHING DASHBOARD SHOWING WHERE YOUR ORGANIZATION IS AT RISK



RISK ANALYSIS AND AUDIT REPORTS

3. Risk analysis and audit reports

All companies, organizations and even you personally are under constant threat of some type of cyberattack. 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)
- Research reports from security firms identifying user behaviors that lead to information security incidents
- Internal audit reports that document security risks

COMPLIANCE STATUS

4. 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 in Exercise 1.2. on page 49.

Compliance obligations can be regulatory, contractual, industry-related, privacy-based or financial. Many of them require annual assessments or compliance status reporting. These can be used to identify specific weaknesses that need to be corrected. Some, such as PCI DSS or GDPR, require you provide awareness training in order to be compliant.

Remember, if you have any questions or doubts about your organization’s compliance status, you should contact your legal, compliance or privacy teams to help you identify compliance obligations that must be included in your program.

EXERCISE 1.5.

IDENTIFYING KNOWLEDGE GAPS

What topics do you need to prioritize to increase the overall security awareness? What topics will reduce the discrepancies between the current and desired security practices?

A. 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
- Other: ....

□ **Managers**
- Surveys
- Phishing simulations
- Interviews
- Other: ....

□ **End Users**
- Surveys
- Phishing simulations
- Interviews
- Other: ....

B. Make a list of all existing relevant reports regarding your company's security incidents or thefts that have been reported. (See page 63 for report types).

□ **Public research reports**
- Source 1: ....
- Source 2: ....
- Source 3: ....

□ **Internal audit reports**

□ **External audit reports**

□ **Compliance reports**
- Source 1: ....
- Source 2: ....
- Source 3: ....

C. List all your organization's compliance obligations, and any available compliance status reports. Refer to your answers in Exercise 1.2. on page 49.

....

....

....

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

6. ASSESSING MOTIVATION

How motivated are people to change the way they do things and adopt best practices so your organization is better protected against cyberattacks?

Remember the example of drivers wearing seatbelts? Some drivers are motivated to wear a seatbelt because they are convinced it will save their life. Others simply do it because they don't want to get a fine. Then there are those who simply won't participate no matter how hard you try to convince them to buckle up!

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

MAKING IT ALL ABOUT THEM

One of our clients, a small corporation located a few hours outside of a major urban center, with a workforce of about 200 employees. This company is an important employer in the region, and the local population depends on it, and it depends on the local population.

Being such a close-knit community, the leadership team simply knew from experience that employee motivation to do security awareness training would be low. They did their analysis by means of years of observation. It was informal, but an analysis nonetheless.

Given this corporate set-in-their-ways culture, it would prove very difficult to impose behavioral changes to reduce the security risks faced by the company. They came to us for assistance and, together, we created a "Lunch & Learn" conference for all employees.

We made the training all about them—all about the employees. We promoted the conference as a company initiative that would help them and their families be safer when shopping online, posting on social media, surfing the net and so on.

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

Although the Lunch & Learn had a hidden agenda, the impact was very positive. It was a first step towards security awareness.

Understanding the role of motivation

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

When you are implementing your security awareness program and campaign, you may face resistance from your different target audiences, especially if part of your campaign involves exercises that are not directly related to their jobs. They might, as a result, underestimate their own responsibilities and the impact of their actions on your organization's overall IT security.

There are a number of reasons why your target audiences may not be motivated to participate in your security awareness program, including:

- Training is not mandatory.
- The importance of security has not been clearly communicated.
- They feel they already know everything.
- They feel 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.

➔ ***Remember, awareness-raising activities are aimed at human beings.***
It is therefore essential to consider their needs and mindset when planning your activities.

IMPORTANT:

If your target audience belongs to a bargaining unit, a union or syndicate, you will surely have to interface with them through your HR or legal team or through labor relations.

You might need to get their "non-objection" to participating in your security awareness initiatives or they may object to being evaluated.

Types of human motivation

Motivation is analyzed in depth in the field of behavioral change management, and is classified into three categories based on specific indicators:

1. Intrinsic motivation

2. Extrinsic motivation

3. Amotivation

INTRINSIC MOTIVATION

1. Intrinsic motivation… sure, I'm on board!

People who are intrinsically motivated (i.e. motivation that comes from within) consider their behavior as important. They will participate in your security awareness program and apply what they learned because they understand their role in protecting information assets. To increase their commitment to security, you might:

- Directly involve them in various stages of the security awareness program (e.g. planning, content selection and evaluation). Giving them a voice allows them to take ownership in your program's success.
- Offer them the opportunity to help you develop other security awareness activities.
- Make them "champions" of your security awareness program within their sphere of influence.

Indicators: I have fun learning how to do this. It is important to me and consistent with my personal values and interest.

EXTRINSIC MOTIVATION

2. Extrinsic motivation… ok, I guess I have to…

People who are extrinsically motivated (i.e. motivation that is driven by external factors) do things because they are asked to do so. Their actions are in response to external pressures. Strict instructions, a controlled environment and use of rewards are examples of mechanisms that can influence them. To increase their commitment to your security awareness program, you might:

- Make the awareness activities mandatory.
- Make the awareness activities interesting and interactive in order to capture and maintain their attention.
- Make it about them. Communicate how the topics can help them stay secure in their personal lives and include topics that

are not work related, such as “Staying Savvy on Social Media” or “Keeping Your Home Computer Safe”.

- Introduce gamification. For example, create competitions between departments and offer a small prize to the team that finishes first or has the highest participation rates.
- Use rewards (e.g. prizes, contests, etc.) to increase participation.
- Use constant communication to inform your target audience of their responsibilities.
- Reprimand those who repeatedly compromise information security.
- Announce and reward good behaviors that prevented an incident.

Indicators: I do it because I am asked or forced to.
I also want the reward.

➔ ***Your aim is to change extrinsic motivation into intrinsic motivation.***

AMOTIVATION

3. Amotivation… I don’t see why I have to do it… what’s in it for me?

People who are amotivated (i.e. unwilling to participate) show a lack of desire to follow instructions. This is usually due to their inability to recognize the impact of their actions, or because of their feeling of incompetence or general disinterest. They challenge the reasons for being asked to behave in a particular way and usually do not see the concrete benefits. To increase their commitment to your security awareness initiatives, you might:

- Use formal or informal events to explain why security is important and the reason for security awareness programs.
- Demonstrate the results of a given behavior (e.g. through a phishing simulation).
- Illustrate to them that they are directly concerned (e.g. through a quiz).
- Reprimand those who repeatedly compromise information security.

Indicators: I do not know why I have to behave this way. I feel like I’m wasting my time trying to learn how to behave this way. It is not my responsibility.

➔ ***Your challenge is to change amotivation into extrinsic motivation and ideally into intrinsic motivation.***

When people put up a little resistance…

One of our clients—a university—that was having a hard time getting its employees to complete their security awareness training, which actually wasn't all that surprising. For starters, their management had decided the training wasn't mandatory, and the overall attitude of the staff was indifference with a dash of "I already know all that."

We suggested performing an analysis of their current level of awareness. In that analysis, we included a survey to establish a baseline of what staff members actually knew in terms of security awareness and what they didn't know.

We also had a *hidden agenda* in conducting this survey: we wanted to find out *how many* people would participate in the survey on a voluntary basis. We asked them to fill out the online questionnaire, explaining that the university was building a new security awareness program and needed their help. "Please tell us the key elements about information security that concern you so we can build a more tailored program." We were asking them to be part of the process—and part of the solution. Yet, despite repeated and frequent reminders, participation in the survey was extremely low.

Our takeaway: If you can't get them to do a simple survey, how are you going to get them to do the awareness training?

We used that information to prove to the information security team that they have a problem: you can deploy all the training you want, but your people are not motivated to learn. You are going to waste time and money buying courses, paying for licenses and deploying training because very few are going to participate.

We knew for sure that participation would be low. Next, we had to determine how alert the unmotivated staff members were to the risks. We decided to measure their awareness using phishing simulations. We sent them fake emails to see if they took the bait. We didn't tell them it was part of an assessment process, so they would end up participating without even knowing the real motive.

And take the bait they did. The results showed us that the university did, indeed, have a security awareness problem.

As I said in the beginning of this case study, management was not inclined to make training mandatory.

Hoping to convince management to reverse its decision, we helped the information security team build a business case, using survey participation rates and phishing simulation results as evidence that the organization was exposed to threats, thus compromising the university's compliance obligations. Allowing training to be optional was no longer viable.

After viewing the report, management and HR ultimately decided to make training mandatory for those who failed the phishing simulation in order to meet their regulatory training and reporting obligations related to privacy and PCI DSS. Those staff members were advised they would keep getting escalating reminders until the training was completed.

As a final measure to course correct for the future, we recommended making training mandatory for all new hires, especially since it is relatively effortless to include it in their onboarding training.

➔ ***This would be the beginning of a new culture of security. A new mindset.***

EXERCISE 1.6.

ASSESSING MOTIVATION

Motivation plays a fundamental role in your security awareness program. You therefore have to determine:

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

At Terranova, we use a simple, straight-to-the point survey to gage motivation levels. The information we glean from this survey gives us insights into what we can do to increase motivation, if needed.

Here is an example of a quick motivation survey:

ABC COMPANY SURVEY

We would like your opinion!

Our company is planning to roll out a security awareness program to keep you and your fellow employees better protected against phishing scams, malware and other cyber threats.

Please tell us how you feel about the following statements on a scale of 1 to 5.

1. Strongly disagree
2. Disagree
3. Neither agree or disagree
4. Agree
5. Strongly agree

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

Survey objectives

This survey will shed light on two key elements:

1. The number of employees (%) 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 to meet expectations and fulfill corporate obligations (extrinsic motivation)?

Scoring and interpreting your results

- More agreement with question #1 indicates *intrinsic motivation*.
- More agreement with question #2 indicates *extrinsic motivation*.
- More agreement with question #3 indicates *amotivation*.

The scope of your security awareness program will depend on the percentage of intrinsic motivation vs extrinsic motivation vs amotivation 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 useful and will be the first to complete the program. **These users can be selected as your security awareness champions or participants in the pilot test, which we will discuss in more detail on page 136.**
- 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 their participation (e.g. a coffee shop gift certificate, promo items). You might also try gamification by creating competitions between individuals or departments to get them more involved.
- 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 understand 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.

7. IDENTIFYING YOUR AVAILABLE SUPPORT RESOURCES

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

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.

There are a number of scenarios that could pose challenges you will have to overcome.

To be successful, you are therefore going to need support.

When choosing awareness-raising activities, you have to take into account your allocated budget, your support resources and their availabilities, the equipment you need and other requirements. You may have to rely on the assistance of other departments within your organization, or even call on the services of external resources.

We have identified 3 support resources:

1. Upper management support

2. Security awareness champions

3. Operational support

1. Upper management support

Getting strong support from management will help you secure the budget you need for your security awareness training. Furthermore, it will legitimize and raise the visibility of your program. If management is actively behind you, motivation levels and participation rates will certainly be higher.

Therefore, prior to planning and implementing your program, you should solicit support from upper management. In particular, you will need to find an executive to act as your **program sponsor**—someone engaging who would be a good spokesperson for your security awareness program and who your target audiences recognize. I go into more detail about the program sponsor in ***Step 2 – Plan, Building Your Team on page 89.***

2. Security awareness champions

To raise security awareness effectively, many organizations use security awareness champions to liaise with a major site, a business function or a business unit. These ambassadors are people who are *intrinsically* motivated.

They are ideally business people with an in-depth understanding of the inherent risks of technology, and they are therefore able to enthusiastically explain why the security awareness program is so important to your target audiences.

Security awareness champions are your ambassadors—people you know you can count on to be highly supportive of your initiatives and who will actively encourage others in your organization to participate in your security awareness program.

3. Operational support

Before and during your security awareness program deployment, you will certainly need operational support from your **IT department** (for user list file transmission or synchronization considerations for single sign-on, Internet bandwidth sizing, helpdesk interventions and other support activities).

As we saw in the case study on page 69, your **Human Resources** department should be included in your support resources, particularly if you want training to be mandatory for new hires.

Working with a **behavioral change expert** can also be very 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.

➔ ***You need a solid support team that can assume some of the responsibilities of deploying a successful security awareness program.***

EXERCISE 1.7.

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: ....

Others: ....

....

....

□ **Identify potential information security awareness champions and ambassadors**

....

....

....

....

□ **Identify the operational support required to run your security awareness program**

....

....

....

....

8. ANALYZING GLOBALIZATION

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

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

Let's start off this section with a quick questionnaire.

It is important to keep globalization in mind if you answered "yes" to any of the above questions, because you may have to customize the content and delivery of your security awareness program to reflect a variety of geographic regions or cultures. (See chapter 3 on page 102 for a more in-depth discussion.)

Complexities like multiple locations or multi-language environments can also make deployment of your security awareness program a little bumpy, so they need to be identified and addressed early on. Imagine putting so much effort and planning into deploying your security awareness program worldwide and then you realize that one of your teams speaks predominately Portuguese—but your program is not currently available in that language. It would drastically delay your program if you had to wait for everything to be translated before you could deploy.

EXERCISE 1.8.

ANALYZING GLOBALIZATION

Do you have multiple offices or facilities?

□ Yes □ No

If yes, what are they?

Are they local, national or international?

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

□ Yes □ No

If yes, what languages are they?

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

□ Yes □ No

If yes, what are they?

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

□ Yes □ No

If yes, what are they?

....

....

....

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

□ Yes □ No

If yes, what are they?

....

....

....

Are there any local support departments or are they centralized?

□ Yes □ No

If yes, what are they?

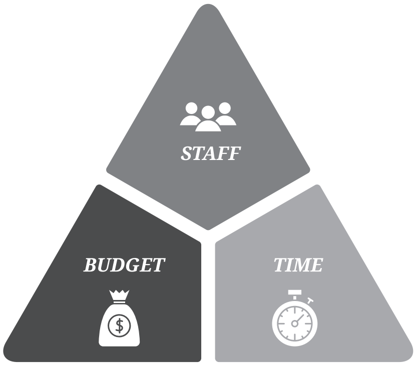
....

....

....

If you operate in more than one language or in more than one geographical location, you have to consider not only how you will **communicate** and **customize** your content to your different target audiences, but also how you will **deliver** your security awareness program.

9. WORKING OUT YOUR COSTS



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

This information will also help you determine if you can allocate funds for outsourcing or professional services if your security awareness program is too complex to handle entirely in house.

Typical costs associated with a security awareness program

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)
- Learning management system (LMS) 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, hand-outs)
- 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 required

Indirect costs

Always remember that "time is money." Although these items are already budgeted by your organization, these are indirect costs attributed 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 significant operating cost for large organizations)
- Program sponsor's time

- Time spent reviewing the overall content by legal and HR departments and others
- Time spent validating translations

Developing content vs purchasing content

Some clients have asked us for advice on developing and producing their own awareness training content. We took a serious look at the question and did the math. There is a lot of content available on the market and providers update their content every year. It is difficult for an organization to do that on its own, especially since it is not their core business. We recommend purchasing ready-made content that can be customized and letting the provider do the updating. It is simply more cost effective than researching and developing new content in house.

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

EXERCISE 1.9.

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?

□ Yes □ No

If yes, how many? ....

Do you need any full-time employees to run your program?

□ Yes □ No

If yes, how many? ....

Do you need a project manager to oversee the program?

□ Yes □ No

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?

□ Yes □ No

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 an external security awareness professional to oversee more steps in your security awareness program).

□ Step 1 – Analyze

□ Step 2 – Plan

□ 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 LMS platform will you be using to deliver your training and/or phishing simulations?

....

Will you purchase or develop awareness content?

□ Purchase □ Develop

Will you require awareness material (e.g. posters, mousepads, hand-outs)?

□ Yes □ No

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?

....

Taking the time to plan your resources, time and budget upfront really matters. Knowing what you need and what is available to you will allow you to make informed decisions about product choice, what is feasible to do on your own and where you need support resources and external professional services.

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

1. Strategic Program Goals
2. Compliance
3. Target Audiences
4. Scope (Topics)
5. Level of Knowledge
6. Motivation and Culture
7. Support Resources
8. Globalization
9. Costs (Resources)

Ready to start *Step 2 – Plan?*
Let's do it!

STEP 2 – PLAN

1	*2*	*3*	*4*	*5*
Analyze	*Plan*	*Deploy*	*Measure*	*Optimize*
○	●	○	○	○

By taking the time to plan properly and work out the fine details,
you are putting success on your side.

Welcome to *STEP 2 – PLAN* of the *Terranova Security Awareness 5-Step Framework.*

Now that you have completed ***Step 1 – Analyze***, you are ready to embark on ***Step 2 – Plan*** of the ***Terranova Security Awareness 5-Step Framework***. You will use the data you gathered in your analysis to plan your security awareness campaigns.

Failing to plan is planning to fail.

— Benjamin Franklin

This is probably my all-time favorite mantra. I would much rather put in the time to plan than revisit what went wrong later. It's amazing to me how so many people have no time to plan, yet they have plenty of time to do things over again to correct what didn't work.

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

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

Planning allows you to:

- Meet contractual obligations
- Anticipate and address roadblocks
- Stay aligned with your goals and objectives
- Stick to your timelines
- Stay within your budget
- Be better set up for success

PLANNING PAYS OFF

A goal without a plan is just a wish.

— Antoine de Saint-Exupéry

Planning takes time. That's a fact. Initially, it may seem like a lot of your energy and resources are being spent on details. Until, that is, the time comes for you to deploy your security awareness program.

When you are well prepared, your deployment runs smoothly. You deliver a more solid program—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.

➔ ***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.***

PARETO PRINCIPLE: THE 80/20 RULE

20% Effort
80% Results

Perhaps you have heard of the *Pareto Principle,* also known as the 80/20 rule, named after the late 19th-century Italian economist Vilfredo Pareto. It originally referred to the fact that 80% of Italy's wealth belonged to only 20% of its population.

Today, the 80/20 axiom is applied to many things. In business management, it suggests that 80% of your results can be attributed to 20% of your effort. This is especially important to keep in mind during your planning activities. Know where and how to prioritize. Refer back to your answers in ***Step 1 – Analyze*** to make sure the awareness initiatives you plan are aligned with your goals. This is key because the opposite is also true: if you spend 80% of your efforts on non-essential activities, you will only achieve 20% of your goals.

Where should you focus your efforts?

Sometimes the tasks that are of high value are the most daunting and difficult, but they also yield the greatest rewards. In the ***Terranova Security Awareness 5-Step Framework***, we have created everything you will need, so you stay focused on the important details. Efficiency and productivity are the very reason why we developed the ***Terranova Security Awareness 5-Step Framework***—and why I wrote this book!

➔ ***Planning keeps you on track to get 80% of your desired results with 20% of your effort!***

PLANNING TO SUCCEED

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

In ***Step 1 – Analyze*** you defined the "why", and in the following pages you will define the "who, what, when and how"—the logistics of your security awareness program.

In ***Step 2 - Plan***, you will make decisions focused on the following 6 key elements:

1. **Team**
   - Identify who will be on your security awareness team. What are the required skills, roles and responsibilities of each member?
2. **Roadmap**
   - Define your strategy.
   - Plan your campaigns per audience and timeframe.
   - Plan your activities per campaign.
3. **Product**
   - Select and customize your content: online training courses, live presentations and reinforcement tools.
   - Select and customize your measurement tools: LMS, phishing simulations, vulnerability assessments, surveys and quizzes.
4. **KPIs and metrics**
   - Define KPIs and metrics in relation to each campaign's objectives so you can measure your results against those baselines to optimize the next wave of your program based on measurable results.
5. **Communication**
   - Prepare and approve in advance the communication plan you will use throughout your program and various campaigns.
   - Create your communications calendar.
   - Select and customize your communication materials.
6. **Program presentation**
   - Create a presentation for senior executives, team members or stakeholders highlighting the main elements of your security awareness program and communication strategies.

EXERCISE 2.0

STARTING STEP 2 – PLAN

Take some time now to review all the answers you provided in ***Step 1 – Analyze*** (your cheat sheet). Your original answers will surely have changed following your analysis. Write down the more important answers here on this cheat sheet and refer back to it while planning out the six key ***Plan*** elements listed on the previous page.

1. Goals

....

....

....

....

2. Compliance obligations

....

....

....

....

3. Target audiences

....

....

....

....

4. The scope of your program – the topics

....

....

....

....

5. **Knowledge gaps**

6. **Motivation levels**

7. **Your support resources**

8. **Globalization**

9. **Your costs – Your budget**

1. BUILDING YOUR TEAM

Now it's time to build your team and get the right resources on board. I cannot stress enough the importance of surrounding yourself with an amazing team. Everyone should bring something of value to the table and help create a synergy that moves your security awareness program forward. And I speak from first-hand experience—I truly believe the success of Terranova is due in large part to the team we have built together.

It's time to start naming names!

On page 72 in ***Step 1 – Analyze***, I talked about the categories of support resources you may need (e.g. upper management support, security awareness champions and operational support). Now, you will put together a team of actual people for these categories.

Who will be on your team?

You will need the skill set 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.

➔ ***Reach out beyond security and IT to build your dream team.***

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

Most importantly, choose team members who are enthusiastic. Seek out those who you discovered are "intrinsically motivated," when you sent out motivation surveys, as suggested in ***Step 1 – Analyze***, page 67.

Roles and responsibilities

Team members will provide unique perspectives based on their own expertise. It's like the old saying goes "two heads are better than one."

> *Few entrepreneurs — scratch that, almost no one — ever achieved anything worthwhile without help. To be successful in business, you need to connect and collaborate and delegate.*
>
> — Sir Richard Branson

PROGRAM SPONSOR

Program sponsor

The **program sponsor** is the spokesperson for the security awareness program. He or she is most likely a senior executive (i.e. upper management) who may not be involved in operational activities, but who participants will recognize and support. See more on page 73 in ***Step 1 – Analyze.***

Responsibilities include:

- Liaising with upper management
- Keeping decision-makers informed
- Securing funds
- Choosing the project manager/coordinator

PM COORDINATOR

Project manager/coordinator

Although **project manager/coordinator** may not be a full-time position, security awareness activities should be a major part of this person's day-to-day activities to ensure your program is successful.

Responsibilities include:

- Building the security awareness team
- Defining, planning, and managing the program
- Overseeing preparation of awareness content
- Coordinating campaign deployment
- Gathering and interpreting program/campaign metrics
- Reporting results to the program sponsor

COMMUNICATION ADVISOR

Communications advisor

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

Responsibilities include:

- Outlining change management strategies
- Defining the communication strategy

- Drafting memos and emails
- Establishing the communication calendar
- Sharing lessons learned from other organization-wide campaigns

Subject matter experts (SMEs)

SMEs (subject matter experts) may come from the security team or other departments, depending on the campaign topics.

Responsibilities include:

- Reviewing awareness material
- Providing guidance on topic selection
- Developing/customizing online courses and reinforcement tools

IT/LMS administrator

The **IT/LMS administrator** supports the implementation of the technical components of your security awareness program.

Responsibilities include:

- Configuring and administering the learning management system (LMS)
- Obtaining up-to-date lists of participants
- Setting up LMS Single-Sign On (SSO) functionality
- Participating in functional testing
- 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 play a role in the support of the overall program.

Responsibilities include:

- Acting as awareness ambassadors
- Providing end-user support
- Gathering metrics data
- Reviewing content customization and translation, as well as geographical nuances, for campaigns in multiple countries and/or in multiple languages

EXERCISE 2.1.

BUILDING YOUR TEAM

The time to put your team together is now, before you proceed with any more planning because you will want input from all team members as you make decisions on key factors such as timelines, program content and communication strategies.

Fill out the following worksheet, specifying the names of those who you believe have the right skills and attitudes to make your security awareness program a success.

People who work for your organization

□ **Program sponsor(s)**

Specify ....

....

....

....

□ **PM/coordinator(s)**

Specify ....

....

....

....

□ **Communications advisor(s)**

Specify ....

....

....

....

□ **Subject matter expert(s) (SMEs)**

Specify ....

....

....

....

□ **IT/LMS administrator(s)**

Specify ....

....

....

....

□ **Additional contributor(s)**

Specify ....

....

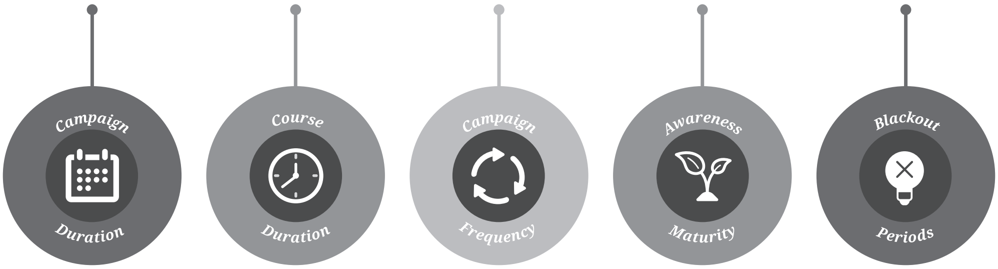
....

....

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. Often they can supplement your internal security awareness team and help ensure the success of your security awareness program.

2. DEFINING YOUR ROADMAP



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

This is not a complex task, but it does require a strategy and some planning since each unique campaign will include specific activities to be carried out at specific times.

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***.

- A learning module can be distributed to one or all of your target audiences, depending on its relevance to them.
- Each security awareness module is released according to an established schedule.

Your campaigns will include 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. newsletter, posters, videos) are used between campaigns to reiterate key messages and keep information security top of mind.

- You will release your reinforcement tools according to an established schedule.

You will use several defined performance metrics to measure the success of a given security awareness campaign. This will allow you to evaluate the campaign's performance against the campaign objectives you defined and to make adjustments 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 need to be mindful of the overall impact and time demands your program will have on both 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 timeframe 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 to any decision makers whose approval and support you need for your security awareness program.

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

1. **Program duration**
2. **Campaign frequency**
3. **Campaign duration**
4. **Course duration**
5. **Awareness maturity**
6. **Blackout periods**
7. **Pre-launch testing**

1. Program duration

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

- Is training mandatory or optional? If mandatory, you can impose a deadlines. If optional, you may provide a longer timeframe 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 of time, 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-sized content so that users can retain the information. If releasing one module per month is too much for your resources, consider releasing modules less frequently to a larger group of people.

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

2. Campaign frequency

How often will you carry out online awareness training?

- Yearly?
- Bi-annually?
- Quarterly?
- Monthly?

Increasing campaign frequency has many benefits:

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

However, increasing campaign frequency also has some drawbacks and may:

- Place a strain on your security awareness team and resources.
- Risk over-soliciting participants, which will cause them to lose interest.
- Require more time between campaigns for making adjustments following pilot testing.
- You may not be able to adapt your strategy between campaigns.

3. Campaign duration

Depending on the campaign frequency, you will decide how long each ***campaign*** should last. Use the following recommendations as a general guideline:

Ex: Frequency of one campaign per month or every two months:

Your campaign should last between 4 to 8 weeks:

- 2 to 4 weeks allocated for participants to complete the online training
- 2 to 4 weeks for communications, before and after the training period

The duration of other types of security awareness campaigns will vary. For example:

- **Phishing campaign**: 1 week (simulation, just-in-time training, results)
- **Awareness week**: 1 week (security booth, daily lunch-and-learns)
- **Awareness month**: 1 month (posters, videos, games, newsletters, micro-learning)

If your campaign is too short, you may not create the desired impact. Participation rates may end up being low and you may be less likely to see any reduction in risky behaviors.

If it is too long, you may not be able to keep the momentum going. The decision on duration is often made based on past experiences and the organizational culture.

4. Course duration

How many modules will you include in your course? Use the following recommendations as a general guideline:

Depending on the frequency of the campaign, the topics and your participants, you may decide to launch:

- 1 or 2 key topics per month totaling 3 to 5 minutes
- 3 to 6 key topics per quarter totaling 15 to 30 minutes
- For millennials and people on the move, we often recommend short courses such as micro-learning modules that last 2 to 3 minutes.

(See page 95 for more about campaign and course duration.)

5. Awareness maturity

Earlier in the book, I introduced ***security awareness program maturity***, which referred to the thoroughness of developing your security awareness program (see page 33). You must also consider ***awareness maturity***, meaning the ***level of knowledge and experience*** of the people in your organization and of your security awareness team.

- 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?

➔ ***Depending on your own 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.***

6. Blackout periods

Are there times when you should not plan awareness activities?

Yes, when it may be difficult to reach your target audience.

Common blackout periods include:

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

By the same token, it would be clever to plan campaigns to coincide with events such as National Cybersecurity Awareness Month.

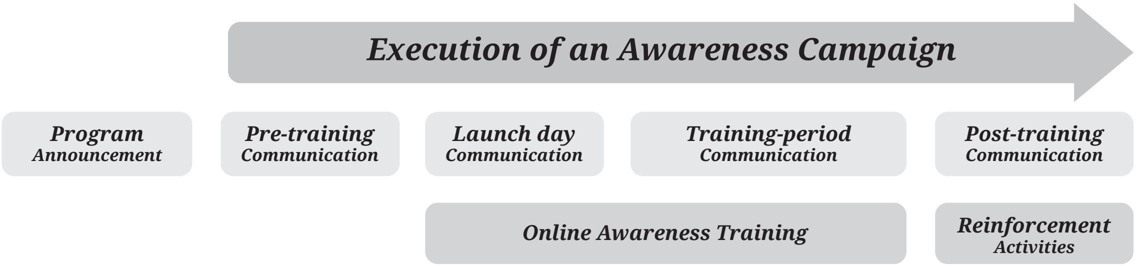
Important: *You must also give yourself enough time to measure campaign success and implement an action plan if objectives and goals are not met. We will look at those aspects in* ***Step 4 – Measure*** *and* ***Step 5 – Optimize*** *later in this book.*

7. Pre-launch testing

Before you launch your program and individual campaigns, you will need to conduct pre-testing to make sure everything will run smoothly on launch day.

Factor in time for content review, compatibility and performance testing of your IT systems and a general pilot test of your actual campaign. I explain in greater detail what each of these tests entails on page 130 in ***Step 3 – Deploy.***

➔ ***Leave enough time in your project plan to conduct your testing—and to make any necessary adjustments.***


Execution of an Awareness Campaign
Program Announcement
Pre-training Communication
Launch day Communication
Training-period Communication
Post-training Communication
Online Awareness Training
Reinforcement Activities

EXERCISE 2.2.

DEFINING YOUR ROAD MAP: CONSIDERATIONS

Planning a security awareness program can be lengthy and complex. Doing the proper groundwork and asking all the right questions will allow you to start planning 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. This will give you a good overview of the time you will need to allocate.

PROGRAM DURATION

How long should your program last?

CAMPAIGN FREQUENCY

How often will you carry out online training?

- □ Yearly
- □ Bi-annually
- □ Quarterly
- □ Monthly

Considerations

CAMPAIGN DURATION

How long should each program campaign last?

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?
(See page 97 on ideal course duration.)

AWARENESS MATURITY

Have participants ever completed security awareness training in the past?

□ Yes □ No

If yes, please specify

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

□ Yes □ No

If yes, please specify

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

BLACKOUT PERIODS

Are there times when you should not plan awareness activities?

□ Yes □ No

If yes, what are they?

....

....

....

PRE-LAUNCH TESTING (see page 131 for more explanation)

How much time will you allocate for:

Content review

Testing ....

Adjustments ....

Compatibility and performance testing of your platforms

Testing ....

Adjustments ....

Pilot testing

Testing ....

Adjustments ....

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

3. SELECTING YOUR PRODUCTS

So now the question is… what content will you include in your program in general and in each of your campaigns? Will you purchase products that are 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.

1. Selecting and customizing your content

A. Online training courses

B. Live presentations

C. Reinforcement tools

2. Selecting and customizing your measurement tools

A. LMS

B. Phishing simulations

C. Vulnerability assessments

D. Surveys and quizzes

1. Selecting and customizing your content

Your next round of planning decisions is focused on the content you want to include in each program campaign. To make your selection, you must consider a number of variables, including your participants' motivation, your organization's culture, your training budget and your capacity to implement and distribute the content in its various forms.

Variables to consider when selecting your security awareness program content

1. Strategic Program Goals
2. Compliance
3. Target Audiences
4. Scope (Topics)
5. Level of Knowledge
6. Motivation and Culture
7. Support Resources
8. Globalization
9. Costs (Resources)

Refer to your revised answers in your Step 1 – Analyze exercises or to your Step 1 – Analyze Cheat Sheet on page 42.

Decisions, decisions

For the longest time, when we heard the word *hacker*, we pictured a disheveled loner living in a basement apartment, fooling around on a computer.

Not anymore.

Today, we know cyber criminals are sophisticated, calculating and very, very good at their chosen profession. What is their job? Whether they are self-employed, a free agent or the employee of a nation-state or organized crime network, their job is to find ways to access your confidential data. They are using new strategies, tools and tactics to hit you in your most vulnerable spot: your people, the weakest link.

The scope and creativity of the evolving cybercrime landscape is mind-numbing.

➔ ***You must deal with cybercrime on all fronts, but where do you start?***

How do you prioritize your training content?

What kind of security awareness training do you initially offer your participants?

A lot of organizations don't know where to start. You may be saying to yourself, "Okay, I am going to begin with a 15-minute courses… three or four topics… but which topics do I pick first? Which ones are most important?"

That was precisely the case with one of our clients, a well-established media company with 5000 employees, most of whom are knowledge workers.

This company asked Terranova to build a solid plan for its first-ever security awareness program. During one of our key consultation meetings, the Director of Information Security shared the topics he wanted to include. As he spoke, his opinion changed, he sounded unsure and debated how his program would take shape.

"I have identified 25 topics to cover, but there's no way I can communicate everything at once. Maybe I should start with passwords… no maybe information classification…"

Our Professional Services consultant gently interrupted him and suggested: "Let's look at your real-world situation together."

The client and the Terranova team went back to the basics in ***Step 1 – Analyze***. We needed to assess their employees' level of knowledge and did so using three information sources (see page 60 for a broader explanation):

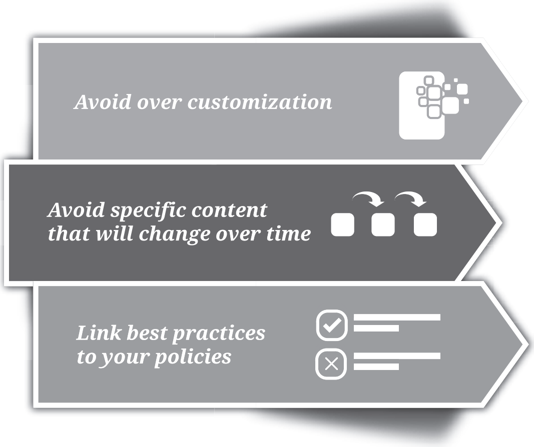
- Quizzes and surveys
- Phishing simulations
- Risk analysis reports and incident reports

First, we conducted a survey to measure the current level of security knowledge among their employees. Next, we studied the company's reports related to their information security issues, and then asked all the important questions: Were there any security incidents targeting employees such as virus infections or social engineering scams? Did any employees fall for these scams? We also deployed a phishing simulation to see if we needed to include phishing training in the program.

After reviewing the results, we were able to go back to the client with a comprehensive list of potential content, prioritizing topics based on internal weaknesses. "In your case, your employees are strong with passwords, so we can address that later in the program. However, they are clearly more vulnerable to social engineering, so we will start with appropriate training to address that pain point."

In short, together we prioritized the high-risk topics and built a security awareness program that took into account what was happening in their organization and what was happening globally in terms of cyberattacks and security risks. It was a sensible, practical approach that took the guesswork out of their topic prioritization.

Customizing your content


Avoid over customization
Avoid specific content that will change over time
Link best practices to your policies

Customization is a very powerful capability when it comes to communications. Essentially, it involves working with a template template and adding elements that make your content more engaging and relatable—and get people more motivated to participate.

Course customizations can include delete:

- 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 over customization

When you build a program for the first time, make sure that your *subject matter experts* (SMEs) do not cover too much information in a single course.

Your goal is to turn participants into security advocates. You don't need them to be security 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, it is best *not* to provide the email and extension number of a particular contact person at your organization—that person may get a promotion or move to a different department. Their contact information may then change. Instead, provide a general point of contact such as your helpdesk. Better yet, create a generic INFOSEC inbox to collect and consolidate all participant feedback, questions and concerns.

3. Link best practices training to your policies

Including your organization’s policy statements in the best practices section of your course is an effective way to reinforce acceptable uses of technology. 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. The assortment of awareness tools available to you have varying degrees of impact depending on the context and the target audience.

Below is a list of ways you can communicate your security awareness message and content:

A. Online training courses

B. Live presentations

C. Reinforcement tools

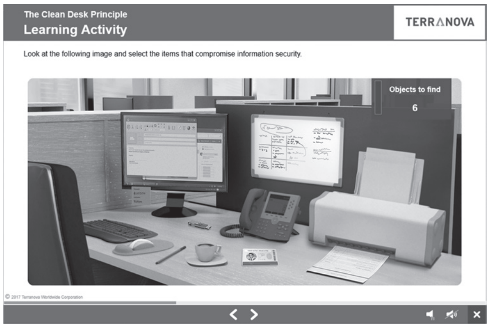
A. Online training courses

There is a learning theory which suggests that the more human senses are involved in the learning process, the more the information will be retained. Seeing, hearing, and touching the information helps it to sink in—and **interactive** online training courses certainly have those visual, auditory and tactile properties.

Online awareness training courses are effective tools for communicating knowledge and best practices with the goal of changing human behavior. They are typically available in various forms and lengths, ranging from 3-minute micro-learnings to 20-minute courses. You should use course content with interactive instructional exercises, games, quizzes and evaluations to enhance the learning experience. (See page 108 for more on recommended lengths.)

Target audiences

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 their role and responsibilities.



The Clean Desk Principle

Learning Activity

TERRANOVA

Look at the following image and select the items that compromise information security.

© 2017 Terranova Worldwide Corporation

In-house target audiences

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

** 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

Advantages

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

Online training considerations

> As you plan and prepare to roll out your online training course,
> you will have to make decisions about certain functional aspects of the training:
>
> a. Mandatory vs voluntary participation
> b. Evaluation and passing grade
> c. Course duration and frequency

a. Mandatory vs 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
- Increase the likelihood of meeting compliance obligations

➔ ***Make sure there are no union or labor contracts that would prevent your training from being mandatory. You may consider having a mix of mandatory and voluntary topics, depending on the situation.***

b. Evaluation and passing grade

Deciding whether to add a test at the end of your online training is an important consideration. If you choose to include a test, you must set a passing grade. Such decisions must be in keeping with the culture of your organization. Also, make sure there are no union or labor contracts that would prevent 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 simply take the test again?

You must also consider how you plan to measure your program's effectiveness.

c. Course duration and frequency

When rolling out an online course, it is important not to include too much content all at once. You might end up overwhelming the participants and they may not be able to absorb the key knowledge, acquire new skills and adopt desired behaviors.

The duration of the modules within a campaign should be aligned with your organization's culture and operations. For example, let's say you are a retail company and you need to train your sales associates. These employees are typically on the sales floor, interacting directly with customers, and do not have a dedicated computer. Therefore, you may have to approach their training in a different way. You could ask them to leave the sales floor for a very short period of time 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 are training your remote salesforce and they have a semiannual sales meeting scheduled, that might be the right time for them to do a longer training session as part of their sales meeting agenda.

- Ideally, a campaign should not cover more than 3 to 6 key topics in 15 to 30 minutes, maximum, with each topic lasting approximately 5 minutes.
- You could also launch:
    - 1 topic per month
    - 3 topics per quarter
    - 1 course per year
- We often recommend using micro-learning modules — bite-sized courses that last 2 to 3 minutes.

Sometimes, delivering shorter courses at more frequent intervals is the way to go with millennials or with participants who are on the move and not necessarily sitting in front of a computer screen all the time.

> 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.

EXERCISE 2.3.

ONLINE TRAINING CONSIDERATIONS

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

1. **Is participation in the training mandatory?**

   □ Yes □ No

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

   ....

   ....

   ....

   ....

2. **Will you impose a passing grade?**

   □ Yes □ No

   If yes, please specify and note any special considerations.

   ....

   ....

   ....

   ....

3. **Do all your different target audiences have a dedicated computer?**

   □ Yes □ No

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

   ....

   ....

   ....

   ....

4. **How long should your courses be and how often will you distribute them?**

□ One campaign per year: training from 30 to 45 minutes each
□ Multiple campaigns per year: training from 3 to 20 minutes each

Note any special considerations.

5. **What about training for new employees? Will they:**

□ Start with a course or campaign that is currently under way
□ Start your program from the beginning
□ Receive a custom program for new hires that includes all the security essentials

Note any special considerations.

TIPS FOR EFFECTIVE SECURITY AWARENESS CONTENT

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

B. Live presentations

Offering an online course to certain audiences, such as executives or senior managers, may not be the most effective approach. Live presentations are a better option in such 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 and 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

Target audiences

- Executives
- Senior managers

Advantages

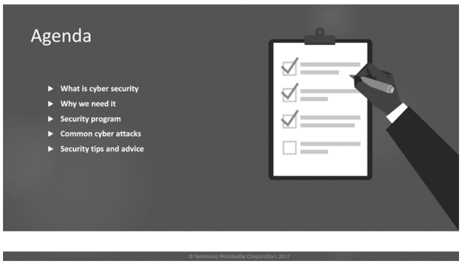
- They are short (15 to 20 minutes), but long enough to cover the specific awareness concerns of this particular audience (e.g. threats and relevant news stories).
- Executives—who tend to be very busy—are more likely to make time for a short presentation rather than complete online awareness training.
- You can add your presentation to the agenda of a meeting that is already scheduled.

C. Reinforcement tools

After you launch 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 and posters are just a few ways you can 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



Agenda

- What is cyber security
- Why we need it
- Security program
- Common cyber attacks
- Security tips and advice

© Terranova Worldwide Corporation, 2017

Advantages

- Reinforcement tools are used to send the message home, keeping security awareness top of mind so that the people at your organization change their behaviors and make information security a priority.
- With so many media channels at your disposal, you can reach your target audiences in so many different ways, and in so many different 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 micro-modules are great for highlighting and reinforcing best practices related to a specific risk or threat.

2. Selecting and customizing your measurement tools

What are measurement tools, exactly? Well, they are any of a variety of mechanisms that provide you with information to assess the effectiveness of your campaigns. Such tools are important to have in place because they give you insights, as well as 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.

Below is a list of powerful measurement tools we recommend for every security awareness campaign:

A. LMS (Learning management system)

B. Phishing simulations

C. Vulnerability assessments

D. Surveys and quizzes

A. Learning management system (LMS)

The LMS you use in your campaigns will allow you to measure online training participation rates and determine the percentage of users who have completed the courses successfully.

As I have discussed throughout this book (in particular on page 16), you have to define objectives and metrics and produce reports on your program's performance to make sure you are reaching your campaign objectives and your strategic program goals. You can produce actual reports using the LMS by configuring it to collect data related to user participation.

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

B. Phishing simulations

Phishing simulations are a great tool to measure your organization's ability to recognize and deal with cybersecurity threats.

Note: Phishing simulations should not include third-party target audiences without their approval.

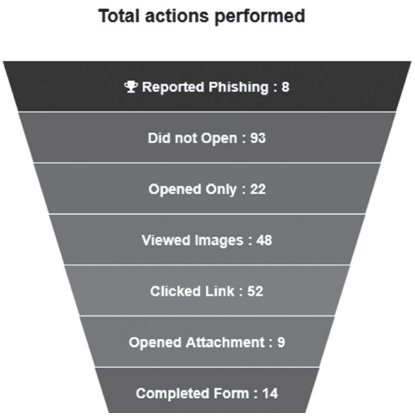
Target audiences

- 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.
- They can be used before and after awareness training to determine the effectiveness of training.
- They can be enhanced with just-in-time training to build a comprehensive phishing awareness program.
- They can be used with real-time reporting and dashboards (when used with a phishing platform).

Phishing simulation considerations



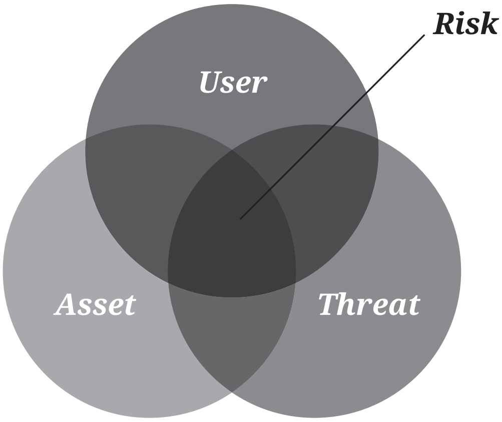
When preparing a phishing simulation, it is important to do the following:

- Clearly define the strategy, as well as the lines of communication, before launching.
- Inform all stakeholders concerned that they will be notified when you conduct a phishing test.
- Avoid sending messages alphabetically if you opt for a gradual deployment. If they seem to be in some sort of order, participants may realize it is a test.
- Perform a validation and clean-up of email addresses prior to the simulation.
- Participants who detect phishing may report it as real. Therefore, establish a response mechanism for the security team.
- After a phishing simulation, 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.
- Phishing simulation can be used to deliver just-in-time training for users who fail to detect the threat.
- Consider local laws and regulations related to phishing users.

C. Vulnerability assessments

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

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



Target audiences

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

Advantages

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

D. Surveys and quizzes

Surveys, assessments and quizzes are great measurement tools both before and after your security awareness program.

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

- Keep quizzes short (10 to 15 questions)
- Provide feedback with each question answered when quizzes are used as awareness tools
- Withhold feedback when quizzes are used as evaluations to assess the awareness levels of your organization

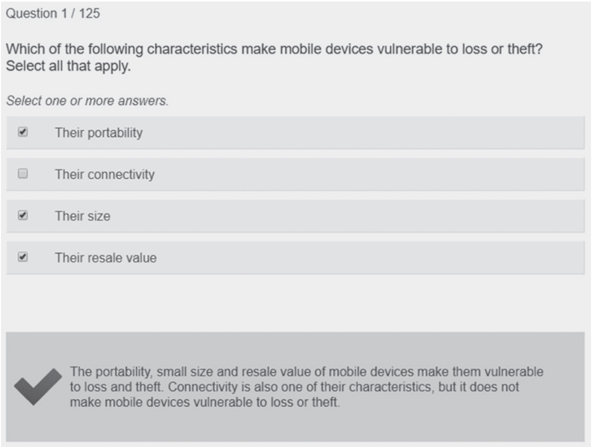
Target audiences

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

Advantages

- They provide a means to measure current levels of awareness.
- They allow you to prioritize awareness topics.
- You can give participants the choice to opt out of online training if they pass the pre-training evaluation.
- You are able to measure overall gains and knowledge retention (as a pre- and post-training assessment).

SURVEY EXAMPLE



Question 1 / 125

Which of the following characteristics make mobile devices vulnerable to loss or theft? Select all that apply.

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.

4. DEFINING YOUR KEY PERFORMANCE INDICATORS (KPIs) AND METRICS

In your planning phase, once you have selected your content and campaign objectives, the next task is to define your key performance indicators (KPIs) and metrics.

In fact, 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 important insights into its effectiveness. This will be discussed further in the ***Step 4 – Measure*** section of this book.

Your metrics should be aligned with your program goals and campaign objectives.

For example, you might track course enrollment, course completion details, phishing simulation results and other indicators in order to determine whether the target audience is meeting 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
- These metrics can actually be captured
- These metrics are understandable by those to whom you will present your findings
- Frequency for publishing your metrics has been agreed upon with your security awareness team

Common metrics

Awareness measures fall into 5 different categories, each providing specific insights into your program or campaign:

1. **Training statistics**
2. **Participant satisfaction**
3. **Training effectiveness**
4. **Return on investment (ROI)**
5. **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
Return on investment (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	**Other metrics:** ▪ Office chatter 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

EXERCISE 2.4.

DEFINING YOUR METRICS

Campaign 1: ....

Objective 1: ....

Metric 1: ....

Collection method: ....

Metric 2: ....

Collection method: ....

Metric 3: ....

Collection method: ....

Objective 2: ....

Metric 1: ....

Collection method: ....

Metric 2: ....

Collection method: ....

Metric 3: ....

Collection method: ....

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.

5. CREATING YOUR COMMUNICATION PLAN

A security awareness campaign is much more successful when it is supported by a smart communication plan. Your communications must advertise your campaign to target audiences at strategic moments to keep your security awareness campaign top of mind. 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

Consistency is also important, as it will help brand your campaign and establish a relationship with your target audiences.

A communication plan has two components:

A. Communication strategy

B. 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.

A. Communication strategy

Your communication strategy must identify the following:

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

Effective communications

What are you going to say about your security awareness program, and why? What do you want your target audiences to do? Is your message clear? Will they interpret what you are saying the way you intended? Will they act?

Effective communications require facts, knowledge and an understanding of your organization's culture. You should look back in ***Step 1 – Analyze*** at the description of your target audiences, their motivation levels and the suggested topics for inspiration on how you are going to talk to them (i.e. tone, level of language, topics).

Involve your security awareness team and co-workers 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!

Getting people on board and motivated to participate in your security awareness program is sometimes a challenge, so you have to get a little creative. One of our clients, a North American medical supplies company, created a series of YouTube videos to announce the program. Who can resist watching a fun company video?

Another client, a dairy company in the Asia-Pacific, used a different strategy. To demonstrate corporate support of the program, the executives personally announced the program to the employees, using an empowering message. They needed to change the perception of information security as **only** an IT Security issue. The executives, instead, talked about the value of the company's workforce, the employees' contribution to its longevity and their role in keeping it safe and protected from attacks.

TIPS:

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

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

EXERCISE 2.5.

CREATING YOUR COMMUNICATION PLAN

Start planning out the logistics of your communications by completing this worksheet.

Who is responsible for drafting and/or signing memos, emails, etc.?

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)

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:

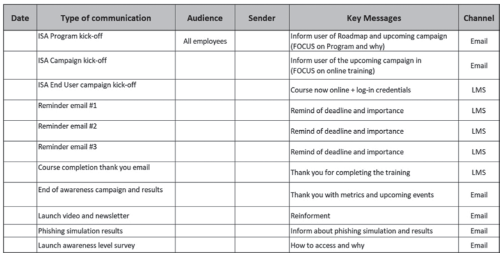
Be part of the solution. Let's prevent security breaches. Participate in our organization's awareness training today!

B. Communication calendar

Your communication calendar should include details about every communication activity involved in each of your campaigns, even if the communication strategy is the same for all. Anticipate any challenges that may arise if your organization has multiple sites, remote users and multiple languages, etc.

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 the upcoming campaign in (FOCUS on online training)	Email
	ISA End User campaign kick-off			Course now online + log-in 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			Reinforment	Email
	Phishing simulation results			Inform about phishing simulation and results	Email
	Launch awareness level survey			How to access and why	Email

Making sure your message gets across

Times to communicate

a. Pre-training

b. Campaign launch

c. During online training

d. Post-training

Pre-Training
Campaign Launch
Online Training
Post-Training
Creative and Impactful

a. Pre-training communications

Pre-training communications are used to:

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

I usually suggest sending out the **program announcement** once (or yearly), which should be signed by your security awareness sponsor (see page 73). Subsequently, a **campaign announcement** should be sent for each separate campaign.

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

b. Campaign launch communications

Campaign launch communications are:

- Used to officially launch the security awareness campaign
- Usually sent 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

c. Online training communications

A common mistake is to launch a campaign and not send out any other communications afterward. Online training communications are designed to boost participation and keep the momentum strong following the campaign launch.

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

d. Post-training communications

Post-training communications are used to:

- Officially inform your target audiences that the campaign has ended
- Publish campaign results
- Announce the next campaign

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

Creative and impactful communications

COMMUNICATION TIPS:

If you limit your communications to your campaign launch, you may see low participation rates. A key to your success is to communicate at strategic moments—and to keep your messaging engaging.

- The campaign's launch communication should inform participants about how to access the online training, the completion deadline and who to contact for support.
- Provide information about why security is important, and why a security awareness program is being implemented.
- The topics covered in the online training should be presented prior to the campaign launch, in a separate communication.
- Plan for consistency, flow and branding in your communications. For example, a 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 have the unit that will provide support as the signatory.

➔ ***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:

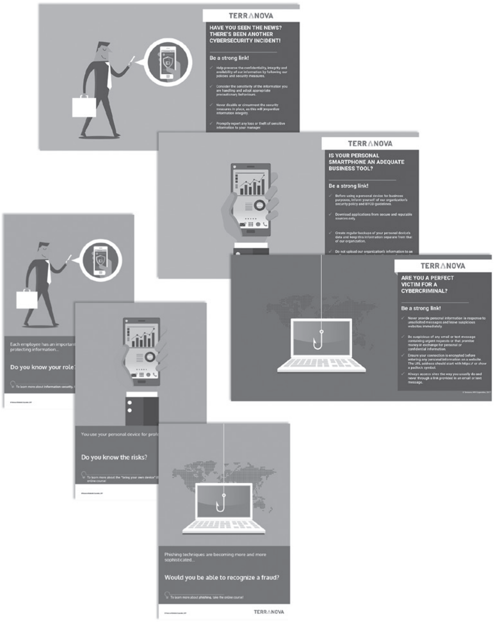
- highlight security best practices
- reinforce your overall messaging
- maximize the visibility of your security awareness program

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 important knowledge (e.g. newsletters)
- Reinforce knowledge (e.g. micro-learning) about a specific risk, threat or best practice



TERRANOVA

HAVE YOU SEEN THE NEWS? THERE'S BEEN ANOTHER CYBERSECURITY INCIDENT!

Be a strong link!

- ✓ Help preserve the confidentiality, integrity and availability of our information by following our policies and security measures.
- ✓ Consider the sensitivity of the information you are handling and adopt appropriate precautionary behaviours.
- ✓ Never disable or circumvent the security measures in place, as this will jeopardize information integrity.
- ✓ Promptly report any loss or theft of sensitive information to your manager.

TERRANOVA

IS YOUR PERSONAL SMARTPHONE AN ADEQUATE BUSINESS TOOL?

Be a strong link!

- ✓ Before using a personal device for business purposes, inform yourself of our organization's security policy and BYOD guidelines.
- ✓ Download applications from secure and reputable sources only.
- ✓ Create regular backups of your personal device's data and keep this information separate from that of our organization.
- ✓ Do not upload our organization's information to an

TERRANOVA

ARE YOU A PERFECT VICTIM FOR A CYBERCRIMINAL?

Be a strong link!

- ✓ Never provide personal information in response to unsolicited messages and leave suspicious websites immediately.
- ✓ Be suspicious of any email or text message containing urgent requests or that promise money in exchange for personal or confidential information.
- ✓ Ensure your connection is encrypted before entering any personal information on a website. The URL address should start with https:// or show a padlock symbol.
- ✓ Always access sites the way you usually do and never through a link provided in an email or text message.

Each employee has an importan
protecting information...

Do you know your role

To learn more about information security,

You use your personal device for prof

Do you know the risks?

To learn more about the "bring your own device"
online course!

Phishing techniques are becoming more and more sophisticated...

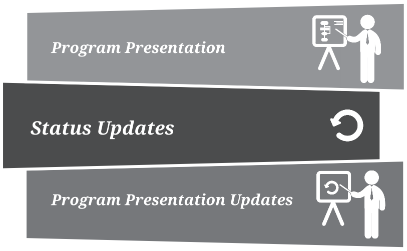
Would you be able to recognize a fraud?

To learn more about phishing, take the online course!

TERRANOVA

6. CREATING YOUR SECURITY AWARENESS PROGRAM PRESENTATION

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



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

Your target audience for this presentation could be a security governance committee, members of the security awareness team or any stakeholders who need to be informed of awareness initiatives.

➔ ***If you need to add supporting arguments for your program to your presentation, see pages 18 and 19 in the Preface of this book. I provide a full discussion on 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 is one that tells a compelling story, is easy to understand and 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:

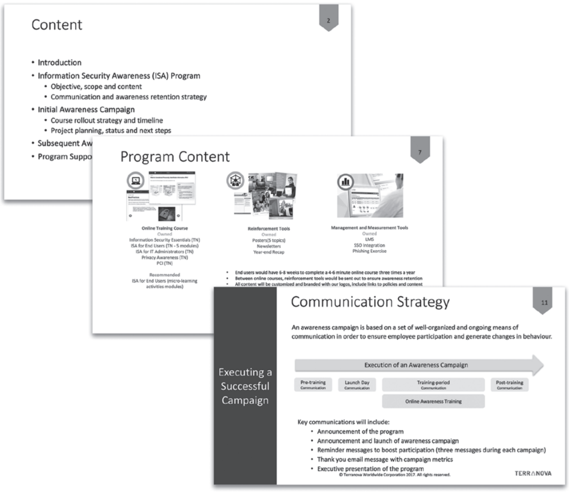
- Project milestones, timeframes and current status
- Campaign results, lessons learned and an action plan to deal with shortcomings

Program presentation updates

Your program presentation should be updated at least once a year, but preferably after each major security awareness campaign and before each stakeholder meeting.

Since the program presentation is a strategic document, it is best to limit your information to the main strategies and milestones. Using graphics to illustrate your points is very helpful.

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



Content

2

- Introduction
- Information Security Awareness (ISA) Program
  - Objective, scope and content
  - Communication and awareness retention strategy
- Initial Awareness Campaign
  - Course rollout strategy and timeline
  - Project planning, status and next steps
- Subsequent Aw
- Program Suppo

Program Content

7

Online Training Course
Owned
Information Security Essentials (TN)
ISA for End Users (TN - 5 modules)
ISA for IT Administrators (TN)
Privacy Awareness (TN)
PCI (TN)

Recommended
ISA for End Users (micro-learning activities modules)

Reinforcement Tools
Owned
Posters(5 topics)
Newsletters
Year-end Recap

Management and Measurement Tools
Owned
LMS
SSO Integration
Phishing Exercise

- End users would have 6-8 weeks to complete a 4-6 minute online course three times a year
- Between online courses, reinforcement tools would be sent out to ensure awareness retention
- All content will be customized and branded with our logos, include links to policies and content

Executing a Successful Campaign

Communication Strategy

11

An awareness campaign is based on a set of well-organized and ongoing means of communication in order to ensure employee participation and generate changes in behaviour.

Execution of an Awareness Campaign

Pre-training Communication

Launch Day Communication

Training-period Communication

Online Awareness Training

Post-training Communication

Key communications will include:

- Announcement of the program
- Announcement and launch of awareness campaign
- Reminder messages to boost participation (three messages during each campaign)
- Thank you email message with campaign metrics
- Executive presentation of the program

© Terranova Worldwide Corporation 2017. All rights reserved.

TERRANOVA

CONGRATULATIONS!

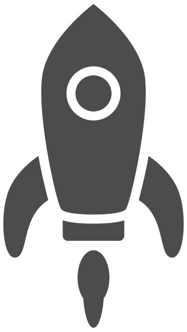
You have just completed ***Step 2 - PLAN*** of the ***Terranova Security Awareness 5-Step Framework.***

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

PLAN CATEGORIES

1. Team
2. Roadmap
3. Product
4. KPIs and Metrics
5. Communication
6. Program Presentation

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



STEP 3 – DEPLOY

1	2	3	4	5
Analyze	*Plan*	*Deploy*	*Measure*	*Optimize*
○	○	●	○	○

Everything you have completed so far is preparing you for an effective launch.

Welcome to *STEP 3 – DEPLOY* of the *Terranova Security Awareness 5-Step Framework.*

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

➔ ***Just before your kickoff, you need to do some pre-testing to make sure the campaign runs smoothly. You will need to follow up with a reinforcement phase both during and after your deployment, so you are better positioned to reach the security awareness campaign objectives you have set.***

Preparing for deployment

YOU SHOULD ALWAYS DEPLOY YOUR CAMPAIGNS IN 3 PHASES:

1. 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.

2. Launch

- Launch the campaign and communicate with employees.

3. Reinforce

- 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

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 important deployment details
- To validate the flow and customization of content
- To improve your probability of success

Making time for testing

Remember to factor a buffer into your planned rollout schedule so you have enough time to correct any issues that may arise during the testing phase before the actual production deployment begins.

Testing only one week prior to rolling out a campaign, for example, may not give you the time you need to correct any problems that may have been detected.

Allow at least one full week of testing along with one to two additional weeks to make any adjustments that might be necessary. Make sure this is taken into account in your communication calendar as a pre-deployment activity.

Types of pre-launch tests

There are three main types of pre-launch testing that we at Terranova recommend.

Pre-launch testing types

1. **Content review**
2. **Compatibility and performance testing**
3. **Pilot testing**

➔ ***For each test, leave enough time in your overall deployment schedule to make adjustments.***

1. Content review

In ***Step 2 – Plan***, you selected your program content and divided it into a series of campaigns. Prior to deployment, you should have the content of each of your campaigns reviewed by key people to be sure it is aligned with your organization's needs, objectives and compliance obligations.

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

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

- Subject matter experts (SMEs) to review the course content and customization
- Your security awareness champions or ambassadors to review the course and give their feedback on the content and its relevance to their day-to-day activities
- Native speakers to review the translation to ensure terminology is correct and that it is culturally appropriate if the course has been translated
- Departments with a stake in the program to review its content (e.g. audit, compliance, legal, HR).

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

EXERCISE 3.1.

YOUR CONTENT REVIEW

Use this worksheet to list every person who should review your content to make sure it is aligned with your organization's needs, objectives and obligations.

DEPARTMENT	NAME	CONTENT DETAILS TO BE REVIEWED

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

2. Compatibility and performance testing

You put so much time and thought into your campaign, the last thing you want on launch day is for a technical issue sabotaging your rollout schedule. It is therefore important to conduct a number of compatibility and performance tests with assistance from your IT and/or HR department(s) to make sure 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. If you are using the SCORM vendor's LMS, this will not be an issue.

- **Browser compatibility testing:** Verify the compatibility of the various web browsers that your participants will be using to access the online training. Make note of any web browsers that are not compatible and, when you send out your launch email, specify in the system requirements which browsers should be used.

- **Form factor testing:** Make sure the SCORM package is tested using the various form factors that exist in your organization (e.g. smartphones, tablets, laptops, desktops). Additional technical testing will be needed if access is allowed from personal devices. Make note of any device types that are incompatible and, when you send out your launch email, specify in the system requirements the form factors to be avoided when doing the training.

- **Performance stress testing:** Ensure your LMS and network can support the number of users who may be accessing the course material at the same time, especially at the initial launch or near the campaign deadline. If you are using the SCORM vendor's LMS 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 are using an external LMS to send your launch and reminder emails, you will probably have to "spoof" your email address so it looks as though it was sent internally. You need to notify your network team so that these emails are not blocked by your firewalls or anti-spam mechanisms.

- **User synchronization:** Verify that the user list is uploaded to the LMS or the synchronization process with the LMS produces an accurate trainee database.

- **LMS/Single sign-on integration:** If you are using SSO functionality 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.

- **Browser settings:** Determine whether the awareness content requires specific browser setting (such as pop-ups), and ensure compatibility with the standard settings in your organization.

- **Verify reporting:** After loading the trainee database, **v**erify that LMS reporting capabilities will satisfy your metrics and compliance requirements, and that participant groupings are adequate.

EXERCISE 3.2.

YOUR COMPATIBILITY AND PERFORMANCE TESTING

Use this worksheet to 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 LMS web application		
Remote location performance testing		
Remote access performance testing (e.g. VPN)		
Firewall and anti-spam settings		
User synchronization		
LMS/Single sign-on integration		
Test production deployment monitoring procedures		
Pop-ups		
Verify reporting		
Other:..		

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

3. Pilot testing

A pilot test is a real-life deployment of your complete campaign, including related emails, but to a very limited audience. This test gives you the chance to troubleshoot any remaining issues prior to 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 points of access (e.g. corporate HQ, remote locations, remote dial-up or VPN)—preferably choosing those who you determined to be "intrinsically motivated" in ***Step 1 – Analyze***.

In your pilot, be sure to include

- 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—preferably as many of them as possible, since they will provide you with actionable observations

Reporting issues

Make sure you establish a clear feedback mechanism so participants in your pilot test can report any issues they uncover quickly and efficiently. The report should include:

- A short description of the problem
- What action was being taken when the problem occurred
- A screen shot of the problem, if possible
- The contact information of the person reporting the problem

What you are evaluating during the pilot project

- Access to online training
- Course content displaying correctly
- Course content screen-flows operating properly
- Course audio quality at different access bandwidths
- Communications delivery (e.g. email, videos, web banners)

➔ ***When you conduct your pilot project, advise your IT staff to give you feedback on any pilot technical issues that might be reported directly to them.***

EXERCISE 3.3.

YOUR PILOT TEST

Use this worksheet to list different people in different departments of your organization who you want to be involved in your pilot testing. Remember, your list should include security awareness ambassadors or champions that you selected in ***Step 1 – Analyze***, additional contributors you selected in ***Step 2 – Plan*** and members of your IT team.

DEPARTMENT	NAME	CAMPAIGN NAME

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 completed and all the necessary adjustments or corrections have been made, it's time to use the communication plan you developed in ***Step 2 – Plan***. You can now begin sending out your various forms of pre-deployment communications that you identified in your communication strategy and communication calendar.

An email or video sent by your security awareness program sponsor stressing the importance of the program or campaign to your organization is a great form of kickoff communication. Having "teasers" about the upcoming campaign show up on your internal intranet is another good way to get the hype started. Posters might even be used to 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 pre-training communications outlining why the campaign is necessary and other important details, such as the topics covered and whether the training is mandatory (see ***Step 2 – Plan*** on page 120).

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
- Who to contact for support

➔ ***This is your time to shine: be prepared, be visible and keep up the momentum!***

IT'S D-DAY! D FOR DEPLOYMENT.

The deployment golden rule

1. **Be prepared**
2. **Be visible**
3. **Keep up the momentum**

1. Be Prepared

It happens. We can easily get so caught up in the details and last-minute preparations that we sometimes overlook basic things like making sure everyone is ready for action.

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 out an email with a strong subject line. If your email platform does not allow you to see who opened your message, it would be a good idea to create an email with "please confirm that you are ready" in the title email.

- Are the team members aware of their responsibilities?
- Are the LMS 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 3.4.

LAST-MINUTE TOUCH BASE

Use this worksheet to list all the people in various departments who play a role in your campaign deployment to make sure they are all ready for action!

NAME	DEPARTMENT	ROLE

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.

2. Be Visible

Information security is actually a pretty cool topic, especially given today's evolving cybercrime landscape. You want your target audiences to be enthusiastic and participate in your campaigns. Think about engaging ways to create some hype around your campaign, make it interesting and get everyone talking about it. For example:

- 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 with branded giveaways (e.g. branded mugs or screen wipes).
- Offer your participants a unique email address where they can contact you with any comments, suggestions or critiques regarding their experiences in doing the training.
- Add a prize drawing for participants who have passed the course in the required time.

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

EXERCISE 3.5.

BUZZ-BUILDING BRAINSTORM

Use this worksheet to brainstorm ideas with your security awareness team. Explore creative ways you can get people at your organization talking about your security awareness activities.

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.

3. Keep up the momentum

You want to get as many people as possible to start their training on Day 1. However, let's be honest—you may have to reach out to a significant percentage of your target audiences multiple times before they participate. Some may have valid reasons, such as juggling a full work load 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 (see motivation types and incentives on page 65).

THE RULE OF 7

If your participation rates are low in the beginning, stay positive and keep in mind the Rule of 7.

The Rule of 7 is a marketing precept that says people need to see or hear a message **as many as seven times** before they will act or respond.

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

Staying top of mind

A common mistake is to launch a campaign with great fanfare and then go silent. Keep everyone engaged and motivated to participate by communicating with them at strategic moments throughout the campaign.

- Go beyond email to get your message out there using:
    - Teaser videos
    - Newsletters
    - Posters
    - Web banners
    - Screen savers
- Send out reminders emphasizing the deadline for participation and encouraging non-participants to join this new cybersecurity 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 (see page 145 below).

REINFORCING 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.

Reinforcements can be used for various reasons:

- 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

Reinforcement tools are, in essence, marketing tools and include posters, newsletters, videos and web banners. They are designed to grab attention, raise awareness and ultimately trigger shifts in behavior. They are especially powerful when you use them in different combinations, since you repeat the same message but deliver it in different ways. Leveraging the Rule of 7 (see page 143), this creates a more immersive experience for your target audiences and your message is more likely to resonate with them.

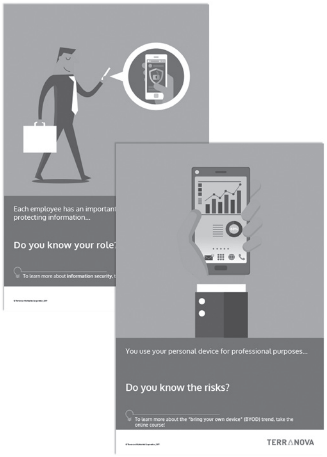
A good example of this “immersive experience” is advertising at a sports event. You see the logo of a particular soft drink on the cups people are holding. There are bold posters in the restrooms, maybe with a special offer. When you sit in your seat, you look up and see a flashing media board in the center of the stadium playing a commercial with a familiar jingle. Suddenly you are thirsty and head to the concessions stand.

➔ ***By using a combination of reinforcement tools, you keep security awareness fresh in their minds and make your campaigns much more impactful.***

TYPES OF REINFORCEMENT TOOLS

Here is a recap of some of the reinforcement tools that our clients find especially effective (see page 111 for more details).

- Videos
- Posters
- Web banners
- Screensavers and wallpapers
- Newsletters
- One-page reminders
- Reinforcement events and activities



Each employee has an important role in protecting information...

Do you know your role?

To learn more about information security,

You use your personal device for professional purposes...

Do you know the risks?

To learn more about the "bring your own device" (BYOD) trend, take the online course!

TERRANOVA

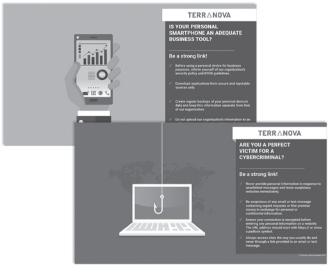
Be a strong link!

Create regular backups of your personal device's data and keep this information separate from that of our organization.

Be a strong link!

Consider the sensitivity of the information you are handling and adopt appropriate precautionary behaviours.

© Terranova WW Corporation, 2017



TERRANOVA

IS YOUR PERSONAL SMARTPHONE AN ADEQUATE BUSINESS TOOL?

Be a strong link!

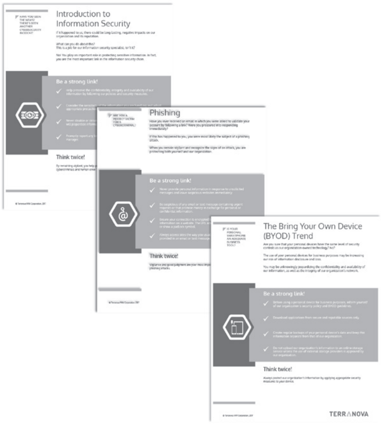
- ✓ Before using a personal device for business purposes, inform yourself of our organization's security policy and BYOD guidelines.
- ✓ Download applications from secure and reputable sources only.
- ✓ Create regular backups of your personal device's data and keep this information separate from that of our organization.
- ✓ Do not upload our organization's information to an

TERRANOVA

ARE YOU A PERFECT VICTIM FOR A CYBERCRIMINAL?

Be a strong link!

- ✓ Never provide personal information in response to unsolicited messages and leave suspicious websites immediately.
- ✓ Be suspicious of any email or text message containing urgent requests or that promise money in exchange for personal or confidential information.
- ✓ Ensure your connection is encrypted before entering any personal information on a website. The URL address should start with https:// or show a padlock symbol.
- ✓ Always access sites the way you usually do and never through a link provided in an email or text message.



Introduction to Information Security

If it happened to us, there could be long-lasting, negative impacts on our organization and its reputation.

What can you do about this?
This is a job for our information security specialist, isn't it?

No! You play an important role in protecting sensitive information. In fact, you are the most important link in the information security chain.

Be a strong link!

Think twice!

Phishing

Have you ever received an email in which you were asked to validate your account by following a link? Were you pressured into responding immediately?

If this has happened to you, you were most likely the subject of a phishing attack.

When you remain vigilant and recognize the signs of an attack, you are protecting both yourself and our organization.

Be a strong link!

Think twice!

The Bring Your Own Device (BYOD) Trend

Are you sure that your personal devices have the same level of security controls as our organization-owned technology? No?

The use of your personal devices for business purposes may be increasing our risk of information disclosure and loss.

You may be unknowingly jeopardizing the confidentiality and availability of our information, as well as the integrity of our organization's network.

Be a strong link!

Think twice!

Always protect our organization's information by applying appropriate security measures to your device.

TERRANOVA

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 3.6.

REINFORCEMENT IDEAS

Think about some interesting ideas that will keep your target audiences engaged after your 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.

IDEA	DEPARTMENT	CONTACT

Keep the momentum up and the visibility high with reinforcement tools that get people at your organization truly interested in security awareness. Be creative—think beyond emails and newsletters.

CONGRATULATIONS!

You have just completed ***Step 3 – DEPLOY*** of the ***Terranova Security Awareness 5-Step Framework.***

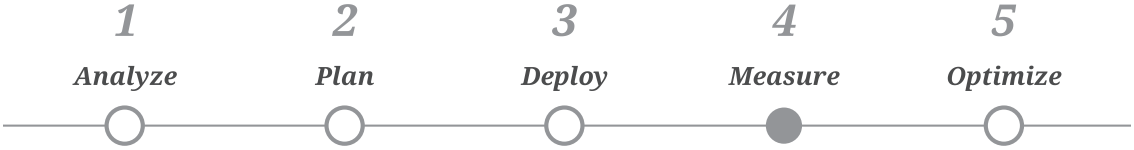
When you deploy a campaign, it's a big day. All your hard work goes into action—and you have a lot of details to oversee. Remember to test, deploy and then follow through with well-chosen reinforcement tools to make your campaign a great success.

SUMMARY OF DEPLOYMENT ACTIONS

1. Test
2. Deploy
3. Reinforce

Ready for *Step 4 – Measure?*
Let's do it!

STEP 4 – MEASURE



1 Analyze

2 Plan

3 Deploy

4 Measure

5 Optimize

The success of your security awareness program can often depend on how your metrics are measured, interpreted, reported and acted upon.

Welcome to *STEP 4 – MEASURE* of the *Terranova Security Awareness 5-Step Framework.*

Deployment of your security awareness campaign has begun and information on overall performance is being shared. In ***Step 4 – Measure***, you will use the metrics identified in ***Step 2 – Plan*** to evaluate the success of your campaign and determine if it is meeting your objectives.

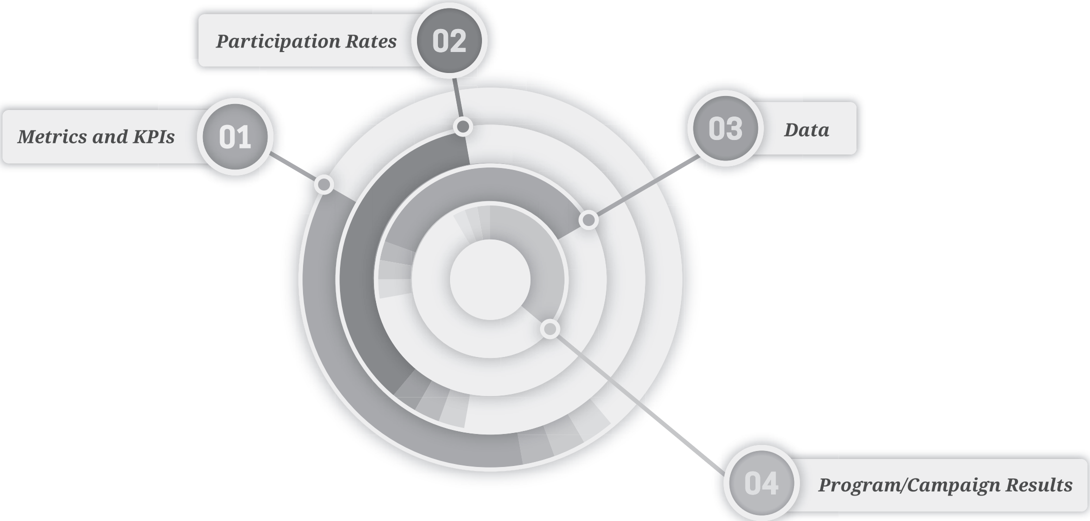
➔ ***These metrics will give you important insights that you will use in Step 5 – Optimize. You will compare your initial program goals with measurable results and identify new campaign objectives so you can tweak your next campaign to make it even more impactful.***

HOW TO MEASURE THE SUCCESS OF YOUR CAMPAIGN OR PROGRAM

Measuring performance, participant satisfaction and compliance will allow you to identify areas where your program needs to be improved.

YOU'VE LAUNCHED YOUR CAMPAIGN, AND NOW YOU WANT TO HAVE A CLEAR INDICATION OF HOW WELL IT IS PERFORMING. IN THIS PHASE, YOU WILL:

1. **Gather data**
   - Measure your progress according to your predefined metrics
2. **Track progress**
   - Effectively manage and monitor your campaign/program
3. **Report**
   - Communicate information about campaign performance to departments across your organization and demonstrate adherence to compliance requirements



1. GATHERING 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.

Common security awareness metrics

1. **Training statistics**
2. **Participant satisfaction**
3. **Training effectiveness**
4. **Return on investment (ROI)**
5. **Subjective indicators**

Use the following sources as starting points to define metrics and gather data (see page 129 for details):

- LMS and phishing simulation 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)

➔ ***Opt for existing data analysis tools and automated processes rather than manually inputting into a spreadsheet.***

Common security awareness measures

Key performance indicators (KPIs)

In ***Step 2 – Plan***, you defined the objectives that are associated with your key performance indicators (KPIs). These are the KPIs that you are tracking to monitor the effectiveness of your security awareness campaign. They will tell you if your participants are learning and applying their new knowledge. A reduction in security incidents would indeed indicate that your campaigns are helping to change risky behaviors.

1. Training statistics

Although great for compliance reporting, **training statistics** such as participation rates provide information on the progress made in terms of behavioral and cultural changes. Training statistics can be tracked in real time with most **learning management systems** (e.g. participation rates, time taken to complete training, pass/fail statistics, etc.).

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)	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 score in post-training quizzes and assessments

2. 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% of users reporting they can apply what they learned
Participant satisfaction	Percentage of overall satisfaction	80% of users are satisfied with the content
Training material is efficient	Time 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% of users report that material is too complex or not relevant
Ensure accuracy of translation, if applicable	Reported translation issues	Reduction in translation mistakes

3. 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 improper 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 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

4. Return on investment (ROI)

The metrics related to ROI are quite straightforward.

If 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.

You recall, 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 will significantly reduce the likelihood of an occurrence and make detection faster.

As an interesting exercise, go back to your worksheet on page 80 to review your budget and cost estimates. Then, investigate some of these costs of a typical security incident at your organization. Inquire as to how many occur annually and do a comparison.

This is a very good exercise to do when presenting the results of your program to decision makers and senior management.

5. Subjective indicators

In my opinion, 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 work groups	An indicator that awareness sponsorship and leadership is crystallizing
Encourage users to inquire and discuss about information security	Informal discussions are occurring about topics within the security awareness program	An indicator of curiosity, and that awareness about the topic is becoming a "state of mind"
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

2. TRACKING PROGRESS

As you gather and analyze your metrics data, keep the following in mind:

- **Metrics and KPIs should be tracked prior to program/campaign deployment** to set a baseline against which future results will be compared.
- **Participation rates** should be monitored as soon as online training is launched, and on an ongoing basis to track progress and trends. This will allow you to gauge whether or not you are on track to meet your objectives. If not on track, you will be able to take corrective actions.

3. REPORTING

Benefits of 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 has to 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

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

Planning, forecasting and budgeting for implementing and managing your programs largely depend on accurate and complete data. These include:

- Areas of vulnerability to determine priorities
- Content appreciation by audience
- Resource allocation requirements

Demonstrate compliance

Metrics can be used 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 to decision makers who are key to your security awareness program. They would be especially interested in your ROI report.

Presenting reports and metrics

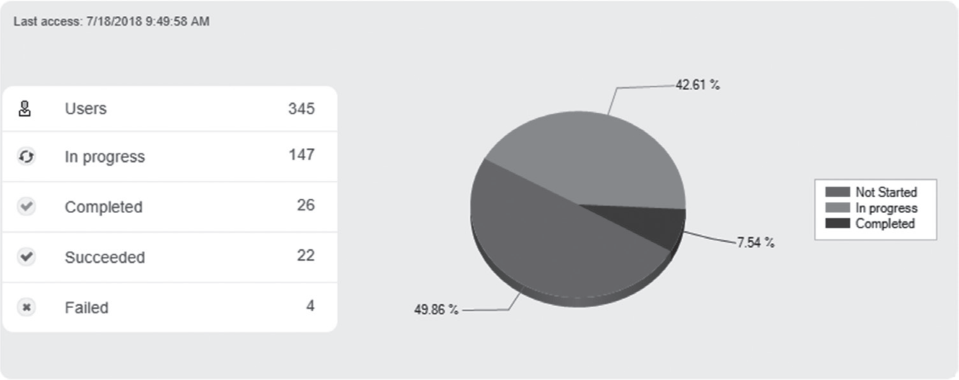
Metrics often consist of raw data that must be analyzed and interpreted, and then presented in a report. A format that is simple, easy to understand and visually appealing helps ensure the information is easily processed and understood. Remember that a picture is worth a thousand words, so include graphics whenever possible.

When preparing your reports, also consider the following:

- Why is this report relevant to the viewer?
- Is the information organized in a format that provides value?
- Can the information in the report be cross-referenced with data from other sources to identify trends or symptoms (e.g. if there is an SIEM, campaign data can be merged with other data)?
- Are there any decisions to be made based on unfavorable or favorable results?
- Do you have any recommendations for improvements based on the reported metrics?

➔ ***Present your findings in a concise, targeted, well-organized report.***

REPORT DATA EXAMPLE



Last access: 7/18/2018 9:49:58 AM

Users	345
In progress	147
Completed	26
Succeeded	22
Failed	4

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

Decision: If participation is not at the expected levels, the department lead or program manager must issue a reminder. This report can also serve to demonstrate employee participation in information 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

Decision: According to feedback received, the content, format, length or target audience for the training can be adjusted. Feedback should be gathered early on in a program to allow for timely adjustments prior to 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

Decision: If this data is not easily obtained within the organization, public reports from researchers and security service providers can be used to identify how most of the security breaches occur. This data can be used to tailor content based on the most common vulnerabilities and then to prioritize topics based on frequency and the potential impact of harmful events**.**

CONGRATULATIONS!

You have just completed ***Step 4 - MEASURE*** of the ***Terranova Security Awaress 5-Step Framework.***

Taking the time to assess the performance of your security awareness activities provides valuable information you can use to make improvements to your program. What's more, it also allows you to illustrate to decision-makers the effectiveness of your security awareness initiatives.

SUMMARY OF MEASURE ACTIONS

1. Gather data
2. Track progress
3. Report

Ready for *Step 5 – Optimize?*
Let's do it!

STEP 5 – OPTIMIZE

1	*2*	*3*	*4*	*5*
Analyze	*Plan*	*Deploy*	*Measure*	*Optimize*
○	○	○	○	●

> Insanity: doing the same thing over and over again and expecting different results.
>
> — Albert Einstein

Welcome to *STEP 5 – OPTIMIZE* of the *Terranova Security Awareness 5-Step Framework.*

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 important to act upon your findings. Keep updating and improving your security awareness program and campaigns so that you meet your objectives and keep security top of mind across your organization over the long term.***

In *Step 5 – Optimize,* you will do the following to determine if and where you need to make improvements to your campaigns and program:

1. Analyze your metrics
2. Compare results with campaign objectives and program goals
3. Identify improvement opportunities
4. Identify new objectives
5. Conduct a postmortem meeting

ONGOING IMPROVEMENT

One of the most significant benefits of gathering and analyzing data is the ability to identify areas for improvement and start developing an action plan to address them.

For a given campaign:

> You may need to take action if goals and objectives are not being met. For example, if participation is low, you could review your communication strategy and then send out a more engaging reminder, perhaps using a different medium than you did previously (see page 143 for ideas).

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 it is necessary to change priorities and schedule future campaigns differently.

OVERVIEW OF TASKS TO DETERMINE IF AND WHERE OPTIMIZATION IS REQUIRED

1. **Analyze your resulting metrics from Step 4 – Measure**
   - Investigate statistics, interpret data, validate assumptions and take any necessary corrective measures.
2. **Compare your results with your campaign objectives and program goals**
   - Assess the current situation and gaps in your security awareness program.
3. **Identify improvement opportunities**
   - Optimize your campaigns based on your KPIs and metrics.
4. **Identify new objectives**
   - Determine changes in training and behavioral objectives for a follow-up campaign.
5. **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.

1. Analyzing your resulting metrics

Anything that does not add value is a waste.
Waste only adds to time and cost.

Time to crunch some numbers! This is where you roll up your sleeves to review your metrics and interpret your results. This process will show you where your campaign is strong, as well as any weak spots, so you can zero in on the right corrective measures and ***optimize*** your program.

Optimizing your security awareness program is a part of your long-term strategy. Each campaign will take you a little farther along the learning curve, revealing new insights that will allow you to build an even stronger campaign the next time.

You may recall my discussion in ***Step 2 – Plan*** about the "Pareto Principle" or the 80/20 Rule (page 85). It talks about working smart: you can spend 20% of your effort to produce 80% of results, or 80% of your effort to produce 20% of your results. When you start to optimize and you begin looking at the overwhelming amount of data available to you through your LMS, phishing simulations, quizzes and other feedback, you may start wandering down a path that leads you away from improving your security awareness program.

Focus your efforts and resources on activities that are aligned with your goals and objectives. Work with the relevant KPIs and metrics you defined in ***Step 2 – Plan***. Everything else is superfluous—an unproductive use of your time.

Common security awareness metrics

1. Training statistics
2. Participant satisfaction
3. Training effectiveness
4. Return on investment (ROI)
5. Subjective indicators

TIP: You should gather training metrics, participant feedback and look at performance indicators to identify areas for improvement.

2. Comparing objectives with results

This part of the process takes a number of steps, as well as some time to analyze results.

First, you have to review your program goals and campaign objectives (see page 15 in the Preface) that were identified in ***Step 1 – Analyze***.

Your awareness goals are divided into 3 categories:

1. **Risks and behaviors**
   - To reduce risk and foster behavioral change
2. **Security culture**
   - To instill or reinforce a culture of security
3. **Compliance obligations**
   - To ensure compliance with your organization's security or regulatory obligations

Next, you have to compare your objectives to your actual campaigns results.

Assess the current situation and gaps in your security awareness program. Your team can compare your objectives with the results after each campaign or on a yearly basis. After a major activity, schedule some time with key players on your security awareness team to do this review.

EXERCISE 5.1.

COMPARE YOUR OBJECTIVES WITH RESULTS

List your program ***goals*** that you identified in ***Step 1 – Analyze*** on pages 42 - 47 under the related categories below (risks and behaviors, security culture and compliance obligations).

Next, transcribe the campaign ***objectives*** that you identified in ***Step 2 – Plan*** on pages 99 – 118 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.

GOAL – RISKS AND BEHAVIORS:

Objectives ↓	Results ↓	Shortcomings identified ↓

GOAL – SECURITY CULTURE:

Objectives	Results	Shortcomings identified
↓	↓	↓

GOAL – COMPLIANCE OBLIGATIONS:

Objectives	Results	Shortcomings identified
↓	↓	↓

3. Identifying improvement opportunities

> *Excellent firms don't believe in excellence – only in constant improvement and constant change*
>
> — Tom Peters

Once your campaign is under way, you may encounter any number of issues. Although some of you may have the tendency to see these as absolutely catastrophic, I want to reverse your thinking here – and turn any negative reaction into a positive one.

Remember, your security awareness program is not a project, it is an ongoing process. Every issue that arises is an opportunity to make improvements to your overall program and fine-tune your upcoming campaigns.

After helping thousands of clients around the world build and deploy their security awareness programs, we have observed that the issues that create improvement opportunities fall into three specific categories.

Improvement opportunities

1. Overproduction
2. Technical issues
3. Logistical issues

1. Too much is too much – overproduction

Sometimes less is actually better. Avoid information overload caused by bombarding end users with:

- Online training modules that are too long and time-consuming
- Content that is not relevant to them or their job function

In your LMS, make a note of the time it is taking 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*** on page 99 and make sure you have selected the right content for each of your target audiences.

When planning your subsequent campaign, keep this issue in mind and focus more attention 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, greater success.

2. Troubleshooting after the fact: technical issues

In the pre-launch phase of ***Step 3 – Deploy***, I described the need for pre-launch testing, including running a pilot test. If there are technical issues while your campaign is already under way, 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 that may occur include:

- Content not displayed properly on target form factors (e.g. tablets, laptops, smartphones, etc.) making it impossible to complete a module
- Difficult access and a complicated LMS authentication process, causing 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

Should a technical issue arise ***during*** a campaign, alert the assigned support team members to have it resolved as quickly as possible. Then, revisit your Compatibility and Performance Testing worksheet from ***Step 3 – Deploy*** on page 135 to ensure that you include more testing and troubleshooting in your next campaign, and that you schedule this testing well before your launch date.

3. Sometimes it’s logistical issues

Keeping all the plates spinning when running a security awareness program is not an easy feat, especially if members of your security awareness team have other responsibilities or if they 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 make sure they are ready for action on deployment day (see ***Step 3 – Deploy*** on page 139).

What would you 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 clients’expectations, not on your campaign?
- You did not set realistic timelines for the development and delivery of the communication material?

These types of scenarios are what we might call a logistical nightmare. How you deal with these situations and prevent them from happening in the future has a direct impact on your ongoing success.

You should approach it from a different angle and ask yourself a few questions:

- Did this happen because a security awareness team member dropped the ball?
- Was it a scheduling issue? Was I realistic?
- Did I take everything into account when creating my campaign calendar in ***Step 2 – Plan***? 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 then consider making changes if necessary.

Finally, when you create your next communication calendar (see ***Step 2 – Plan*** page 122), you not only have to be more realistic, but also more thorough. Use your updated checklist in order to keep track of everything that needs to be done to make your campaign a success.

Hiring external services

Running an effective security awareness program requires all hands on deck. What if the issue simply lies in the fact that your organization cannot provide you with the team members you need in house?

To make such a determination, first verify that all your scheduled activities were deployed and completed on time. If there were any issues, determine if they were because you do not have sufficient resources to manage your awareness activities.

Taking the helm of a security awareness program after it has been designed requires someone with 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.

4. Identifying new objectives – updating your program

In addition to applying all of your lessons learned, you need to evaluate if the goals and objectives you identified in ***Step 1 and 2*** 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 take a number of factors into consideration to identify any new security objectives for your campaign:

Factors of change

A. Compliance
B. Evolving risk landscape
C. Product backlog
D. Industry benchmarks

A. Compliance

A change in your organization's mission, key operational activities, geographical location or a new regulation may affect your compliance ecosystem. Make sure you are up to date on all contractual and regulatory compliance obligations affecting your organization. If there are any new ones since you first completed **Step 1 – Analyze**, go back and update your Goals worksheet on page 47.

B. Evolving risk landscape

As we have discussed at length throughout this book, the cybersecurity threat landscape is changing on a daily basis, which means you may have to develop an entirely new security awareness campaign at some point. You absolutely 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 powerful training modules in your program.

Another factor that affects your risk posture is a change in your organization's key operational activities, or the implementation of new business processes or technologies. Consult your IT, HR, security, finance, administration and any other relevant departments to find out if they have introduced any new systems that may be targeted by cyberattacks.

C. Product backlog

A product backlog is a list of work priorities that you draft in relation to your program and its requirements, with the most important items at the top, so your team knows what to deliver first.

You should hold discussions with your teams to establish priorities and ensure that everyone shares the same mindset about the program. Once the product backlog is drafted, it is important to maintain and update it on an ongoing basis to keep pace with the program.

It is important to note that your organization's decision makers may challenge priorities, compelling you to identify new priorities.

D. Industry benchmarks

Relative comparative data is not always readily available to an organization due to differences in size, sophistication and business sector. Many organizations therefore rely on industry or trade association reports to gather best-practices data. Other sources include conferences, magazines and the Internet. They may shed light on new trends, updated statistics or new breeds of cybercrime.

When you discover new industry information that could affect your organization, you need to be nimble and responsive. You have to make changes to your programs to make your people aware of the new threats and therefore able to fend off a cyber attack.

5. 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.

As the old saying goes: “Two heads are better than one.” Sharing insights into what worked and what didn’t work with your security awareness team is such a powerful exercise. Everyone has had a different experience in the development and delivery of your program and campaigns, and they all have suggestions that will take your program to the next level of effectiveness.

Postmortem meeting tips

- After a major activity, schedule a meeting with key players to discuss what worked and what went wrong.
- Have a whiteboard or flip chart available to capture their comments as they are stated—it will make it easier to decide on priorities when they are visible to all attendees. Take photos of the whiteboard or flip chart entries to have a record of what was said so you can document it after the meeting. Recording what you have learned will ensure it is not lost or forgotten, and that errors will not be repeated.
- Pick the top three items to address as your first priorities, rather than try to resolve all the issues at the same time. 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 successfully transform human risk behaviors into higher levels of security alertness. 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.

Your optimization plan will involve:

1. Reviewing feedback
2. Identifying best practices and lessons learned
3. Selecting priorities
4. Assigning responsibility
5. Conducting a follow-up

1. Reviewing feedback

Prior to the postmortem meeting, send out a survey to all team members, support staff, champions, sponsors, subject matter experts and key clients so that you have a preview of their perceptions and thoughts about your program. You should also review any direct feedback and comments that were sent to your security awareness team during the campaign from the participants.

2. Identifying 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

3. Selecting priorities

When you and your security awareness team meet, plan and prioritize your upcoming improvement activities. You should always be thinking of ways to optimize your program so that you achieve increasingly better results with each wave. Your optimization plan should therefore specify:

- Optimization priority
- Current organizational situation/context
- Recommended initiatives
- Expected benefits of the optimization initiative
- Expected completion date

4. Assigning 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.

5. Conducting a follow-up

Once all the optimization activities have been assigned and delivery dates have been set, incorporate them into your program schedule and update your security awareness team. Allocate time in your schedule for follow-up and for collecting progress reports from those responsible.

EXERCISE 5.2.

EVALUATING YOUR SECURITY AWARENESS PROGRAM

When evaluating your security awareness program, you have to answer the single-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?

Use the evaluation questions below as a guide for 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 the right topics?

□ Yes □ No

Explain

Do you need to consider adding another target audience?

□ Yes □ No

Explain

Did the program take into consideration the needs of all target audiences?

□ Yes □ No

Explain

Did the target audiences react favorably to the program?

□ Yes □ No

Explain

Which communication channels worked best?

Which communication channels did not work, and why?

Do you need to consider different methods for delivering your messages?

□ Yes □ No

Explain

Were you able to deploy all your planned awareness activities and communications in time?

□ Yes □ No

Explain

OUTCOME EVALUATION

Were any assumptions made at the start of the program incorrect? Refer to your Analyze Cheat Sheet on page 44.

□ Yes □ No

Explain

Were any actions taken to compensate for unforeseen events?

□ Yes □ No

Explain

Were any workarounds developed to compensate for technical issues?

□ Yes □ No

Explain

Were your security awareness program goals met?

□ Yes □ No

Explain

Did any of the awareness team members receive direct feedback on the program?

□ Yes □ No

Explain

Were the campaign activities beneficial to the target audiences?

□ Yes □ No

Explain

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 negative effects?

□ Yes □ No

Explain

Is your security awareness program aligned with your organization's current policies?

□ Yes □ No

Explain

....

....

....

What else can be done to improve your security awareness program?

Explain

....

....

....

RESOURCES EVALUATION

Does everyone on the security awareness team understand their roles and responsibilities?

□ Yes □ No

Explain

....

....

....

Does your security awareness program team need any additional resources?

□ Yes □ No

Explain

....

....

....

Are the costs of the program's activities reasonable in relation to the benefits?

□ Yes □ No

Explain

....

....

....

Does your security awareness program have the required budget to continue its activities?

□ Yes □ No

Explain

....

....

....

EXERCISE 5.3.

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 program level of success.

PRIORITY #1

What will be optimized? Describe?

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?

PRIORITY #2

What will be optimized? Describe?

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?

PRIORITY #3

What will be optimized? Describe?

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 just completed ***Step 5 – OPTIMIZE*** of the ***Terranova Security Awareness 5-Step Framework.***

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 each of your campaigns so that cybersecurity stays top of mind across your organization over the long term!

SUMMARY OF OPTIMIZE 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 the fifth and final step in the *Terranova Security Awareness 5-Step Framework.*

My objective in writing this book is 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

A security awareness program to help you fight cybercriminals

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 and dramatically reduces the likelihood of a breach at your organization.

This book is designed to be your go-to manual for masterminding the right security awareness program for your organization. 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 cyberattacks aimed at organizations like yours.

The security risk landscape is rapidly evolving, and the threats are not going away any time soon. On the contrary! They will become even more prevalent and persistent as long as people continue to click on links or change their password as instructed by an innocuous email. When it comes to security, the industry saying is true: People are the weakest link.

In this day and age, it is not enough to rely on security technology, or have a "tick the box" mentality and merely go through the motions in order to say "security awareness training completed." We need to employ a ***human fix*** to address the human risk factors.

As you know, ***cybercriminals target the people at your organization*** with phishing scams, social engineering and other cyber threats to try gain access to sensitive information. In response, ***you have to engage the people at your organization*** with the right security awareness training that is relevant, interactive, engaging, ongoing and repetitive to get them to change their risky behaviors and to 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.

It is therefore incumbent upon 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.***

A security awareness program tailored to your needs.

To keep cyber threats at bay, you have to be proactive and strategic. You have to mastermind a plan customized to the specific realities and needs of your organization. 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 reduce risky behavior from your ranks.

A security awareness program using a structured approach: a framework

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 a smart, powerful and extremely effective process that has helped thousands of companies around the world implement effective security awareness programs.

Time and again, 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:

1. View security awareness as project, not as an ongoing process.
2. Start at the deploy phase, releasing online courses and/ or videos without proper analysis and planning.
3. Just want to check the box of compliance.
4. Don't set goals and objectives for the program and campaigns.
5. Don't establish key performance indicators (KPIs) or measure results.
6. Don't make the campaigns interesting and interactive for participants.
7. 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

➔ ***Without a framework, it's just trial and error—you are leaving it to chance.***

** See end of the Conclusion for the **Terranova Security Awareness 5-Step Framework** in brief.*

The big takeaways

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 have to keep in mind a number of factors that have a direct impact on 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

Moving forward

As you work with this book, I hope that 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 in order 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 secure behaviors among the people at your organization.

Need any help?

Remember, the experts on my Terranova Security Awareness Team are always happy to assist you in any way they can. Please contact us if you have questions or if you need support of any kind. Think of us as your security awareness partner. info@terranovacorporation.com

Thank you once again for reading ***The Human Fix to Human Risk***. I wish you good luck and great success with your security awareness program!

THE TERRANOVA SECURITY AWARENESS 5-STEP FRAMEWORK IN BRIEF

The five steps to designing and implementing a successful security awareness program.

Step 1 – Analyze

The analysis phase is crucial. It will provide you with important insights so you can create and implement a successful security awareness program. In this step, you will determine the following:

1. Strategic program goals

- What are the overall goals of your security awareness program?

2. Compliance

- Do you have any contractual, industry-related or regulatory obligations?

3. Target audiences

- Who will receive the training? What are the profiles of your different target audiences? Are they all in house or do you also have to include third parties?

4. Scope (topics)

- What training is required, based on the current level of awareness and the threats affecting your people, contractors, business partners and customers?

5. Level of knowledge

- What is the current awareness level of each target audience? Any risk behaviors that compromise information security?

6. Motivation & culture

- What is the current organizational culture? How motivated are people when it comes to information security?

7. Support resources

- Do you need to build a support team?

8. Globalization

- Do you have to offer your program in more than one language? Will you have to customize content to reflect any geographic or cultural nuances?

9. Cost

- What resources, time and budget do you need and what is available to you?

Step 2 – Plan

Now, you have to plan your program. In this phase, you will define the who, what, when and how – the logistics.

1. Team

- Identify who will be on your security awareness team. What are the required skills, roles and responsibilities of each member?

2. Roadmap

- Define your campaign objectives.
- Plan your campaigns per audience and timeframe.
- Plan your activities per campaign.

3. Product

- Select and customize your content: online training courses, live presentations and reinforcement tools.
- Select and customize your measuring tools: LMS, phishing simulations, vulnerability assessments, surveys and quizzes.

4. KPIs and metrics

- Define KPIs and metrics in relation to each campaign's objectives so you can measure your results against those baselines to optimize the next waves of your program.

5. Communication

- Prepare and approve in advance the communication plan you will use throughout your program and various campaigns.
- Create your communications calendar.
- Select and customize your communication materials.

6. Program presentation

- Create a presentation for senior executives, team members or stakeholders highlighting the main elements of your security awareness program and communication strategies.

Step 3 – Deploy

You've crossed every T and dotted every I. Now you are ready to launch! In this phase, you will carry out the following activities:

1. 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.

2. Launch

- Launch the campaign and communicate with participants.

3. Reinforce

- 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.

Step 4 – Measure

Your campaign has been launched and you want to have a clear indication of how it is performing. In this phase, you will:

1. Gather data

- Measure your progress according to predefined metrics.

2. Track progress

- Effectively manage and monitor your campaign/program.

3. Report

- Communicate information about program performance to departments across your organization and demonstrate adherence to compliance requirements.

Step 5 – Optimize	In this phase, you will look into ways to improve your program based on the data you gathered in Step 4. Specifically, you will: **1. Analyze metrics from Step 4 – Measure** ■ Investigate statistics, interpret data, validate assumptions and take any necessary corrective measures. **2. Compare results with campaign objectives and program goals** ■ Assess the current situation and gaps in your information security awareness program. **3. Identify improvement opportunities** ■ Optimize your campaigns based on your KPIs and metrics. **4. Identify new objectives** ■ Determine changes in training and behavioral objectives for a follow-up campaign. **5. Conduct a postmortem meeting** ■ Once you have gathered and compiled your observations and the gaps you discovered, you need to share your learning with your security awareness team to identify areas for improvement.

INDEX

THE HUMAN FIX TO HUMAN RISK™

5-steps to masterminding an effective security awareness program™

The Terranova Security Awareness 5-Step Framework will guide you through everything you need to do to develop and deploy a successful security awareness program.

A lot of companies start at the deploy phase and launch online courses or videos thinking it will change risk behaviors. They fail to conduct a proper analysis or plan their program, and overlook the importance of setting objectives and measuring results—all of which are crucial to a successful security awareness program.

In this book, based on the Terranova Security Awareness 5-Step Framework, you will cover the five essential steps (Analyze, Plan, Deploy, Measure and Optimize) to ensure that the people at your organization understand and apply security awareness best practices—and become your strongest line of defense against malicious cyberattacks and social engineering.

> “ Gartner identifies several elements of a broad security program that today are crucial to an organization’s overall sense of knowledge and accountability. To begin, a security awareness program informs employees and partners what they should -- and should not -- do to achieve security. Consistent and focused education can elevate the staff’s understanding of threats, risks and responsible behavior. It can illustrate the accountabilities they hold for the larger security mission. ”
>
> - Gartner, **How to Secure the Human Link**, Amanda Sabia, Joanna Huisman, 2 May 2018.

> “ An effective and successful security awareness program must include well-defined and measurable objectives, a strong knowledge of your target audiences, and topics that are chosen based on assessments of your organization’s risks. ”
>
> - Laraine A. Weglarz, CISSP
> Former CISO of a €15 Billion multinational conglomerate

ABOUT THE AUTHOR

Lise Lapointe, CEO of Terranova Worldwide Corporation, is a visionary through and through. She’s a true entrepreneur who has dedicated the last two decades of her career to training, IT and security awareness. Working in partnership with clients to deliver thousands of successful security awareness programs to millions of users around the globe, Lise and her Terranova team of experts have acquired incomparable expertise in the field and they’re excited to share the lessons learned with you in this valuable how-to manual built on the **Terranova Security Awareness 5-Step Framework.**

Lise believes that the most powerful way to address security awareness is by taking a human approach and by leveraging proven techniques that effectively change human risk behaviors. When the people in your organization are more acutely aware of cyber threats, they are less vulnerable to them. Making her home in Laval, Quebec, Canada, Lise surrounds herself with top strategic thinkers in security awareness and has ongoing plans to scale up her company so that she can help more organizations worldwide stay protected from cyberattacks.

9 781999 420604