The Introductory Guide to

Creating and Managing a Successful Security Awareness Program

the security awareness COMPANY

Welcome to the Introductory Guide to Security Awareness Programs!

So your job is to create, launch and manage your organization's security awareness program. Where do you even start? It can seem like a daunting challenge and many people come to us asking for help. That's why we've put together this handy guide with some tips and tricks to help you create an awesome DIY awareness program.

The following pages are full of information that will help you in the initial planning stages. We will continue to release resources and information you can use for your awareness program. Down the line we will release a comprehensive guide to take you through the entire process step-by-step. This beginner's guide is merely a launching point.

At the end of this guide, there is a worksheet that will help you begin laying out your in-house security awareness program. To get you started, here are some other resources to help you along the way:

Free Content Archive

We've revamped our freebie archive, so check it out to download FREE awareness materials! Newsletters, posters, videos, and more. We update it every month, so bookmark it and come back later. Yes, it's all really free. No strings!

SAC YouTube

Our channel is full of videos that you can use to supplement existing materials and/or to teach key concepts in short, easy-to-understand snippets. Be sure to check out our music videos!

The SAC Blog

We post a wide range of articles that you can use in email blasts to your employees. Look through our archives for tons of advice on running successful awareness campaigns, as well as simple tips that appeal to the average user.

Paper.Li

This service keeps you up-to-date with our daily newspaper, which aggregates all the top stories from our Twitter feed, our partners, and other social media outlets. A new edition is available every morning!

SAC Twitter

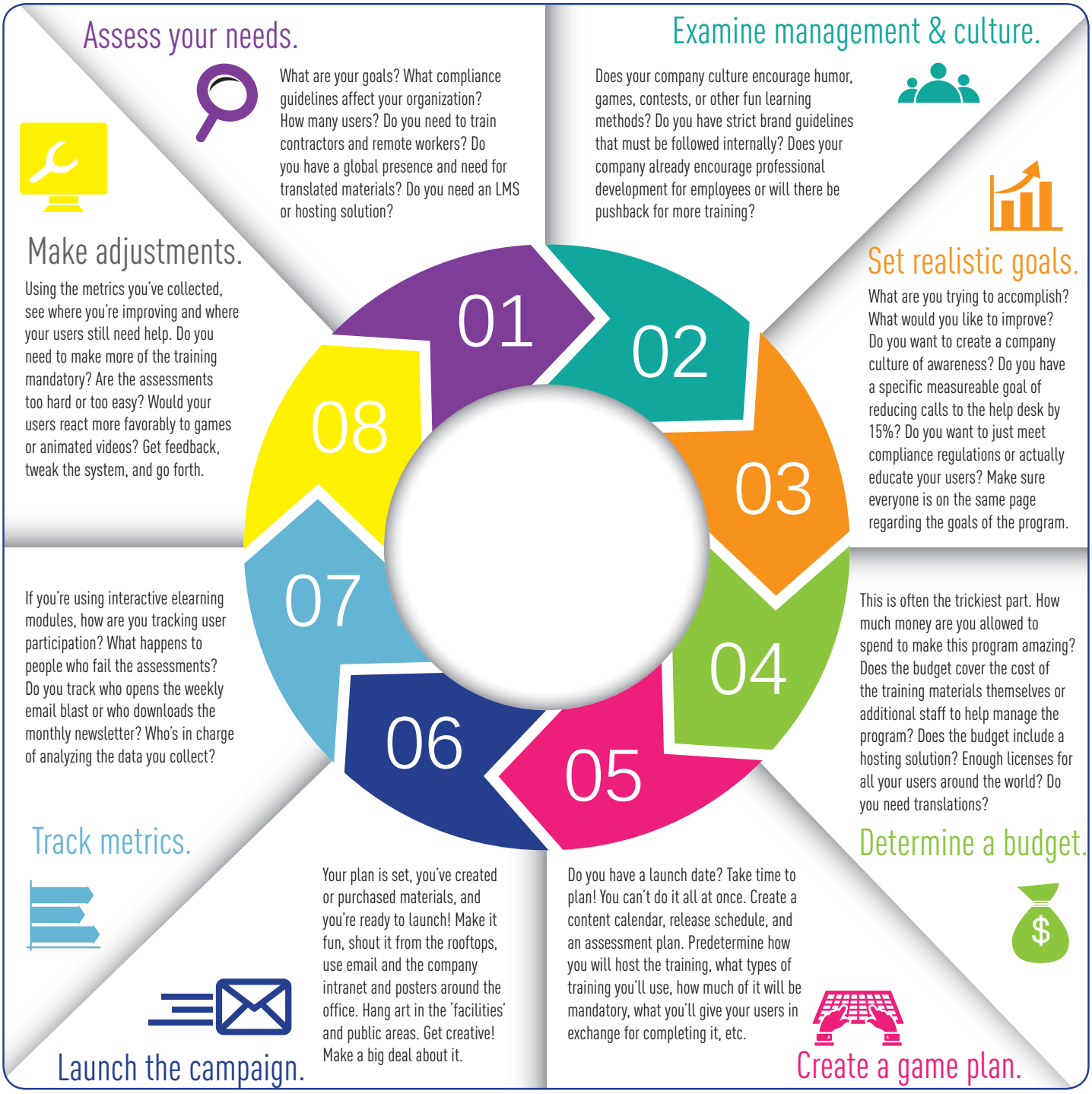
By following the right accounts, your newsfeed can be full of infosec news, tips and tricks. Follow us for access to FBI-issued security alerts and important stories posted around the industry.

All of these ***free resources*** are super valuable for small companies that still need to meet specific regulatory and compliance requirements.
What better way to get started than with Security Awareness Company content?

You can't change users' behavior without changing their mindset, so we believe in approaching security awareness from an advertising and marketing standpoint. We find inspiration in the same places all the top advertising firms find theirs, and we take cues from pop culture and web trends as well as e-learning giants and industry experts. Think about your awareness program as a messaging campaign. **Focus on regularity, frequency, and relatable content.** By making awareness content personal, it will resonate with your users much more than if you just focus on policies and compliance. By using regular and frequent messaging—such as posters, short videos or games—you will reinforce you messages much better than by relying on once-a-year training. **Make awareness part of your company culture** and it will become part of your users' mindsets. Then you'll start to see a shift in behavior and a shift towards more security.

? Where do I start?

Follow our Circle of Awareness to help you build and manage an awesome security awareness program. These eight steps will help you get on the right track to shifting your users' mindsets and changing behavior. Pretty soon you'll have a whole team of human firewalls!



09 Rinse and repeat.

Treat your awareness campaign like a marketing and advertising campaign. Does Coke run just a few commercials a year? Do movie companies only run one trailer for upcoming releases? Subway ads, billboards and window displays change regularly to send consumers the same messages in different ways. Once you've followed steps 1 - 8, start again. Awareness is a dynamic process, not a thing. Re-assess your needs, update your goals, and make improvements to your campaign.

How to Convince Your Boss to Let You Spend Money on a Security Awareness Program

Often the biggest hurdle a security team has to jump is getting a budget big enough to meet their needs. They're given a mile-long To-Do list and exactly enough funding to get 25% done. Then the boss comes shouting down the hallway, "*Who's responsible for this data breach? How come our employees are making poor security decisions? You need to train our users!*" The security team throws their hands in the air but the boss won't hear it. He wants them to do more, more, more with less.

So how can you convince your boss to give you the money that will let you do your job?

The answer comes down to motivation. Humans are motivated primarily in two ways, both of which can help you convince your boss to increase spending, give you more team members, buy new equipment, etc.

Fear and Desire. These are the reasons we do anything. They are the motivating factors behind every decision people make hundreds of times every day. If you're worried you'll be late to work, you leave the house a little early. Worry is a form of fear. Wanting to impress the boss with your hard work ethic, you show up to the office before the others. Want is just another word for desire.

Fear

Most organizations are scared to death of data breaches. What would happen if your organization got breached? There's the possibility of losing money, losing customer or employee PII, losing the faith of your clients and damaging your reputation. There's not an organization that isn't worried, on some level, about a breach. The fear of financial loss, data loss or reputation damage is what leads to most organizations needing security awareness training. The trouble is if the fear isn't strong enough, the security awareness program won't receive the level of priority it truly deserves.

Thus, it's your job to scare the living daylights out of the right people.

First, figure out what your organization is most scared of – losing money, data, clients or reputation.

Second, learn which language to use when talking to decision makers. Do they speak Dollars, Identity Theft, Followers…?

Third, do some research. Find stats to scare your bosses. Find the companies that you ***don't*** want to emulate and use them to your advantage.

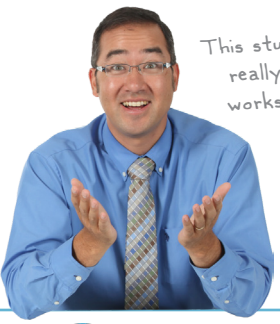
It will probably take more than one conversation. Much like awareness training itself, this is not a one-and-done situation. It might take cozying up to some other departments to back you up, and it might take putting your research on display more than just once. Think about the scary research out there about tobacco; we know it causes cancer. **Often, people are not truly motivated by the fear until they see it first hand, or until they've seen the consequences.** Get ready to act like a broken record and get to scarin' up some money so you can train your users and secure your organization!

Desire

People are often more motivated by desire than by fear. We want to have fun so we drink wine and eat cake and drive on congested roads despite any worry, or fear, that alcohol could poison our livers, that cake will pile on the pounds or that roads could lead to an accident. Many people exercise not because they're scared of heart disease or Osteoporosis, but because they want to look good and have others desire them. Many people work hard and long hours not because they are worried they will be passed over for promotion but because they desire earning more money.

While some organizations fear data breaches and public humiliation, other companies want to be a step ahead of the curve. Their executives want to be on the forefront of progress, with super secure employees who make smart decisions not out of fear of losing their jobs but because they are cyber savvy users. Some organizations are not concerned (aka fearful) about meeting compliance mandates but actually want **an educated army of security aware individuals working the front lines of defense**. If you proactively train users instead of reactively, results will skyrocket.

Strong leadership means they want to encourage a healthy, happy, secure work environment in which they promote professional educational development. They want to impress your clientele with your users' security awareness. Your bosses just want a safer internet for everyone and know that educating users is the place to start.



The Final Word

We all know that effective security awareness training can secure an organization from inside out but sometimes it will take a little extra coercion to get the C-levels to sign off on the money required to do so. **It's up to you** to figure out what motivates your upper levels and then use research to help you exploit that motivation to everyone's advantage.

5 Ways to Get User Participation in Your Security Awareness Program

Sometimes it's tough to get users to participate in your information security awareness program. Employees don't want MORE work thrust upon them, even if it is something that will help them be better at their jobs (and help protect their families at home)! So you, the awareness program manager, have to get creative. Let us help!

Make it mandatory.

The best way to get user participation is to **force them to participate**. Now this doesn't make it the most successful way to earn user buy-in or engagement, but if your goal is strictly 100% participation this is the way to go. You can spin it by making 'part of the job' in the same way that occasionally working late nights or going to after work social events are 'part of the job' — not mandatory, you won't get fired for not doing it, but it is expected of you.

Attach real consequences - both positive and negative.

People need reasons to do things. We workout because we want to get healthy. We drive the speed limit because we don't want a speeding ticket. We take classes to learn new skills or to get better at our jobs.

So why should I take this awareness training? Will I get in trouble if I don't? Will I get called out in a meeting for not completing it? Will I get praised if I do? Could I get a pat on the back from my manager if I do? Is the training an expected part of my job or will I slide by unnoticed if I just happen to forget about it?

Give your users a reason! Unless your users understand the consequences—either positive or negative—you will have a hard time getting them to participate.

Make it fun and competitive.

Think Fitocracy. Think Duolingo. Think about all those video games you've played and why you liked them: getting that high score and beating JohnSmith334. **Bragging rights and competing** with friends/coworkers can make something mundane (such as exercise, language learning or policy training) more appealing and fun. "*Oh, a new awareness video just came out? And if I watched it I can earn 500 CyberSavvy points? YES please! Because then I'll only be 1000 points away from getting the Most Security Aware Employee Badge.*" If your culture permits it, **friendly online contests** like Security Jeopardy, etc., that offer rewards ($50 at Amazon, e.g.) could be a real motivator, along with bragging rights.

Do it for your users, not for compliance.

If you approach your awareness training like, "*Let's get this over with and check off that compliance box*" then your training won't be very good and your users won't think it's important. But if you **approach it from a positive and enthusiastic viewpoint**, one that empowers your users to be better at their jobs and at protecting their families, then you're going to get less resistance. Awesome, entertaining content will reflect how it was created, meaning if it was created with passion, it will be better than if it was created with a lot of head-desk-banging and feet-dragging. Your users will be more responsive if they think that the organization cares about their personal security and privacy, and isn't just trying to comply with industry regulations for the sake of compliance.

Ask yourself: what would I do?

Go ahead, we'll wait. If you were told you had a pile of training to complete, what would you do? Would you read that newsletter if you knew it didn't matter? Would you take that voluntary training module if you knew no one would ever ask you about it? **Would you do something on a purely voluntary basis** if there was no reward for doing so or no punishment for not completing it? Would you resent the extra work if it were made mandatory without any cutbacks elsewhere? Stop being *You the Admin*, and be *You the User*. **What would make you happy?**

Have you found a different tactic to get increase user participation? Tweet us at @secawareco and share your secrets to help fellow cyber security admins improve their awareness programs! For more advice, check out our blog post about user participation and bribing your users.

Which is better: Proactive User Training or Reactive User Training? With Security Awareness the answer is BOTH.

Many clients come to us in crisis: "*Help! Too many of our employees are falling for phishing scams!*" or "*Help! We got breaches last year*!" or "*Help! We didn't pass compliance and need to train our users!*" They reach out to us, panic in their voices and desperation in their eyes because they see dollar signs and lost trust from their own customers. To them they're in a sinking lifeboat full of holes and need us to fill those holes with plugs as fast as they can.

We also have a lot of clients come to us because their peers have been breached. They are on a tight schedule, sometimes trying to get in under a deadline to impress an exec or beat a compliance deadline, but they haven't been hit yet and want to keep it that way.

Both ways—reactive and proactive—result in awareness programs. But which way is better?

Ideally, we should try to prevent situations from arising by teaching users how to create strong passwords, how to recognize social engineering scams, how to prevent personal identity theft and why data classification is so important. But if something cyber-bad does happen, we should also react with training, not as a punishment but rather to reinforce lessons we're already teaching, and to correct unsecure and careless behavior.

Here are a few tips and tricks we've learned in providing awareness for 20 years:

Use minor mistakes as learning opportunities.

If someone forgets their badge, can't remember their password, or neglects to lock their desktop screen before getting up, these are not huge infractions but can be a good opportunity for you to remind them of policy.

Require training for the whole group, not just the offenders.

If something bad happened and everyone knows about it (an insider gone bad, a data breach, an outside attack, etc.), let the employees know that's the reason for the training. One bad apple does spoil it for the whole bunch. No one wants to be the bad apple.

Phish your employees.

You should also require additional training for anyone who fails. This is an immediate reactionary, defensive form of training since the person who falls for the phishing email will receive an immediate learning opportunity and see what they did wrong.

Make it personal.

People care way more about themselves than they ever will about the company they work for. Give them some useful information about securing their own lives & protecting their own privacy. At the end, just be sure to say, "*Hey, by the way, all this stuff we're teaching you? Do it here at work, too.*"

New Hire Training is a must.

"Start 'em while they're young," is something we've all heard about teaching kids about whatever particular subject matter is at hand. Don't wait until employees have been there six months. Catch them while they're new. Hit them with awareness training from the get-go to ingrain it into their work behavior.

Once-a-year won't cut it.

For employees who have been there more than a few months, don't just rely on a yearly compliance review. Remind them regularly of policy, of best practices, and of why security awareness should be at the forefront of their minds in everything they do.

Top Tips to Creating Your Own Information Security Policy Training Program

So you've been tasked with building a security awareness program? It's a tough job. You've got to figure out how to tell people about the program, teach them the security lessons that are most important to your organization, and stay within a tiny budget.

What's even tougher is figuring out which lessons to teach, which messages to focus on, and what kinds of materials work best for your company. Do you need to use an LMS to track user data? Will your users prefer watching one short video every month, or one long video every quarter? Should you offer incentives for the employees who finish the training?

Every organization is different, and we can't tell you how to run your security awareness program. But what we can do is offer you some free resources, tips and helpful hints to make the process a lot easier.

Find Inspiration

The internet is full of awesome stuff but sometimes the sheer amount of information can be overwhelming. Follow some infosec people and companies on Pinterest to find useful infographics, posters, quotes, and blog posts you can send to your users or use as inspiration for making your own materials!

Make It Personal

In order to change behavior, you've got to change their mindsets. And the only way to change the way they think is to get them to CARE. If you get them to care about protecting their family and teach them how they can be safer online at home, then it's easy to slide in that company reminder. "Oh, by the way, all that stuff we taught you about protecting your family? Do it here at work, too!"

Remind Users Frequently

We live in an ADHD world. No one has the attention span to read a policy book front to back (did you?). But people are used to watching short, 3-minute-or-less YouTube clips, and reading quick 1-page-or-less blurbs in magazines. Every month, pick a topic (phishing, social engineering, passwords, backup) and create short newsletters and/or videos on that topic, distributing them at the same time, every month. The regular (but not annoyingly frequent) reminder will bring security to the forefront of everyone's minds.

Keep It Simple

Most users don't need to become experts or even need much technical know-how in order to be security aware, so don't try to overload them with technical jargon, complex diagrams or intimidating cyberspeak. Keep things simple by teaching the basics in easy-to-understand language. Not everyone understands what 'social engineering' is but everyone understands what a con artist is. So teach about the dangers of social engineers by making real world comparisons to con artists and scammers to drive the point home.

Don't Do It All At Once

Start slow. Build momentum. Don't start with everything all at once. Unless you have a huge dedicated staff, you're not going to have the time, manpower or mental bandwidth to handle all of the things all at once. This means instead of doing a really awesome job and rolling out an eye-catching, engaging and effective awareness program, you're going to end up with something poorly developed and haphazard. It's not going to be successful and you'll be frustrated. So don't try rolling out a program that includes training modules, and videos, and posters, and newsletters, and interactive games, and a gamified LMS all in the same month or quarter — and certainly don't just dump all of your awareness materials on an intranet and hope people will click on them.

Establish Who's Boss

Too many cooks will ruin your program. Find out who has to be involved in the decision process, then streamline as much as you can. One person should be the single point of responsibility for the entire program.

Use a Spoonful of Sugar

Humor is an effective learning tool. Put a smile on your user's face & they will be more likely to remember the lesson than if you go at it with cut-and-dry policy language. Use graphics & videos, use some pop culture examples, use cats. Do whatever you need to make them take their security awareness medicine, so to speak.

Brand Your Program

A recognizable brand & theme helps users identity anything you present & drives the message home. Mascots and character development assist in teaching awareness.

Rinse & Repeat

Security Awareness is like advertising. In order for the message to stick and for the user to take action, it's got to be in front of them multiple times during a year. Once a year training is not enough. Quarterly training is okay but monthly and/or weekly reinforcement is even better. Treat your SA program like a marketing campaign using monthly newsletters, screensavers, posters, weekly email tips, videos, quizzing and learning games to engage and educate your user population. The more they see the message, the longer it will stay in the forefront of their minds and the better their behavior will be.

Avoid Death by Powerpoint

Don't waste your time creating long presos that will bore your audience. You want them paying attention, not playing Candy Crush while you drone on about security policies. If you HAVE to use a powerpoint presentation, use funny photos and avoid a lot of text on the screen. Use videos on YouTube to get your point across. Entertain your users into actually learning something!

Security Awareness Program Planning Worksheet

Organization Name:

Awareness Campaign Name:

Does your program and/or department have a brand? (Colors, logo(s), mascot, etc.)

Lead Campaign Manager:

Campaign Teammates:

Goals for program:

1)
We will tackle this goal by:

2)
We will tackle this goal by:

3)
We will tackle this goal by:

Circle the three subject areas management is most concerned about and will best help you meet your goals. *For example, if your goal is to reduce the number of users who click on phishing links, you might want to focus on Phishing and Social Engineering.*

General Security Awareness	Social Engineering	Executive Awareness
Compliance Regulations	Safe Surfing	Acceptable Use
Physical & Non-technical Security	Company Policy	Mobile & the Cloud
Phishing	Data Classification	Passwords

What kind of content will you start with? (emails, PDF newsletters, posters, screensavers, e-learning modules, videos, animations, in-person training, games, etc.)

How will you deliver content? (LMS, intranet, email blasts, etc.)

Campaign Start Date:

First Assessment Date: