### TABLE OF CONTENTS

3  What Is Security Awareness?
5  Dealing With Human Risk
6  5 People-Centric Elements To Build Security Awareness
7  High Quality Content
9  Personalized Campaigns
10 Collaborative Partner
11 Security Awareness 5-Step Framework
17 Security Awareness As A Service
19 Conclusion
CHAPTER 1

What is Security Awareness?

To successfully discuss security awareness, let’s begin with a definition.

In the Magic Quadrant for Security Awareness Computer-Based Training, Gartner, Inc. says, “The term security awareness is commonly used to refer to a broad range of education, communication, and behavior management activities and learning outcomes. These outcomes include:

- Complying with regulations that mandate security training;
- Establishing clear behavioral guidelines to support disciplinary processes, which are typically described in acceptable-use and/or security policies;
- Improving employee knowledge of security and risk topics;
- Motivating desired security behaviors in the appropriate context.”

With new regulations such as the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR), your business may be required to show it has a security awareness program in place in order to fully address compliance with the regulations.

Security awareness programs also help prevent negative business impacts, such as financial costs or operational and reputational issues, by reducing the risk of data breach. The 2018 Cost of a Data Breach study conducted by the Ponemon Institute revealed a data breach of 1 million records cost a company an average of $40 million; with 50 million records breached, the estimated average cost is $350 million (not including any costs associated with legal settlements).

In the end, security is everyone’s responsibility. All it takes is one convincing – yet fraudulent – email or phone call to trick an untrained, security unaware employee into opening the door to cyber criminals. The depth of security awareness training will vary depending on an employee’s role. For example, employees in IT, application development and human resources may have more training modules that are role-specific than someone in marketing or administration. But no one is exempt from security responsibility and security awareness training.

Security awareness programs make employees aware of security best practices; they change employee behavior so it’s more secure; they create a security-aware culture; and they reduce the number of human-caused security incidents.
But achieving all that takes time.

It takes time to build a security-focused culture filled with employees who have shifted from the weakest link to the strongest link in the cyber security chain.

In the following sections, you’ll see why taking a people-centric approach to cyber security awareness is the only way to address human risk, instill long-term behavior change in employees and build a culture of cyber security.

Don’t waste any more time with a “one size fits all” program. The time to launch a people-centric awareness program is now!

The Definitive Guide to People-Centric Security Awareness has been written to help security leaders reduce human risk in their organizations by applying the five people-centric elements for phishing simulations and security awareness training. We will explore each people-centric element in detail and explain how each plays a key role in educating users to help change behavior and instill a security culture.
CHAPTER 2

Dealing With Human Risk

Organizations try to deal with human risk by employing security technologies and processes, but that’s not enough. Technology can’t stop someone from clicking a link and processes can be ignored. Without a focus on people, your security strategy rests on a two-legged stool.

Human risk demands a human fix -- one that effects the person, modifies employee behavior to be more security aware and instills a security mindset in daily activities. A people-centric, security awareness program adds the human element to complete the three-legged stool supporting your security strategy.

Taking a people-centric approach to security awareness trains employees to spot fraudulent messages and teaches them what to do if they receive one. A people-centric approach to security awareness educates the employees on why security technologies and processes are in place and must be followed.

The training and education in a people-centric security awareness program is designed to reduce human risk by producing long-term employee behavior change and instilling a security-focused mindset in employees as well as a security-focused culture across the organization.

“Security Awareness involves people, processes and technologies – getting all three in the right measure is the real art of a successful security program”

CISO - Leading Mobile Telecommunications Company

It’s been said that people change their behavior when the pain of staying the same becomes greater than the pain of changing. You don’t want to reach the painful point of suffering a data breach before your employees change their behavior. By then it’s too late!

In the next section we’ll discuss the people-centric approach to security awareness and how its five elements work together to change the behavior of employees and make the organization’s culture security proactive.
CHAPTER 3

5 People-Centric Elements To Build Security Awareness

We’ve established that humans are the weakest link in the cyber security chain and we need to change human (employee) behavior to secure the organization.

We have also discussed why technology and processes aren’t enough to protect an organization. There must be a people component in any cyber security strategy.

93% of cyber security professionals agree that humans and technology need to work together to detect and respond to threats (like phishing attacks).

Source: Ironscales Email Security Report 2017

To change employee behavior and build a security culture, there are five people-centric elements to use as the foundation for security awareness success:

1. High Quality Content
2. Personalized Campaigns
3. Collaborative Partner
4. Security Awareness 5-Step Framework
5. Security Awareness As A Service
1. High Quality Content

High-quality, relevant content is central to any security awareness program in order to engage users and provide a training program that is fun, resonates and changes behavior.

Here are the five key factors that influence the quality of content and ultimately the learning experience for the modern learner:

1. **Content should be created by a team of domain experts**

Experts should understand adult learning, the psychology of changing behavior long-term, knowledge transfer, the most current cyber security trends and breaches as well as governance and privacy compliance requirements. Content should be created in-house by the vendor selected in order to provide a common look and feel across the content library as well as the ability to be agile and customize the content for a more personalized approach. Read more about campaign personalization on page 9.

2. **Proven pedagogical approach and methodology for adult learning**

Content developed with a proven pedagogical approach to adult learning will help users attain the highest degree of success. Such an approach is characterized by the following:

- Content is relevant and meaningful focusing on the “why”
- Instruction is task-oriented instead of promoting memorization
- Learning is self-directed for adult learners, with guidance provided when needed
- Locked, mostly linear navigation prevents the learner from “nexting” through the topic and requires interaction to move forward
- Content is narrated and displayed on the screen (cc closed caption) to accommodate both visual and auditory learning styles
- Courses can be customized to meet unique cultural requirements
- Teaser videos are included at the beginning of each module to engage the learner and introduce the topic
- Topic evaluations that are customizable – number of questions, randomization and scoring can be modified to suit each organization’s requirements
3. Microlearnings provide risk-specific content to reinforce security awareness behaviors

Microlearnings have the following attributes and your vendor of choice should have a comprehensive library that can be leveraged throughout your awareness program:

- Short 2D video with audio
- Focused on one risk, easily consumable bites of content
- Scenario-based branching design
- User decision making to allow a learner to see the immediate impact of making the right or wrong security decision
- Up to three minutes in length

4. Gamification for increased user engagement and motivation

Recent findings stress the need to adopt modern ways, such as gamification, to transfer new knowledge and information to learners. Gamification in training can improve motivation and engagement. Consider the following attributes for including gamification in content:

- Pedagogical approach to increase engagement and motivation
- Can complement the course test and provides a positive learning experience
- Real-time points accumulation displayed in leaderboard (peer ranking)
- Competitive strategy between countries, departments, roles
- Provides opportunity for incentive-based initiatives

5. Role-based content

Learning activities are designed with what the audience’s roles and responsibilities are within the organization, making the training significant and impactful. Roles within your organization that can benefit from role-based content due to the type and level of sensitive data they have access to include:

- Managers
- IT Administrators
- IT Developers
- Human Resources
- Marketing
Personalization of your security awareness program components and campaign elements is important for driving motivation among employees and increasing their knowledge retention rates to change behavior. If employees can relate to the content – whether by role, brand or images – they will be more engaged and retain the information more effectively.

Personalization touches a wide scope of areas in a people-centric security awareness program and includes:

**Content**
An employee’s role and responsibilities within the organization dictate their security awareness training requirements. While all employees require core security training programs, positions such as finance, legal, human resources, application development, IT and marketing require additional, specialized security awareness courses that focus on specific security issues pertinent to their roles. For example, HR employees may need specialized security training in handling employee records; software engineers may require additional training on secure development. By incorporating training modules that are role-specific you personalize the content increasing motivation and learning. You also can personalize content by format – quizzes, text, video, narration, etc. – depending on employee motivation assessments.

**Branding**
Adding corporate branding, such as logos, and corporate images of people, offices and products adds a level of personal connectivity during security awareness campaigns.

**Communication tools**
There are a variety of communication tools in a people-centric security awareness program, such as email, video, newsletters and posters. These can be personalized for improved attention and retention of message.

**Security awareness platform**
The people-centric partner you choose to work with on your security awareness program should offer platforms which can be personalized and customized to your company. The user interface should be familiar to the organizations corporate interfaces; the phishing templates should have the look and feel of your business, and the scenarios they depict should be relevant and personalized for your company.

**Language**
This is an especially important personalization point for global organizations. The ability to deliver security awareness training end-to-end in the native language of the country you operate in is important for driving motivation and knowledge retention. Cultural nuances must also be considered, and the ability to support multiple time zones with regional hosting is beneficial.
A cyber security awareness training provider is not just a supplier, but should be a collaborative partner. Seek out a company that engages in a consultative approach and will really take the time to understand your unique situation. The right partner has the experience and the subject matter expertise to help you plan and execute a security awareness program that is designed specifically for your organization.

By bringing in a partner, you have an expert team with the knowledge to assess and analyze the data to measure and optimize your security awareness program. Remember, you are not alone!

A consultative partner in security awareness will:

- Offer expert advice and coaching as you plan and execute your security awareness program. A partner should have an impressive track record in the security awareness field and have implemented a vast array of security awareness programs. A partner also will understand the potential roadblocks, anticipate challenges and be available to you throughout your campaigns.
- Provide expertise and knowledge transfer to make sure your programs are optimized to motivate users and drive behavior change.
- Work with you to take the data and assess results, pinpoint strengths and successes, and identify areas for improvement.
- Apply a proven pedagogical approach and methodology for adult elearning.

Best Practices

- Plan campaigns and build courses with automated results-based learning including foundational training, microlearning, phishing simulations and just-in-time training.
- Define a tailored awareness strategy to help address the different learning needs per group i.e. new joiners, champions, repeat clickers, etc.
- Identify the security awareness goals that will help your leadership approve and support your program.
- Determine metrics and KPIs to help measure the success of your program and align objectives to support your corporate business strategy and mission.
To reach any goal in life, it’s helpful to use a proven framework or path to get there. When aiming to complete a marathon, you wouldn’t cross the start line without any preparation. You would probably start training a long time in advance, following a training schedule - or framework, if you will - that can accommodate your schedule and guide you in your journey towards success.

The same holds true for security awareness. To effectively change employee behavior and build a culture of security, you need a comprehensive program that is carefully planned based on your organization’s specific needs and objectives. You can achieve this by applying a proven framework – an ongoing methodological approach consisting of the following five steps:

### 4. Security Awareness 5-Step Framework

#### Step 1 - Analyze

The “Analyze” step in the framework is essential to any security awareness program. A thorough analysis of the situation will give you all the information you need to build your security awareness plan with a solid foundation for success. And nowhere is it clearer that a people-centric approach to security awareness is the right route to take than in the analysis phase. Nearly every category in this step touches on people. Whether you’re identifying the target audience or assessing motivation, a focus on people – your employees – is critical.

As you do your analysis and assessment, you should focus on nine data-gathering categories:

1. **Program goals.** Your goals – what you want to achieve with your security awareness program must be defined so that you can properly plan all the steps to achieve them, including how you will measure if you’ve achieved them. Clearly defined goals also will help garner support for the program which will range from funding to employee time and executive backing. The buckets your goals will fall into could be: Risks and behaviors; security culture; and compliance obligations.

2. **Compliance.** Gathering all your organization’s compliance obligations will help you build a comprehensive awareness training program covering all your regulations. It also will help you identify the target audiences for these areas of training and whether they need both compliance and security awareness training.
3. **Target audiences.** Communication is a foundational part of any security awareness program. It is essential to identify the target audiences whose behavior you aim to change because that is the group with whom you will be communicating. Understanding your audiences is important for defining the topics and content your security awareness program will cover. You also will be better equipped to adapt your messages and communication methods to amplify the impact and effectiveness of your program. Audiences will include direct employees such as executives, managers, general staff and IT staff. Within those direct employees, you will want to segment specialized groups, such as software engineers, human resources staff or finance personnel, who may need additional, role-based security awareness training. You also will want to consider third party audiences such as contractors and vendors.

4. **Scope (topics and content).** Your audiences and your compliance needs will help define the scope of your security awareness program. There will be training content that is common to all target audiences and there will be audience-specific content required in the program. For example, executives and managers may require content on safe handling of sensitive information or common attacks targeting executives. Those in specialized roles, such as HR, may need content outlining privacy best-practices, while the IT service desk staff may require education on social engineering attacks.

5. **Level of knowledge.** Once you have your target audiences identified and you have scoped your program content, the next step is to assess your audience’s level of knowledge and understanding of security. This will help to design a program that brings new information to your employees to fill knowledge gaps and fuel behavior change. You can determine the current level of audience knowledge through surveys, simulations, risk analysis and audit reports and compliance status reports.

6. **Motivation and culture.** Motivation is the key to influencing behavioral change. You must get your target audiences to want to participate and act on the messages and learning. Awareness-raising activities are aimed at human beings. You must consider their needs and mindset when planning activities. Motivation is classified into three categories: intrinsic, where employees are willing participants in the security awareness program and will apply what they learned because they understand their role in protecting information assets; extrinsic, where employees are motivated by external factors, such as rewards or requirements instead of inherently feeling the commitment and drive; and amotivation, where employees are unwilling to participate and they don’t see the impact of their actions. The challenge for you is to move any amotivation employees to extrinsic or intrinsic employees. You can assess motivation using simple surveys.

7. **Support resources.** When choosing awareness-raising activities, you must consider your allocated budget and your support resources. Three key support resources are: upper management, which will legitimize your program and help get you the funding you need; security awareness champions, or employees who are intrinsically motivated and act as ambassadors of the program; and operational support, which comes from different departments, such as IT or HR, to help you engage in your security awareness program.

8. **Globalization.** You must determine whether you have global needs for your security awareness program, such as multiple languages and offices in multiple countries.

9. **Costs (resources).** Before you begin to plan, you should have an idea of what your security awareness program will cost. There are several considerations as you assess your cost: number of employees (or audience members) and fees associated with the content.
Step 2 - Plan

With the analysis and assessment complete, you are now ready to plan your security awareness program. Planning allows you to anticipate and address roadblocks, stay aligned with your objectives, stick to your timeline and budget and ultimately, 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.

During the planning process, you will make decisions in these six areas:

1. **Team.** Identify who will be on the security awareness team. Team members extend beyond the IT and security teams to fill roles such as project manager and communications advisor. For example, a senior executive is required to fill the role of sponsor. Other members may come from across the organization. Departments with a strong stake in security awareness, such as training, HR, communications, legal and compliance should also be involved.

2. **Roadmap.** Your security awareness program is your overall plan defined by the strategic goals. Your program consists of a set of smaller campaigns each designed to meet its own set of objectives. During the roadmap phase, you will be establishing program duration, campaign frequency, and campaign and course duration. Key items to consider during the roadmap planning are the security awareness maturity of your organization, dates that present conflicts or challenges in reaching your audience; and making sure you allow for pre-launch testing time, including time to personalize content, if needed.

3. **Product.** The product decisions you will make for your security awareness program concern the type of content and how it is delivered, as well as the tools you will use to measure its effectiveness. Make sure to use the data from your analysis as that will guide your product selection and help you determine your initial topics. That data also will guide the duration of the courses and will help you decide whether training is mandatory or whether a specific score is required to pass. There are multiple measurement tools that can be considered, including learning management systems, quizzes, simulations and assessments.

4. **KPIs and metrics.** The KPIs and metrics of your campaigns and overall program will allow you to measure your program’s progress and performance, providing you with important insights into its effectiveness. Your metrics should align with program goals and campaign objectives, and you must be able to capture them and ensure they are understood as you present your findings. Common categories for metrics include: Training participation rates, reported phishing attacks, decrease in click rate, training statistics, participant satisfaction rates, training effectiveness and return on investment.
5. **Communications.** To create your communications plan, you’ll need two components: a communications strategy and a communications calendar. Your strategy will outline who is responsible for developing content and materials. It also will include key messages, languages, preferred communications channel and the best times to communicate. Your communications calendar is the timing of all communication, for the program and campaigns.

6. **Business case.** At some point, likely early in your security awareness initiative, you will need to make the case for your security awareness program to the executive team, the security governance team or the security awareness team. The business case should include a brief introduction of the general state of cyber security and your organization’s current level of awareness. It also should include any legal or regulatory security awareness requirements, and cover your program components, from audience, scope (topics) and content to KPIs, the roadmap, measurement and the team.

---

**Step 3 - Deploy**

There are three phases in any security awareness campaign: test, launch and reinforce. Testing is critical and should be accounted for in the planning process. Testing helps avoid a complete failure of an entire security awareness program. If you sit down to devote the time to your training module and it fails to function properly, or your course credit isn’t registered when completed, how likely are you to want to try again?

There are three main types of pre-launch testing recommended.

1. **Content review.** 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.

2. **Compatibility and performance testing.** It is important to conduct a number of compatibility and performance tests with assistance from your IT and/or HR department to make sure everything is ready for your deployment.

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.

Testing will flag any issues and it will validate the flow and customization of content. Testing will also improve your probability of success. With successful testing completed, it’s now launch time.

As you deploy your campaign, clarity and communication are very important. These help ensure everyone knows what to do and helps to keep campaign momentum. An email or video sent by the security awareness program sponsor stressing the importance of the program or campaign to the organization is a great form of kickoff communication. Having “teasers” about the upcoming campaign on the intranet is another good way to get the hype started. Posters might even be used to tease that a special program is being launched.

Reinforcing the campaign with additional communication tools beyond email will keep security awareness top of mind, helping employees retain what they’ve learned and drive continued behavior change. 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.
Step 4 - Measure

Taking the time to assess the performance of your security awareness activities provides valuable information that can be used 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.

In this step you should measure performance, participant satisfaction and compliance. This is the data you should gather:

**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.).

**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.

By tracking progress, you will be able to effectively manage your campaigns and program. Then report this progress by communicating information about campaign performance to departments across your organization and demonstrating adherence to compliance requirements.

**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.

**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 security behaviors.
Step 5 - Optimize

One of the most significant benefits of measuring performance, participant satisfaction and compliance is that you will have the context to identify areas for improvement and start developing an action plan to address them. You will find opportunities to improve in a specific campaign or in your overall program. To pinpoint areas for optimizing, you may want to consider the following:

- Analyze your metrics from Step 4: Measure. Investigate statistics, interpret data, validate assumptions and take any necessary corrective measures.
- Compare your results with your campaign objectives and program goals. Assess the current situation and any gaps in your security awareness program.
- Identify improvement opportunities. Optimize your campaigns based on your KPIs and metrics.
- Identify new objectives. Determine changes in training and behavioral objectives for a follow-up campaign.
- Conduct a postmortem meeting. Share this insight with stakeholders and your team to identify areas for improvement.

Without a methodological security awareness framework, it will be difficult to get people to change their risky behavior. A framework is designed to take everything into consideration, especially how people learn, adopt and maintain new habits, which ultimately leads to a culture of security awareness and dramatically fewer human-connected security breaches.
Choose the best security awareness delivery model for your organization

Your organization's structure and needs will dictate the onboarding model you choose for your security awareness program. Many factors come into play when selecting whether you will self-manage your program, if you will choose to have your partner manage the program in a security awareness-as-a-service model; or if you will select a hybrid model for a combination of both.

Security awareness as a service

Security awareness as a service provides flexibility and support to effectively deploy your phishing simulations, awareness training or both as well as measure and report results. Here are some of the key elements to consider when evaluating this option:

- Dedicated customer success manager
  - Will partner with your organization and ensure the success of the security awareness program
- Import user lists into security awareness platform
- Launch security awareness training including:
  - Content customization
  - Pilot group
  - Administrator support
- Launch phishing simulation including:
  - Template customization
  - Pilot group
  - Email management
  - Administrator support
- Post-campaign feedback
- Reporting on phishing simulation and security awareness training
- Flexibility to select number of annual security awareness training campaigns and phishing simulations
The chart below simply explains what an organization may opt for in a certain scenario. For example, if you have ample staff and have expertise in security awareness training and phishing, you may choose just the products for content and delivery. But if you have limited staff and limited expertise in phishing simulation and security awareness, you may want to choose the option that heavily involves your partner and extra CISO coaching.

<table>
<thead>
<tr>
<th>Choosing your Security Awareness Program Platform Delivery Model</th>
<th>Expertise in awareness and phishing</th>
<th>Limited expertise in awareness and phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Staff available to manage the program</strong></td>
<td><strong>Products</strong></td>
<td><strong>Products</strong></td>
</tr>
<tr>
<td></td>
<td>- Courses</td>
<td>- The Human Fix to Human Risk eBook</td>
</tr>
<tr>
<td></td>
<td>- Platforms</td>
<td>- CISO coaching session</td>
</tr>
<tr>
<td><strong>Limited staff available to manage the program</strong></td>
<td><strong>Products</strong></td>
<td><strong>Products</strong></td>
</tr>
<tr>
<td></td>
<td>- Security awareness as a service</td>
<td>- CISO coaching</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security awareness as a service</td>
</tr>
</tbody>
</table>

No matter what model you choose, you should be able to benefit from a consultative approach, which is supported by CISO coaching, a dedicated project manager and personalized training. You should also have the flexibility to pivot from one delivery model to another as your business needs shift or budget changes.
Conclusion

In the 30-minutes or so it has taken you to read this guide, nearly 400,000 records were breached around the world. Although most organizations have some form of security technology in place to help protect their data and the personal information of their customers and employees, not all organizations successfully address the human risk employees pose to an organization. Because employees are human, not operating with a security mindset, and can make mistakes, they are the weakest link in the cyber security chain.

Phishing simulation and security awareness training can make a difference. When asked in an interview how he would spend an extra dollar on cyber security, Gregory Touhill, former United States CISO, said he would spend it to better train his people.

Effective security awareness programs can reduce risk to an organization by helping to change employee behavior, instill or reinforce a culture of security within the organization, and address compliance demands. But it takes a human fix to battle the human risk.

A people-centric security awareness program is just the human fix your organization needs to motivate your employees for long-term behavior change and impart the knowledge to operate with a cyber security mindset.

Learn how people-centric security awareness continues to train millions of cyber heroes, change behavior and instill security culture globally.