IMPROVING SECURITY AWARENESS USING MARKETING TECHNIQUES
CONTENTS

4 Awareness Programs Today
5 Overcoming Training and Awareness Challenges
   5 / Sales Funnel
   7 / Creating Personas
   7 / Purchase Intention
8 Building the Awareness Program
   9 / Metrics and Measurement
   9 / Validation and Assessment
9 Conclusion
10 Acknowledgments
Security awareness and training is an important control in the security practitioner’s toolbox that helps enterprises to respond better to security threats, that prevents behavior that enables security incidents and, in many cases, is required for regulatory compliance.

Despite the importance of information security awareness and training, many enterprises do not employ it very well or systematically. For example, few enterprises track and measure the effectiveness of their information security awareness campaigns beyond a few simple metrics, e.g., phishing simulation clicks. This lack of sophistication undermines the potential benefits of higher-quality awareness campaigns that are managed with the same level of effort as other security controls such as planning, implementation, and reporting of measurement and metrics.

With just a few adjustments to how your enterprise plans, creates and manages awareness activities, it can build awareness campaigns that are more engaging and perform better. By adapting the techniques that marketing teams use to gauge their brand awareness and interactions with potential customers, your enterprise can get better engagement from end users and more reliably achieve the results intended from security awareness campaigns.

This white paper outlines how to systematically build and launch more effective security awareness efforts, and how to integrate those efforts into your enterprise’s broader security program.
Awareness Programs Today

Measuring the performance of security awareness activities can be difficult, in part, because the underlying goals of a security training and awareness program influence the metrics that are gathered. For example, a hospital required to comply with the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) might define success as all employees watching a webinar, but a different hospital with the goal to reduce the risk of unattended and unlocked nursing workstations might not view an awareness campaign to be successful until the user behavior has actually changed.

This means that there isn’t a standard “one size fits all” set of metrics to evaluate how awareness efforts perform across industry. Even without a common standard to use as a benchmark, research suggests that most security awareness and training programs aren’t working very well.

An Osterman Research, Inc., survey shows that security professionals rate users’ ability to handle phishing attacks with a confidence level of 64 on a scale from 0 (not confident at all) to 100 (very confident).1 One reason may be that awareness and training programs are not prioritized effectively in most enterprises. The 2018 SANS Security Awareness Report reveals that 80.8 percent of security awareness professionals who are directly responsible for awareness in their enterprises spend less than half of their time dedicated to awareness activities.2

As a result, security practitioners are not confident in program results.

Although those data points report the amount of time invested and the confidence level in the performance of security-awareness efforts, the data do not report how well security efforts work. To evaluate how well security awareness and training performs directly, one needs to look at user behavior, specifically at how well security awareness efforts change user behavior. In a 2016 study of social engineering, researchers from the University of Luxembourg found that 48 percent of users agreed to exchange their passwords for a bar of chocolate. Moreover, 30 percent of those they approached would give out their passwords without being offered anything in exchange.3 Social engineering tests conducted during the 2017 annual DEF CON and DerbyCon Social Engineering Capture the Flag (SECTF) found similar results. “The 2017 Social Engineering Capture the Flag Report” states:

...[S]ocial engineering continues to be a security risk for organizations... we have not seen consistent improvements that directly address the human element in organizational security. Even as companies are reportedly investing more in security awareness training and policy development, the results again this year support our belief that overall, companies are still doing a relatively poor job.4

---


© 2019 ISACA. All Rights Reserved.
Overcoming Training and Awareness Challenges

Security awareness campaigns can underperform for many reasons including:

- **Lack of effective messaging**—Lackluster content that fails to achieve the desired outcome
- **Lack of engagement**—Failure to appropriately engage the user or failure to communicate the importance of good cyberhygiene and its impact on the enterprise
- **Campaign design**—Inapplicable or mistargeted campaigns, or content that is too densely packed into a communication channel, causing the audience to stop listening

These specific challenges have been extensively studied in the marketing field. Marketing professionals spend tremendous effort and time measuring how their efforts to optimize content, to increase engagement, and to target campaigns to the intended audience perform. Adopting and leveraging methods used by marketing professionals can be a successful strategy for security managers and executives who want to overcome challenges in security awareness and training efforts.

Methods used by marketing professionals to create a campaign include:

- **Effective messaging**—Create content that is targeted to a specific outcome. Many security awareness campaigns are launched without a clear objective. Effective marketing, instead, seeks to create collateral that is designed with the outcome of moving a customer along a journey from noncustomer to customer. Each advertising or marketing element is designed to move the potential customer along that process.

- **Engaging structure**—Present information in a format that is engaging to the consumer. An engaging structure can employ white space strategically to enhance the message, contain text that is accessible (free of security jargon) and that is delivered in a manner that is familiar to the customer.

- **Consumable units of information**—Ensure that information is modular, so the user is not overloaded with too much information at once. Rather than a single piece of collateral that attempts to communicate everything at once (for example an awareness-oriented poster that includes information on safe web browsing, good password habits, screen lock habits and numerous other things) a campaign can be structured so that individual elements reinforce each other and are targeted at different phases in the customer purchasing journey.

- **Trackable and measurable**—Create collateral for which engagement can be measured. Marketing teams might collect information about how many people view a given piece of collateral, how many of those people take a next step (e.g., click a link) and how many people share the information with others, etc.

Marketing teams use some key principles and tools to support these methods. Chief among these are:

- Sales funnel
- Customer personas
- Purchase intention

Each tool can be valuable to creating awareness campaigns, optimizing awareness collateral and managing the awareness program over time.

Sales Funnel

The sales funnel describes the steps along a journey for a potential customer. The potential customer journey begins at a state in which the customer knows nothing about the enterprise’s product and ends with the customer making a purchase. Although adaptations exist with more or fewer stages, a typical sales funnel has the following four primary phases:

- **Awareness**—The potential customer becomes aware of the enterprise goods or services.
- **Interest**—The potential customer becomes interested in the offered goods or services.
- **Decision**—The potential customer decides to purchase the goods or services.
- **Action**—The potential customer takes action to initiate a purchase.

The customer journey is described as a funnel because only a subset of customers entering into each phase proceed to the next phase (figure 1). Some potential customers cease their journey along the way. As a result, when the journey is depicted top-to-bottom, the shape is similar to a funnel.
The sales funnel can be a powerful tool because it can help marketing teams understand and refine specific areas in which they may be weak, resulting in fewer new customers. An enterprise that wants to make more sales can systematically analyze where it is weakest and put mechanisms in place to help customers along their journey. For example, some potential customers do not know that the enterprise's product even exists. In that case, the enterprise can invest in top-of-funnel activities to bolster awareness of the product. Another enterprise may determine that it is having trouble generating interest after potential customers become aware of the product or service. That enterprise may decide to invest in messaging that highlights the product's value or appeal.

Security managers can use the sales funnel tool in the same way. For example, to evaluate the effectiveness of awareness activities along an awareness funnel, the beginning of the journey is when the users have no awareness of security considerations and the journey ends when the users are fully security conscious. Also, the users exhibit the behavior that the policy requires. Similar to marketing teams, security managers can measure performance at each stage to understand where and how efforts are falling short. Based on these measurements, they can develop and test strategies to optimize the performance of the stages that are most challenging.

There are some obvious differences between using the sales funnel to develop a sales pipeline and using it as a tool for security awareness. For example, many enterprises selling a product may be willing to tolerate loss of those who show interest but will never convert to customers. This subset of individuals represents a predetermined acceptable range of loss for the enterprise. Although this type of loss may be acceptable in a sales context, it is not acceptable in a security awareness context. Those individuals who do not proceed from one stage to the next stage in the security arena represent a potential source of unaddressed risk for the enterprise.

Despite these differences, the method of analyzing security awareness and training as a campaign — in which each stage has a desired outcome and the outcome of each stage can be measured — provides potentially tremendous advantages in the ability to measure the effectiveness of awareness materials.
Creating Personas
Customer personas involve establishing profiles of customers to create tailored content for individual consumers. In marketing and sales, it is a common practice to segment markets to allow tailored outreach within a subset of the market, allowing the enterprise to adapt existing content to different types of purchasers. This practice maximizes the appeal of products based on influencing factors that subsets of potential customers may share. In other words, a persona describes the ideal customer in a generalized, abstract way. These personas are typically based on prospect and customer research, detailing the wants, desires, motivations, buying habits and other information about the customer.

A persona helps outreach in a few ways. First, it can help enterprises refine their messaging by understanding the buyer on an emotional and an intellectual level. By understanding customer motivation, interests, and communication preferences, the enterprise can present a message that engages the customer’s attention, is resonant with customer experiences and interests and is presented optimally to elicit engagement. A persona can also be used to better understand the costs and actions required to acquire particular types of buyers as customers. An enterprise may decide that acquiring a certain type of customer requires fundamental changes to the way that a product or service is delivered. If the enterprise is not prepared to make those changes for some reason, it may decide to forego (temporarily or permanently) targeting those customers.

In a security awareness context, this technique is also valuable. For example, by examining and systematically charting how users prefer to communicate, enterprises can tailor mechanisms to best engage with users. For example, an enterprise can tailor what it sends, how it engages, its methods of delivery, the voice it uses, and numerous other elements about its awareness efforts to better move its audience from one stage of the engagement funnel to the next stage. Each stage of the awareness funnel performs better as a result. Note that the specifics will vary from enterprise to enterprise and from persona to persona. As a consideration, younger professionals may prefer communicating using an application, like Slack while the sales team may prefer a long-form memo that they can print out and take with them on the road.

A critical difference between using personas in a marketing context versus for security awareness is that marketers may decide that the cost of acquiring a certain type of customer is, based on their persona, more effort than it is worth. In a security awareness context, however, an enterprise cannot discard a segment of its user population because they are too challenging (or expensive) to reach. In that instance, the enterprise can tailor and position its outreach efforts to that persona in order to achieve the desired behavioral changes.

Purchase Intention
The last marketing method outlined is analysis of customer purchase intention: purchase intention is used to measure how likely a consumer is to buy a particular product within a given time period. An example is a questionnaire that asks customers, “how likely are you to buy a new appliance in the next six months?” The purpose of the questionnaire is to measure purchase intention. This is a powerful tool for understanding market size and predicting the sales pipeline, but, when used in combination with the other two tools, purchase intention becomes even more powerful. Why? First, knowing where consumers are in their customer journey helps marketing teams to understand the dimensions of the sales funnel. Meaning, it gives marketing teams insight into how many consumers are considering a purchase, how many consumers have decided what they are going to buy and when. So, before marketing teams create marketing collateral, they have a rough idea of how many consumers are in each stage of the funnel. Secondly, when used in combination with customer personas, purchase intention helps enterprises to understand the types of consumers (based on their persona) who are more likely to make a purchase over a given time period. This information helps enterprises to understand the acquisition cost for different types of customers and whether/when a given customer segment will be likely to make a purchase.

Similar to the other tools, purchase intention can be adapted for security awareness by measuring users’
anticipated behaviors in response to hypothetical security relevant situations. Enterprises can present a scenario to users and ask them how they would respond. The users’ responses give the enterprise an understanding of the effectiveness of campaigns that it has launched. For example, by asking users similar questions before and after they are exposed to awareness materials, the enterprise can gauge users’ understanding and retention. The enterprise can couple this information with the personas to understand which segments of the user population are most in need of security awareness, relative to other segments.

Building the Awareness Program

The marketing principles and tools described here can be applied as useful security awareness strategies, but they represent a portion of the effort. The overall approach to managing the security awareness program is the other (arguably more important) part of the effort. Whether the enterprise is setting up a program for the first time or refining/updating an existing program, several elements need to be considered. One way to approach the program is to segment the program into the following phases.

1. **Campaign planning**—development of campaigns that are designed to educate users about a specific message or to reinforce a message
2. **Collateral creation (or adaptation)**—creating or adapting training or other material into campaigns
3. **Campaign execution**—conducting training and disseminating materials
4. **Campaign management and tracking**—tracking attendance or measuring performance of the program

During **campaign planning**, the enterprise plans what it will deliver based on areas of need. Before or during the planning process, the enterprise identifies personas to determine the specific topics and messages that are most important based on enterprise need, the type of user, users’ communication preferences and the jobs that they perform. Combining persona information with data that gauge how users are likely to respond to security relevant situations forms a baseline that can be used to evaluate the effectiveness of the enterprise awareness program and to identify the user areas that have the most need. An enterprise may need to have multiple campaigns depending on the diversity of its user population and their areas of need (and persona type).

Next, during **collateral creation and campaign execution**, the enterprise plans the materials, messaging and engagement strategy for each campaign. This collateral should align with the goals of the campaigns and be driven by user personas (e.g., the manner in which users prefer to consume the information). Incorporate the sales funnel into the planning by thinking through the messaging that is required to move users from one phase of the journey to the next phase. For example, the enterprise may produce collateral that is designed to generate cognizance of security, other materials to solicit user interest and more in-depth materials for the user to gain additional detail to complete the training with sound comprehension.

Think through the metrics that the enterprise will collect as part of **campaign execution**. This allows the enterprise to determine where users are in the journey, how successful the efforts are at moving users from one stage of the awareness funnel to the next phase and how users respond to each campaign overall. User fatigue, which is often the result of the repeated exposure necessary for reinforcement, can be countered by staggering campaigns and collateral. As multiple campaigns are part of the awareness program, thought should be given to how campaigns will be compared to each other for overall campaign effectiveness.

Lastly, begin the ongoing process of **managing and tracking campaigns** over time. Consider two important areas:

- Metrics tracking
- Validation and ongoing assessment
These two areas merit additional discussion because of the importance that they will have in future campaign planning.

**Metrics and Measurement**

As with other enterprise processes or controls, measurement of the security awareness program’s effectiveness is critical for improvement. Measurements that can be evaluated include:

- **Reach**—the number of people with whom the enterprise has engaged over a given time period
- **Views/Hits**—the number of times that a video, page or link was accessed by users, or the number of emails opened
- **Engagement**—the time spent on an information resource, or the length of time spent engaging with content
- **Completion**—the number of individuals that have completed a training module, watched a video to the end or completed a quiz about the presented information
- **Shares/Likes**—the degree to which users share the information with others
- **Interactivity**—how frequently users interact with collateral, such as how long users spend on an informational webpage, how many actions they take while they are on that page, etc.

Ideally, enterprises should compare and review metrics at the collateral and program levels. Both metrics are valuable, but for different reasons. Tracking a given piece of collateral allows an enterprise to rank collateral to see which pieces work best. Looking at a campaign as a group lets an enterprise evaluate progress against the specific goals that it intended for the campaign to achieve. Looking at the whole campaign, program-wide, lets an enterprise measure the performance of its overall awareness. This measurement is valuable for reporting to executives and for evaluating overall progress.

Factor cost and economics into the analysis, to the extent possible, to understand the amount of risk-reduction impact from the awareness activities, relative to the amount of time/budget invested. This comparison can help to justify the need for continued investment in the awareness program. It can also help with decisions around keeping awareness efforts in house or outsourcing/cosourcing portions of the program to service providers.

**Validation and Assessment**

Whether for regulatory compliance, to support internal or external audit, to bolster robust security practices or to report progress to executives, unbiased validation of security awareness efforts is valuable. Metrics are part of this, but they are not the entire story. For example, metrics show the effectiveness of collateral/campaigns, but they do not show the overall risk reduction impact that awareness activities are having overall. To evaluate risk reduction impact, information about enterprise risk is required, i.e., the risk that awareness efforts are expected to reduce and the effectiveness of those efforts. The ongoing evaluation of performance can be synergistic with risk management efforts.

**Conclusion**

This white paper focused on specific tools that enterprises can use to improve security awareness efforts — techniques that enterprises can leverage and overall awareness program management. By leveraging the same techniques that marketing teams use to best reach consumers and influence their behavior, enterprises can make their security awareness efforts stronger and better organized, and tailor the specific collateral they use. Organization and planning in security awareness are the keys to success, whether the enterprise develops materials internally or it chooses to work with a trusted external partner.
Acknowlegements

ISACA would like to recognize:

**Lead Developer**
Ed Moyle
CISSP, USA

**Expert Reviewers**
Robin Lyons
CISA, CIA, USA

Sushila Nair
CISSP, USA

**ISACA Board of Directors**
Rob Clyde, Chair
CISM
Clyde Consulting LLC, USA

Brennan Baybeck, Vice-Chair
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Leonard Ong
CISA, CRISC, CISM, CGEIT, COBIT 5
Implementer and Assessor, CFE, CIPM, CIPT, CISSP, CITBCM, CPP, CSSLP, GCFA, GCIA, GCIH, GSNA, ISSMP-ISSAP, PMP
Merck & Co., Inc., Singapore

R. V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CRISC, COBIT 5 Foundation, GRCP
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
Cyxtera Federal Group, USA

Ted Wolff
CISA
Vanguard, Inc., USA

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5
Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

Theresa Grafenstine
ISACA Board Chair, 2017-2018
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA
Deloitte & Touche LLP, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
INTRALOT, Greece

© 2019 ISACA. All Rights Reserved.
About ISACA

Now in its 50th-anniversary year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its 460,000 engaged professionals—including its 140,000 members—in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

About InfoSec Institute

At Infosec, we believe knowledge is the most powerful tool in the fight against cybercrime. We help IT and security professionals advance their careers with a full regimen of certifications and skills development training. We also empower all employees with security awareness and training to stay cybersecure at work and home. Founded by smart people wanting to do good, Infosec educates entire organizations on how to defend themselves from cybercrime. That's what we do every day—arming everyone with the latest security skills so the good guys win. Learn more at infosecinstitute.com.

DISCLAIMER

ISACA has designed and created Improving Security Awareness Using Marketing Techniques (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

© 2019 ISACA. All rights reserved.
Knowledge is the only impenetrable firewall.

Get your FREE security awareness kit to educate employees

www2.infosecinstitute.com/campaign-kit/