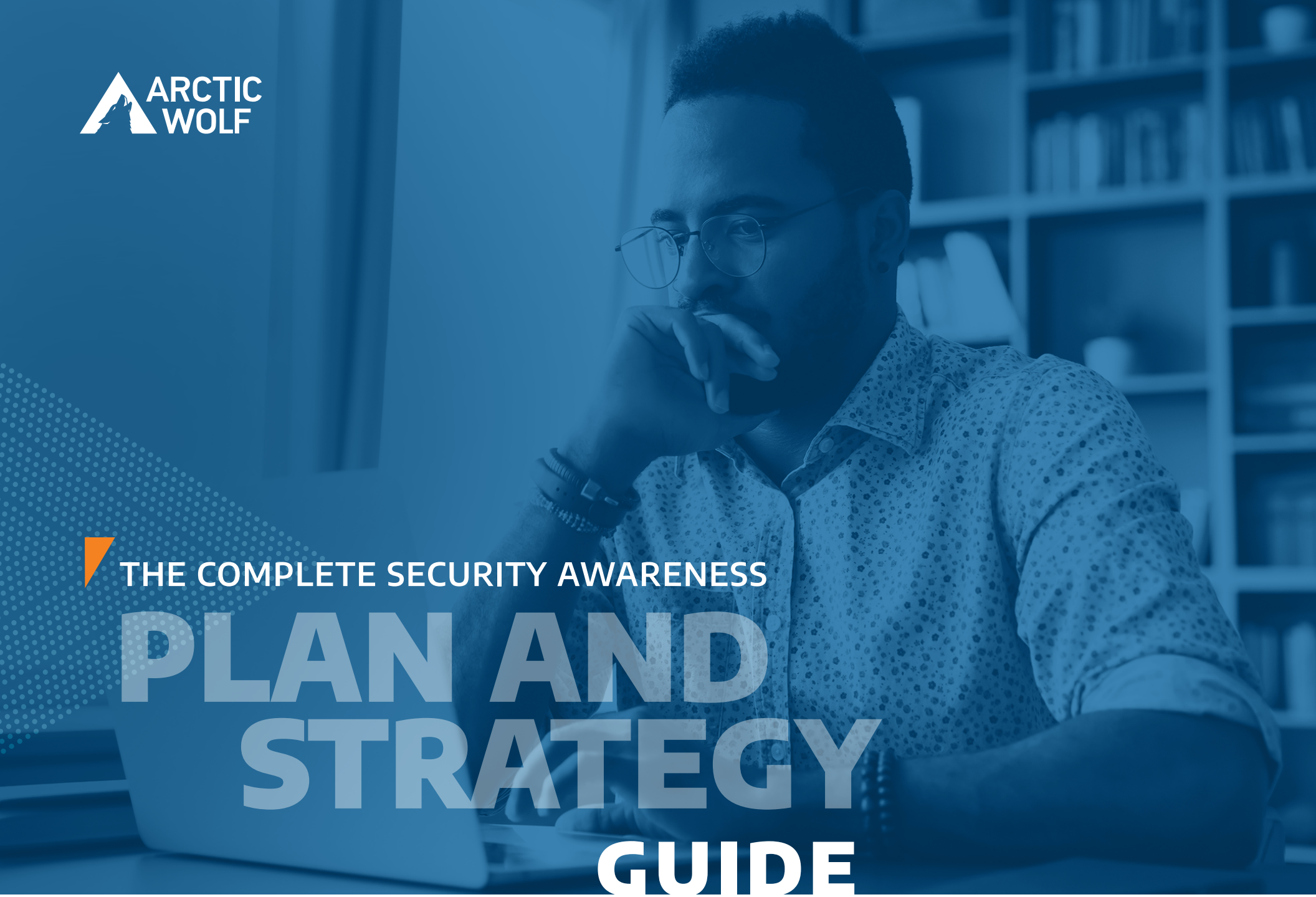

ARCTIC WOLF

THE COMPLETE SECURITY AWARENESS

PLAN AND STRATEGY GUIDE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This guide provides you with actionable guidance and strategy for establishing and maturing your security awareness program. The insights in this guide are based on real-life experiences from the experts who created the security awareness programs for The Walt Disney Company, Sony Pictures Entertainment, Activision Blizzard, and other leading firms.

Security awareness is a highly important function and will have by default, high visibility and impact across the company. It is one of very few programs that regularly interacts with employees, and this fact is something to always keep in mind.

Clearly defining and communicating your security awareness goals and initiatives is the lifeline of your program. Programs that don't engage with your employees or don't connect with the unique culture of your company will quickly fail. Think of it as "security marketing." We're trying to do the same thing as consumer brands: influence a person's decision-making process by effectively communicating the value of the program to the organization and individual user. We're doing it to get users to make better security decisions. Makes sense, right?

A crucial element to the success of your program involves establishing a series of goals and initiatives that gain approval from a small, internal committee. In this guide, we've outlined goals we feel have the greatest impact and have proven successful across multiple organizations, each with their own unique needs.

You'll want to define the purpose of your program. Being able to state this clearly and simply will come in handy over time, trust us. On the next page is a soft example of what we suggest.

The 15-20 minutes you spend reviewing this document will save you dozens of hours on things like having to continually restate the importance of a formal security awareness program, securing budget, and avoiding confusion about why your program isn't working, among other unwelcome activities.

CHOOSING YOUR MISSION STATEMENT

01

Program Mission Statements

At its foundation, the goal of the security awareness program is to change behavior through education. In order to achieve the desired changes, select a mission statement that reflects the outcome you aim to achieve. Some options include:

01 ***Nurture a culture of security***

02 ***Create a secure-minded workforce***

03 ***Strengthen the human element of security***

04 ***Communicate the correct security behavior***

05 ***Avoid the front-page headlines in the news***

Selecting your mission statement is the first step in building a security awareness program that will identify risky habits and replace them with secure ones and instruct users on how to recognize the signs of an attack and how to react to an attack. This is a long-term, custom program designed to meet compliance and legal requirements as well as change behavior.

DEFINING ROLES & RESPONSIBILITIES

02

Now that we have stated the mission of the program, you'll want to define who does what within the program. Roles, titles, and responsibilities around a security awareness program are going to be very different from company to company.

Recognizing this fact will help you build a culture of security with less resistance. Here are the essential roles required for an effective program:

Manager, Security Awareness

Ideally, the security awareness program should be managed by a dedicated individual, focused on building and maturing the role and initiatives of the program. This should be a senior-level management role, or equivalent, within the information security or risk teams.

Historically, successful roles similar to this pull from the creative, right-brain world, and combine that with an aptitude for, if not prior experience in, security awareness.

Select someone with soft people skills, high emotional intelligence, and powerful communication abilities. You likely have enough technical resources and SMEs for this role already, however creativity and effective communication are typically harder to teach.

The security awareness manager's biggest responsibility is to use their influence and leadership to execute a multi-faceted program that permeates through all areas of the organization. They need to be a bridge builder between the technical and the non-technical aspects of the program, as well as those that represent such roles.

What's more, they need to be a talented educator and motivator. An essential component of the position is to get employees to recognize and understand how they specifically contribute to the security of the organization, as well as how security and proper cyber hygiene is directly tied to the organization's success.

Because of the nature of traditional security awareness solutions, the security awareness manager may spend most of their time in an administrative role. They will have a full plate building out campaigns, as well as reviewing and editing content and phishing simulations. Alternatively, they can hire an administrator to oversee the execution of the program, or instead choose a solution that can manage all the administration tasks of the awareness program.

Some organizations may choose a DIY approach for creating and sharing content among their employees. This approach should be reserved only for those with someone who is an experienced teacher, security expert, and program administrator all rolled into one. Because it takes talent in all three areas to run an effective security awareness program helps people change their behavior.

CISO

It is critical that senior leadership across all stakeholder departments acknowledge the importance of the role and provide appropriate support. When possible, the security awareness manager should have a direct line of communication with the most senior information security leadership, typically the CISO, CTO, or CIO.

The CISO needs to champion leadership roles and values of the program. The CISO can provide input and guidance regarding executive board concerns and, in turn, represent the goals of the program to senior leadership. They should gain buy-in of the executive board to provide top-down, unified support for the security awareness program.

CEO

The CEO plays an essential role by endorsing the goals of the program as well as the methods you plan to use in your program. For their part, the CEO should always be kept informed of the program's performance by the CISO or corporate communications manager.

Corporate Communications: The Ongoing Relationship

All mass communications should be coordinated and approved by your communications department. This includes messages to large groups, company-wide distributions, and any content being delivered to "all company."

ESTABLISHING AN ADVISORY BOARD

03

Do you know how companies get big things to happen internally? They have planning committees, and steering committees, and board members. The purpose of these groups is to help establish the program's goals and make sure every stakeholder is represented. These committees are powerful tools, so we suggest establishing one right from the start. When created with purpose, it will become a key factor in your program's success.

Advisory Board

The advisory board should consist of various members from the information security department as well as some key stakeholders from other departments.

The role of the advisory board is to assist the security awareness manager with planning, executing, and maintaining a successful and engaging program. Committee members should be considered from among the following positions:

InfoSec Stakeholders

IR, vulnerability management, governance, privacy

IT

Email, architecture, helpdesk, etc.

Legal Risk

Corporate communications, human resources, marketing

IDENTIFYING KEY USERS & ROLES

04

Once you've established an advisory board, you can move forward with your overall plan and begin to identify your key users and roles across the company who will need advanced training in addition to the training most learners will receive.

It's important to know who makes up your environment, so you can provide knowledge appropriately. Good security awareness policy doesn't need to be too complicated and can be developed at a high-level.

Who to Train

Once you create your list of groups of people to train, answer the following questions:

Why does this group need to be trained?

How does the training need to be administered?

What does this group need to learn?

Are there any unique requirements for this group?

Try to identify specific types of roles or users who, in addition to receiving required training, may need a custom course of training, delivery method, or additional topics.

In the upcoming pages, we offer a generalized look at the four most common groups of employees to consider as you map out your security awareness journey:

01 Full-Time Employees

Full-time employees typically work 30 hours or more per week. These employees are not limited by contractual or legal regulations, such as contractors and consultants, and typically receive compensation benefits and payment directly from the company. Full-time employees must complete compliance-related trainings per policy.

Unique Requirements

Full-time employees tend to be set in their ways and are often more resistant to change. Getting this group to adopt new behaviors requires frequent and effective communication. Clearly state the purpose of training and end benefit to the organization as well as the individual employee.

04

Why?

Often full-time employees are used to assess a baseline of knowledge and behavior expectation across the company. This helps address the most common risks in an organization and provides the quickest compliance completion. This is as close to "check-the-box" compliance as it comes.

However, full-time employees must be treated as much more than a baseline requirement. After all, they are likely to have more access to data and an inner working knowledge of the organization itself. Thus, they may overly trust and allow fellow employees to take shortcuts, circumventing security practices or policies.

And, keep in mind, they may also be the most likely to resist change. This can include new forms of training, such as the security awareness program you plan to implement.

How?

Ongoing required online and live training, phishing training, and new-hire orientation.

What?

Ongoing security awareness education, keeping security defenses, best practices, and cyber hygiene top of mind. Security policy highlights, data classification, acceptable use policy, what is an incident and how to report it, regulatory requirements (PCI, SOX, HIPAA, etc.).

02 Privileged Users

This includes any user whether that be a full-time employee, contractor, or consultant, with privileged or elevated access to any IT resources, customer relationship management (CRM) platforms that hold prospect and customer personal data, electronic health record (EHR) systems, or payment processing tools. Common examples include system administrators, database administrators, network engineers, developers, helpdesk, payroll, human resources, accounts payable, and accounts receivable.

Unique Requirements

Involve an ambassador from each technical group for the development and delivery of technical, specialized security training and role-based requirements. Equip each ambassador with an understanding of where the program is succeeding as well as any areas for improvement that they are in a position to support.

04

Why?

These users require technical training based on their role and must acknowledge and always consider the power and associated risk of their access. Non-full-time employees must provide confirmation of completed training from their source company prior to accessing the network.

Social engineers frequently target and impersonate privileged users in phishing attacks. This is because of privileged users' access to data, their information about processes, and their ability to approve and or make changes within organizational systems.

How?

Ongoing, online and live training, course certification, onboarding requirements.

What?

Password practices and management, security considerations for the software development lifecycle (SDLC), role/industry appropriate, phishing training.

03 C-Level Executives and Their Support Staff

C-level executive roles and their support staff, such as administrative staff and assistants, represent a unique risk as access may be connected at the hip. Often, executive level access is delegated to support staff. Training both roles with a custom program that addresses their unique level of risk provides significant value.

Unique Requirements

Executives most likely require in-person, custom training. Leverage executive assistants to help train and guide their bosses. The assistants should be the first to receive training, as they usually provide clear insight into the habits and behaviors of their bosses.

Assistants frequently execute on many tasks asked of the executives. And an assistant may have authority to request payments and perform other requests or actions without any checks and balances, making them an equally attractive target as their executive boss.

As a result, executive assistants need to be closely trained on identifying phishing attacks and know that social engineers will always attempt to impersonate their executive bosses to trick and victimize them directly.

04

Why?

These individuals represent a high risk to the company due to daily access to highly sensitive information, international travel, and sometimes a habit of making and following their own rules.

Often C-level executives use their authority to exempt themselves from security awareness training. This is NOT recommended. Leaders shouldn't develop a reputation of disregarding security practices and policies.

They are often the most imitated position in an organization and the majority of a social engineer's efforts are successful when they convince another employee to go outside normal policies and make exceptions. If a privileged user has established a firm reputation for abiding and upholding policies and procedures and promotes the security awareness trainings, targeted employees will have higher confidence in turning down and reporting an impersonation attack when it takes place.

How?

Ongoing online and live, in-person sessions with a custom white-glove feel. Direct meetings and reports from the CISO to the CEO monthly.

What?

Training that is curated for specific behaviors and concerns of the role, company culture, and job requirements. Emphasize and educate executives on the key role they play in top down promotion of the security awareness program. Educate executives on the few key metrics they need to have insight. And, importantly, educate the executive on the responsibility they have in the event of security incidents.

04 Contractors and Temporary Staff

HR, IT, interns, consultants, and other external, non-full-time employees working within the network, with access to the same data as employees. Some may be assigned company email addresses; others may be provisioned segmented network access.

Unique Requirements

This group most likely requires custom training during the onboarding period. Legal team should provide guidance on possible limitations regarding such training, but have a definitive support structure for providing training as written into contracts.

Why?

These groups represent a high risk to the company because of limited training. Often these users have elevated or privileged network access as full-time employees yet are not mandated by the same training requirements due to contractual, legal limitations. Nonetheless, contractors should be treated the same as their full-time peers from a risk perspective and receive appropriate training based on role and access.

How?

Onboarding process, ongoing online training, and continual annual verification of knowledge and certifications via the sourcing vendor. There should also be a formalized offboarding process/ training to ensure there are no loose ends when a temporary employee leaves.

What?

Password practices and management, Security considerations for the software development lifecycle (SDLC), and role/industry appropriate program.

BUILDING YOUR TRAINING

05

Now that you've identified who you need to train, determining what to train them on becomes slightly easier. Typically, this includes topics you'd expect to be included as part of security awareness training but should also include topics specific to your culture and roles.

What to Train

Focus on a small number of topics and behaviors that represent the greatest risk to your organization. Identify these risks by meeting with senior Infosec leadership, reviewing past incidents caused by employees, and evaluating industry reports, including the Verizon Database Incident Report (DBIR). In addition, several topics may be required for compliance or regulatory requirements. Traditional cybersecurity awareness training includes:

- ***Policies***
- ***Reporting***
- ***Phishing***
- ***Social Engineering***
- ***Ransomware***
- ***Mobile Devices***
- ***Social Media Policy***
- ***Remote Working***
- ***Wi-Fi***
- ***Security Passwords***
- ***Online Security***
- ***Physical Security***
- ***Privacy***
- ***Security Culture***

EFFECTIVELY DELIVERING TRAINING

06

Now that you know who you want to train—and on what topics—you can now pinpoint the best methods for delivery. Part of a solid strategy involves determining your information security communication plan and how it will cohabitate with the other goals.

How to Train

Execution Strategies for Your Security Awareness Program:

You want to engage people. If users don't listen or aren't motivated to change their behaviors, your program will fail. That's why it is important to engage with your audience on two levels:

Organizational

Individual

01 Organizational

This addresses the company culture. Develop a plan and approach in conjunction with senior management and corporate communications that reflects full, top-down support of the security awareness program initiatives and goals.

Work directly with the teams and leaders to identify opportunities to strengthen support for security awareness and secure behaviors and habits. Think all-hands meetings, CEO involvement, HR involvement—written into employee contracts and job descriptions as performance expectations.

02 Individual

Develop an internal marketing campaign announcing and training employees about what to expect from the training program. Modern marketing has revealed it typically takes people hearing something 7 times before they remember.

Don't expect you can begin a security awareness program by just sending employees the first training session. They won't know what it is, what to do with it and they will have no idea why they should even care about it.

Instead, spend a few weeks leading up to the launch of the program announcing it in many different channels. Send emails, announce during meetings – especially company all hands or executive announcements, put up posters, use collaboration tools, e.g., Slack or Microsoft Teams, and include an announcement about it any place there are regular employee communications.

It's also important to consider ongoing positive reinforcement and rewards for employees participating in the program.

Many security awareness solutions have gamification features or in other words, point trackers that aide in knowing which employees are taking the lead in the program. It is important to utilize this data to offer friendly contests and rewards for the employees who are doing a great job in the program!

Another motivating factor for employees to actively participate in a security awareness program is by giving them an understanding that they are also at risk outside of work.

The intent will be to empower users with the ability to make smart, security-driven decisions in their personal lives that nurture secure habits; along with the tools and resources to maintain secure behaviors at work.

Giving them ways to protect their family is always a big win. Anytime an employee understands how a risk could affect them personally helps them to see the value in whole-hearted participation.

UNDERSTANDING TYPES OF TRAINING

07

Most organizations will have a few different types of training they need to deliver through their security awareness program.

This is good to acknowledge early in the process. Identifying those trainings and putting circles around them will be helpful as your program plan begins to take shape and you start considering maturity and phases.

Here are the types of trainings we've seen included in successful programs:

01 *Compliance Training*

Many compliance training topics are required annually. This is often presented as interactive online training. The goal of the compliance training is to both set the expectations for user behavior and processes within an organization as well as ensure standards are met.

Compliance topics typically revolve around mandated requirements that often fall under the human resources umbrella, such as sexual harassment prevention training, and—as a result—need to be tracked or administered by HR. Plus, completion and/or infringement upon these compliance topics must be enforced by HR policies.

Many other compliance topics may overlap into your ongoing security awareness program, such as payment card industry (PCI) compliance. But just because you must check a box and provide compliance training from a legal or auditing standpoint, that doesn't replace the need for ongoing security awareness training. Stopping a potential breach is far more impactful than simply fulfilling a compliance requirement.

07

02 *Ongoing Security Awareness Training*

The importance of re-engaging with employees on a regular basis – at least twice a month – ensures employees will keep security threats, best practices, and cyber hygiene top of mind.

Scientific data supports providing training on at least a bi-weekly cadence. According to the Ebbinghaus Forgetting Curve, which demonstrates how information is lost over time when there is no attempt to retain new information, people forget 80% of what they learn within a month.

Conversely, the Ebbinghaus Forgetting Curve also shows that if people engage with education on a specific topic more than once a month, they retain 200% more information and accurately react 28% faster than those who learn by other methods.

The frequency of training is only part of the equation. The length of lessons also contributes to a program's success. The ideal length of a learning session as identified by MIT researchers is three minutes or less. This forces content coverage to be succinct and focus only on the most critical information. With a consistently short duration, viewers know that sessions won't waste their time or be overly taxing, which builds trust and ultimately increases engagement.

Driving a culture of ongoing learning through scheduled intervals of re-engagement, and providing short learning sessions are two of six key principles of microlearning. A retention-focused approach to learning that presents information in a similar format to how the brain already functions, microlearning ensures people remember what they're taught and can recall the information exactly when they need it.

For a complete look at how to implement microlearning as part of your security awareness strategy, read our white paper: The Valuable Role of Microlearning in Cybersecurity. There you will find in-depth guidance on creating content that supports the essential functions of an awareness program.

The key for the administrator of any ongoing program is to stay updated in the selecting and scheduling of content campaigns. Many administrators will seek out a fully managed security awareness solution to leave the content and its management in the hands of a trusted vendor, freeing themselves up to be a security awareness leader rather than functioning solely as program administrator.

However, it's important not to get wowed by vendors who offer gigantic libraries of long-form content instead of new and fresh microlearning lessons. When long-form trainings get outdated, they quickly become a drain on employee time and hinder their ability to stay motivated and participate in the program.

ONGOING THREATS REQUIRE ONGOING SOLUTIONS

07

Users retain 200% more information when educated on a specific topic more that once a month.

Still, not all vendors are the same. Some may have extensive libraries that initially look impressive, but when given a closer look, the lessons don't support your program's goals, meet the learning needs of your users, or provide content that is up to date with the evolving threat landscape.

When evaluating vendors, asking the following questions can help you make an informed decision:

- Do you offer short-form video content that is three minutes or less?
- Do you utilize scientifically supported learning methodologies in the development of content?
  - If yes, what learning techniques do you use, and how do they help my users learn and retain information?
- How frequently are new lessons added to your content library?
- How do you deploy your training (e.g., LMS or eLearning portal, directly to user's inbox)?
- What percentage of your available course catalog is short-form content (vs. long-form)?
- Does your library include lessons focused on educating my users on new and emerging threats?
  - If yes, can you provide recent examples of lessons you've created on new and emerging threats?
- Do you provide ongoing tracking, measuring, and performance reporting on the program?

07

03 *Phishing Training*

Phishing simulations should be included with any ongoing awareness program, and always treated as an educational tool. Many organizations begin their phishing simulation efforts with education in mind but somehow lose their way and become overly focused on all the bells and whistles of their phishing simulation tools. Often, they cross a line between trying to educate employees and... trying to trick them.

This may cause employees to develop animosity toward the entire training program. And once the simulation program focuses on tricking employees to catch and punish them, the bridge is burned. Also, if you take a sarcastic tone or shame people who do click on a simulation, employees will begin to avoid the security awareness program at all costs and not react properly when they received a simulated email.

Instead, phishing simulations should be used as educational tools and employees' engagement with them should elicit a "no shame" respectful tone. Sending monthly phishing simulations tied directly to on-the-spot training that teaches them how to properly identify whether an email is a phishing attempt or if it can be trusted is the best way to build a good relationship between employees and phishing simulations.

Along these lines, it is also important to educate employees on how to report suspicious emails. Many different tools can be used to safely handle potentially dangerous emails. A tool that is readily available to many organizations through Outlook and Google Workspace is a "report phishing" button that ensures proper and simple reporting.

New Hires and Contractors

All new employees and contractors should be required to complete an introduction to the organization's security practices during employee onboarding, as well as be immediately enrolled in the ongoing security awareness program.

IMPLEMENTING AWARENESS SOLUTIONS

08

Reinforce key behaviors by using varying methods of training throughout the year to help reach different sub-cultures within the organization. Building a successful culture can only happen when it is practiced regularly.

Major Awareness Initiatives

You can reinforce key behaviors using various methods throughout the year. These methods also help reach the different sub-cultures throughout the organization. These initiatives consist of the following:

01 *Cybersecurity Coaches*

This group of volunteer employees act as liaisons within their department or broader team. Appoint people who have a reputation in the organization as cyber experts, a passion for developing a culture of security, and are patient teachers.
The goal is to empower already security-minded users with the tools and resources they need to spread and strengthen efforts of the company security awareness program.

02 *Executive Assistant Network*

This group consists primarily of executive assistants, but also includes senior-level executives.

Like ambassadors, this group can help promote the program organization-wide. Emails that come from the office of the CEO or their assistant have a much higher open rate by employees, resulting in greater attention when needing to make key announcements to employees.

03 Tracking Execution

This process engages senior management throughout your company to candidly discuss any security concerns or needs unique to their footprint. Results from these discussions help inform you of previously unknown security risks and behaviors. This becomes a powerful assessment of your current environment as it gives you materials and ways to focus on reinforcement and potential training module candidates.

Senior management may not have an exact understanding of the step-by-step actions employees take while performing their jobs. So, this should be a multi-layered effort.

Leadership can receive their ideas on paper, but it's also important to have peer-led discovery meetings where peoples can speak freely, and anonymously, if necessary, and pull the curtain back on practices that might, in fact, be dangerous for your organization. If you want to have employees expose weaknesses and vulnerabilities, you must create a no shame, no blame culture that welcomes the exposition of potential pitfalls.

04 National Cybersecurity Awareness Month (NCSAM)

October is now globally recognized as Cybersecurity Awareness Month. This creates the opportunity to connect and engage with our users throughout the entire month. Activities can include learning sessions, online scavenger hunts, external speakers, and a keynote event typically highlight events designed to take advantage of this special focus.

In the first year or two of implementing your security awareness program, use cybersecurity month as a 'level-up' event. Take the opportunity to leverage special resources and events available from other vendors and organizations to raise the security awareness program of your organization.

As your company's security culture begins to mature, turn Cybersecurity Awareness Month into its own holiday season. Fill it full of prizes after you utilize points trackers for your employees and push your ongoing security awareness efforts to lead up to this month.

03 Newsletters

Newsletters require significant energy and access to editorial and creative resources, which you may or may not have. With the effort required to curate and develop content, newsletters yield low performance returns on time invested. Instead of building something new, focus on utilizing existing communication channels and piggy-back on existing internal marketing and communications activities.

However, if you really feel compelled to do one, send out a quarterly newsletter to InfoSec and senior leadership only—a general audience won't read it. Topics should focus on current strategies, results from initiatives, and projects on the horizon.

REPORTING & PERFORMANCE METRICS

09

Assessments And Scoring

You will need to measure the effectiveness of your security awareness training program in educating your users and changing their behaviors. We recommend the following methods to gauge its success:

01 *Compliance Training Metrics*

Think of this as your completion rates in terms of how many users completed the compliance training and regulatory requirements across the company. If you need to provide reports or documentation to any regulatory entities, be sure to understand what format they need the information in and then keep your records updated for reporting purposes.

02 *Ongoing Security Awareness Education*

The education portion of your security awareness program should have several key measurement capabilities.

- **Participation and Completion**—It is important to know if employees are participating and completing the content they are assigned.
- **Quizzes**—Asking employees questions and gauging their understanding of certain topics is more than just a neat stat for the reports. It further challenges them to quickly recall information which helps to transfer more of what they are learning to long-term memory.
- **Gamification and Leaderboard**—Creating a points scale for participation, quiz scores, and other behavior trackers will give a security awareness program the ability to attribute motivators, friendly competition, as well as accountability.

03 Phishing Simulations

A phishing training program includes lots of metrics. Be careful not to allow the phishing metrics to become the core metric for the program. It is but one of many important reporting numbers representing an overall effort of the program.

The prioritized metrics in your phishing simulation programs should help you assess improvement toward what should be your ultimate goal, which is to educate your employees. Many people lose sight of this when utilizing a phishing simulation tool.

Phishing simulations should be directly linked to specific teaching moments that not only let employees know where they went wrong, but also explain what to watch out for every single time they receive an email to determine if it can be trusted.

It is important to track clicks, completion of follow-up education, and ongoing improvements in individual performance on things like reporting suspicious emails and not clicking on simulated phishing links.

04 Live Trainings

Live trainings are unique and can provide interesting windows into your culture. Keeping track of the number of trainings delivered, number of unique teams participating, and number of attendees. Even being a small part of an in-person company event promotes a positive security awareness culture.

Employees hear directly from the security awareness manager or CISO about the program is a valuable use of time. Not sure what to present on? You can take time to highlight an employee who reported a phishing email that saved the company from potential headaches, take the opportunity to announce or reinforce an upcoming security awareness training, or have leadership endorse the need for ongoing training participation.

Much like marketing programs it is then important to track registrations, attendance, and participation based on how much or how little promoting was done.

05 Incident Response

An effective security awareness program creates enough relevant data directly to the IR teams to enable those teams to become efficient. Tracking efficiency can demonstrate to senior leadership an additional way in which the program adds value. An important statistic involves “reduced time to respond” to phishing threats, because the users themselves are doing the reporting.

06 NCSAM

National Cybersecurity Awareness Month is a behemoth. However, planning ahead of time and with intention can offer multitudes of great metrics—things like hours spent learning, events attended, participants in contests, etc

07 Surveys

Sending out an annual anonymous security awareness survey to measure individual’s understanding of organizational policies and measure their beliefs and attitudes toward information security can provide you with valuable insight.

BUILDING A THRIVING PROGRAM

10

What's really impactful about implementing a sound strategy is that you will build a continuous positive learning curve and give your entire organization a program they can all understand, support, and promote.

Key Building Blocks

Keep it simple.

- **Ongoing Training:** Microlearning lessons, twice a month.
- **Phishing Simulations:** Once a month.
- **Compliance Trainings:** New-hires and annually thereafter
- **Maintain a positive, empowering message:** Always

So, plan big and keep the execution simple.

During year two, highlight maturing year-one goals, and add one or two new programs—like ambassadors and live training, or even role-based training efforts. You can forecast and show how your program matures each year. Doing so is executive team gold.

Above all else, remember that you, and your entire program are in place to educate and elevate employees. Don't get so consumed by administering your program that you forget about your people. Find ways to automate your program so you can spend more time leading your people.

Interested in learning about the future of security awareness?

You're invited to embark on a Managed Security Awareness Journey.

This free time traveling tour will show what it's like to become an Arctic Wolf Managed Security Awareness customer.

You'll participate in microlearning sessions, find out what your Concierge Security Team can do for you, and discover how an ongoing program can change your company culture

Experience a tour of Managed Security Awareness today!

GET STARTED NOW

ARCTIC WOLF

SOC2 TYPE II CERTIFIED

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

CONTACT US

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com

END CYBER RISK

ABOUT ARCTIC WOLF

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, highly trained Concierge Security® experts work as an extension of your team to help end cyber risk. We make it fast and easy for organizations of any size to stand up world-class security operations that continually guard against attacks in an efficient and sustainable way.

For more information about Arctic Wolf, visit **arcticwolf.com**.

AW_G_ Complete_Cybersecurity_Awareness_Plan_1121