IN THIS CHAPTER

- Recognizing the importance of security awareness
- Working with a security awareness program
- Knowing where awareness fits within a security program
- Getting why the so-called "human firewall" doesn't work

Chapter 1

Knowing How Security Awareness Programs Work

A successful security awareness program motivates people to behave according to defined practices that decrease risk. Creating a program that successfully changes behavior throughout an organization involves more than simply communicating a bunch of facts about security awareness. Just because people are aware of a problem doesn't mean they will act on their awareness. In other words, awareness doesn't guarantee action. (Everyone knows that fast food isn't the healthiest choice, but most people still eat it.) This chapter sets the foundation for understanding the issues and the solutions.

Understanding the Benefits of Security Awareness

The thinking behind *security awareness* is that if people are aware of a problem, they're less likely to contribute to the problem — and more likely to respond appropriately when they encounter it.

Users who are *aware* don't pick up USB drives on the street and insert them into their work computers. They're aware of their surroundings and ensure that nobody is looking over their shoulders while they're working. They don't connect to insecure Wi-Fi networks. They're less likely to fall victim to phishing attacks. Essentially, users who are aware don't initiate losses for their organizations.

Organizations typically create security awareness programs to ensure that their employees, or *users*, are aware of cybersecurity problems that are already known to the organization. Phishing messages, covered in the next section, represent the most prolific attack against users.

Reducing losses from phishing attacks

Phishing attacks are common enough these days that many people are already familiar with the term. A working definition is "an email message that intends to trick a user into taking an action that is against the user's interests." A phishing awareness program would ideally train people to properly determine how to handle incoming emails in a way that reduces the likelihood of loss. For example, if a message asks for the disclosure of information, the ideal situation is that a user knows what information they can disclose and to whom while also determining whether the sender is valid.

To appreciate the losses that a phishing attack can cause, consider these prominent attacks:

- **Sony:** The infamous 2014 Sony hack, which was reportedly perpetrated by North Korea, began with a phishing attack. The hack resulted in the leak of information about movies, the movies themselves, and embarrassing emails. Sony reported costs of the hack to be $35 million.
- **Target:** The 2013 Target hack, which compromised more than 110 million credit card numbers and consumer records, began with a phishing attack of a Target vendor. Target reported the resulting costs to be $162 million.
- **OPM:** The attack on the Office of Personnel Management (OPM), discovered in 2014, which compromised the security clearance files of 20 million

U.S. government employees and contractors, began with a phishing attack against a government contractor. The costs and losses are immeasurable because this attack is considered a major intelligence success for China, the perpetrator of the attack named by the U.S. government.

- **Colonial Pipeline:** The Colonial Pipeline ransomware attack in 2021 began with a phishing message that captured user credentials and allowed the criminals to establish a sustained presence on the network. This allowed the criminals to find the most critical systems and eventually install the ransomware, which caused Colonial Pipeline to shut down the pipeline, halting a primary oil delivery to the U.S. east coast. Colonial Pipeline paid the criminals approximately $4.4 million, but the actual costs resulting from the shutdown were tens of millions of dollars to Colonial Pipeline and an incalculable cost to the economy.

TECHNICAL STUFF

The Verizon Enterprises Solutions' Data Breach Investigations Report, commonly referred to as the DBIR, is one of the most often cited studies in the cybersecurity field. The report, which is produced annually, is drawn from data collected directly by Verizon's managed security service. The DBIR, considered a reliable overview of real-life attacks against organizations around the world, indicates that more than a whopping 85 percent of all major attacks begin by targeting users. You can access the report at `www.verizon.com/business/resources/reports/dbir`.

Reducing losses by reducing risk

Just as people get themselves into automobile accidents despite advances in automobile safety, even reasonably aware users may fall victim to cybersecurity attacks. All cybersecurity countermeasures will eventually fail. Countermeasures include encryption, passwords, antivirus software, multifactor authentication, and more. Perfect security doesn't exist. Your goal in establishing a security awareness program is to reduce risk by influencing user actions.

REMEMBER

Don't expect users to be perfect — risk reduction isn't about eliminating risk altogether, which is impossible. Expect your security awareness program to reduce the number and severity of incidents, thereby reducing losses from the incidents.

Also, a more aware user knows when something seems wrong and knows how to react to it. If your users sense that they might have been compromised, they start taking actions to mitigate the loss. If they accidentally email sensitive data to the wrong person, they try to stop the message or have it deleted. If they end up on a malicious website that starts serving adware, they disconnect before additional damage can occur. They know how to properly report any and all potential incidents, so your organization can begin to stop any loss or damage in progress. In the worst case, at least they can launch an investigation after the fact to find out what happened.

In the ideal situation, even when a user takes no potentially harmful action, they report the situation to the appropriate party. They report details such as whether someone tried to follow them through a door, even if they turn the person away, because they know that the person might attempt to enter through another door or follow someone else through the door. If someone detects a phishing message, they don't click on it — instead, they report the message because they realize that other, less aware users may click on it, and then the administrators can delete the message before that happens.

As you can see, awareness requires more than knowing what to be afraid of — you also have to know how to do things correctly. Too many awareness programs focus on teaching users what to be afraid of rather than on establishing policies and procedures for how to perform functions correctly, and in a way that doesn't result in loss.


REMEMBER

The goal for awareness is for users to behave according to policies and procedures. Part of the function of an awareness program is making users aware that bad guys exist and that those bad guys will attempt to do bad things. But awareness programs primarily focus on making people aware of how to behave according to procedures in potentially risky situations.

Grasping how users initiate loss

Users can cause only the amount of damage they're put in the position to cause — and then allowed to carry out. However, even after they make a potentially damaging mistake, or even if they're blatantly malicious, it doesn't mean that the system should allow the loss to be realized.

For example, a user can click on a phishing message only if the antiphishing technology used by your organization fails to filter the message. If the user clicks on a phishing message and ransomware is activated, the ransomware can destroy the system only if the user has permission to install software on the system — and then in almost all cases, you have no standard antimalware on the system.


REMEMBER

User error is a symptom of the problems with your system. Even if a user makes a mistake, or is even malicious, the resulting loss is a problem with the system providing users with potential actions and then enabling the loss.

In essence, users may initiate a chain of actions that create the loss, but the loss is a result of failings in the system as a whole.


TIP

For more information on user-initiated loss, find a copy of my book, written with Dr. Tracy Celaya Brown, *You Can Stop Stupid: Stopping Losses from Accidental and Malicious Actions* (Wiley, 2021).

Knowing How Security Awareness Programs Work

Unfortunately, there is little consistency in what is perceived to be a sufficient, organizational security awareness program. Some organizations just have *users,* or employees, sign a document. Many other awareness programs require employees to read the document once a year (or, increasingly, watch a video).

At the other end of the spectrum, organizations like the National Security Agency (NSA) are naturally much more rigorous in their screening practices, as employees must achieve the appropriate security clearance before they can even begin working. The NSA is a special case, of course — most organizations don't engage in such rigorous screening practices.

The goal of a security awareness program is to improve security-related behaviors. The goal is not to simply make people aware of an issue — the goal is to inspire people to behave appropriately to avoid the initiation of a loss and, ideally, to detect and respond to the potential for loss. Whether people understand how their actions promote security is secondary because the goal of an awareness program is to change behaviors, not just impart knowledge.

At the end of the day, a *security awareness program* is essentially a set of tools, techniques, and measurements intended to improve security-related behaviors. Book 6, Chapter 4 describes a variety of tools that you can incorporate into your program. Some tools are more popular than others; however, no tool is absolutely required. The choice depends on your needs.

Establishing and measuring goals

The ultimate goal of a security awareness program is to change and improve security-related behaviors. Security programs are created to reduce loss. As an essential part of an organization's overall information security program, security awareness should likewise reduce loss.

Book 6, Chapter 5 covers some metrics you can use to judge whether your awareness program successfully reduces loss. Many security awareness professionals talk about the likeability of their tools, the number of people who show up to their events, and the quality of their posters. These metrics and general impressions are nice to know, but they're relatively useless from a practical perspective.

GETTING THE BUDGET YOU NEED

This philosophy generally holds true in cybersecurity:

- You don't get the budget you need — you get the budget you deserve.

Security awareness teams typically compete against other teams for budget funds and other resources. For example, the team may work under the cybersecurity, human resources (HR), compliance, legal, physical security, or another department within the organization. All these teams compete for funding and other resources. Even if your cybersecurity program has sufficient resources to fully fund all teams, including the awareness program, you have to show that you deserve the budget amount you're requesting. You need to financially justify your efforts.

You can have plans for the best awareness program in the industry, but if you cannot demonstrate that you deserve the appropriate budget, you won't get the budget you need to implement it. Book 6, Chapter 5 details how to collect metrics that help you show that you deserve what you need.

A metric demonstrating that you're changing behaviors in a way that reduces loss, or preferably improves efficiency and makes the organization money, is the most useful metric to show that you're producing value. This isn't to say that it's the only possible benefit of a security awareness program. Awareness programs also often provide intangible benefits to the organization. These benefits include protecting the organization from damage to its reputation, illustrating that the organization is committed to security, generating excitement and engagement among employees, and reassuring customers that your organization is actively protecting them.

REMEMBER

If your goal is to contribute to your organization's security effort, you must identify the benefits your program will bring to the organization. These benefits can't be that the program merely provides information. The program should improve behaviors. You must be able to show how the program returns clear value to your organization, and this value should ideally return clear value to the bottom line.

Showing users how to "do things right"

For your awareness program to help create desired behaviors, the program must show people the proper way to perform job tasks, or "do things right." In other words, you provide instructions on how to do things properly by default.

When you consider most of the materials produced by vendors, and a great deal of the materials produced by organizations for internal use, these materials frequently focus on the fact that "bad people" intend to trick you. They tell you about criminals who will do harm if you fall for their tricks. This information can provide motivation, which can be worthwhile, but it's doesn't show users how to recognize suspicious situations as they encounter them.

When you teach people to focus on the ways bad people will exploit them, the training will fail when the bad people try a different trick. Expecting users to combat well-resourced, highly skilled criminals is a losing proposition. You cannot expect users to be consistently effective in thwarting such parties.

The better approach is for your awareness training to focus on the way that users can do their jobs properly. Ensure that users have an established process that they're familiar with and that they know how to follow. The process should account for the potential of bad people trying to game the system.

Consider the example of a large online gaming company that has problems with criminals calling up the support desk to duping the support personnel into changing the passwords on specific accounts so that the criminals could go into the accounts and sell the assets. A possible solution is to create a decision tree support personnel can use to authenticate callers. As long as the support personnel follow the provided guidance, no accounts will be compromised and no one has to train the support personnel to handle each and every possible scenario that bad people might try. None of those details matter. They just need to know the one way to do their job properly.

Though this strategy may not be feasible in every case, for every job function, your awareness efforts should generally focus on providing guidance in how people should do their jobs properly. This requires embedding security within job functions.

In many cases, you may find detailed procedures already defined but not well known or practiced. In this case, your job is to find those procedures and figure out how best to translate them into practice.

Recognizing the Role of Awareness within a Security Program

Awareness isn't a stand-alone program that the security team uses to deal with the *user problem,* as it's commonly called. Security awareness is a tactic, not a strategy, used to deal with the user problem.

As covered in the earlier section "Reducing losses from phishing attacks," for a phishing attack to exploit your organization, your system first has to receive the email message on your server. Your system then has to process the message and present it to the user. The user has to review the message and decide how to act on the message. If the message contains malware, the system has to allow the malware to install and execute. If the message sends the user to a malicious link, the system has to allow the user to reach the malicious web server. If the user gives up their credentials on a malicious web server, the system then has to allow the malicious party to log in from anywhere in the world.

When a phishing attack succeeds, the user action is just one link in a fairly involved chain that requires failure throughout the entire chain. This statement is true for just about any user action, whether it involves technology or not.

Here are several concepts to consider:

- The user is not the weakest link.
- Awareness addresses one vulnerability among many.
- The user experience can lead the user to make better decisions — or avoid making a decision in the first place.
- Most importantly, to stop the problem, you have to engage and coordinate with other disciplines. See Book 6, Chapter 3.

Dealing with user-initiated loss (after all, the actions can be either unintentional or malicious) requires a comprehensive strategy to deal with not just the user action but also whatever enables the user to be in the position to create a loss and then to have the loss realized. You can't blame a user for what is typically, again, a complex set of failures.

Though it's true that, as an awareness professional, you can just do your job and operate in a vacuum, doing so inevitably leads to failure. It goes against the argument that you *deserve more*. This doesn't mean that the failure wouldn't happen even if everyone cooperated, but operating in a vacuum sends the wrong message.

REMEMBER

Awareness isn't a strategy to mitigate user-initiated loss — it's a tactic within a larger security strategy.

The security awareness program isn't the sole effort responsible for mitigating user error. If you say nothing to oppose this idea, you give the impression that you agree with it. Worse, you give the impression that users are responsible for any loss resulting from harmful actions that you already anticipate they will eventually make, such as clicking on a phishing link or accidentally deleting a file.

You have a responsibility to reduce risk by encouraging secure behaviors. But you're also part of a team and you should work in concert to support that entire security team to reduce loss. In a coordinated cybersecurity department, each team determines their part in reducing losses related to user actions and takes the appropriate actions. Likewise, each team determines how best to support each other in the overall reduction of user-related losses.

As a security awareness professional, you can be the tip of the spear in coordinating a comprehensive solution to reducing user-related losses. Your primary focus is to create behavioral improvements that reduce the initiation of losses.

Disputing the Myth of the Human Firewall

The section heading might anger a lot of security awareness professionals, but the idea of the human firewall is a dangerous myth. The idea that users are your last line of defense (which is a catchphrase for many phishing simulation companies) is fundamentally *wrong.*

First, consider that users are *not* the last line of defense in any practical way. For example, if a user clicks on ransomware, the user environment can stop the user from downloading malware by not giving the user permission to install software. Even if the software is downloaded and installed, antimalware can stop the ransomware. To accept that the user is the last line of defense, you have to discount many useful technologies that are commonplace in organizations.

Michael Landewe, the CTO of Avanan, said it best:

> If a user is our last line of defense, we have failed as an industry.

Regarding the claim of creating a human firewall, in principle it sounds great, but any security professional knows that even technical firewalls will fail. Users are less reliable than technology. Creating a human firewall implies that you will create an entire organization of users who always behave appropriately and securely. That isn't possible, however. Though humans can consistently behave well, no individual (and especially no group of humans) in the history of mankind has always exhibited error-free behaviors.

Consider also that although other technologies do only what they're instructed to do, humans can have malicious intent. If you leave your users as your last line of defense and they're malicious, the results will be disastrous.

I want you to create the best security awareness programs possible, but you need to remember where you fit within the overall chain of actions. If you give the impression that the user has ultimate control of your systems, then the first time a user fails, you fail in your self-described mission, which can damage the credibility of your program. Consider that you don't even see people who manage firewalls imply that their firewalls will stop all attacks from getting in. If you spout off to management that you will create a human firewall to repel all attacks targeting humans, then the first time a user fails, your program has failed based on *your* statements. Everything else you do will be met with skepticism, including requests for budget funds, personnel, time, and other resources. Don't set yourself up for failure from the start.

The reality is that most people don't give users and security awareness programs enough credit. Every time a user avoids clicking on a phishing message, your awareness efforts are successful. Every time a user locks up sensitive information, your awareness efforts are successful. Every time a user protects their screen from shoulder surfers, your awareness efforts are successful. These successes happen all the time.

Your users are a critical part of your organization's system, and your efforts can significantly reduce loss. Aware users help organizations avoid disaster. Even when attacks are reported after the fact, aware users respond appropriately, alert the appropriate people, and significantly reduce the resulting loss.

The awareness programs you create can provide an immense return on investment. Just be sure that you set realistic expectations.