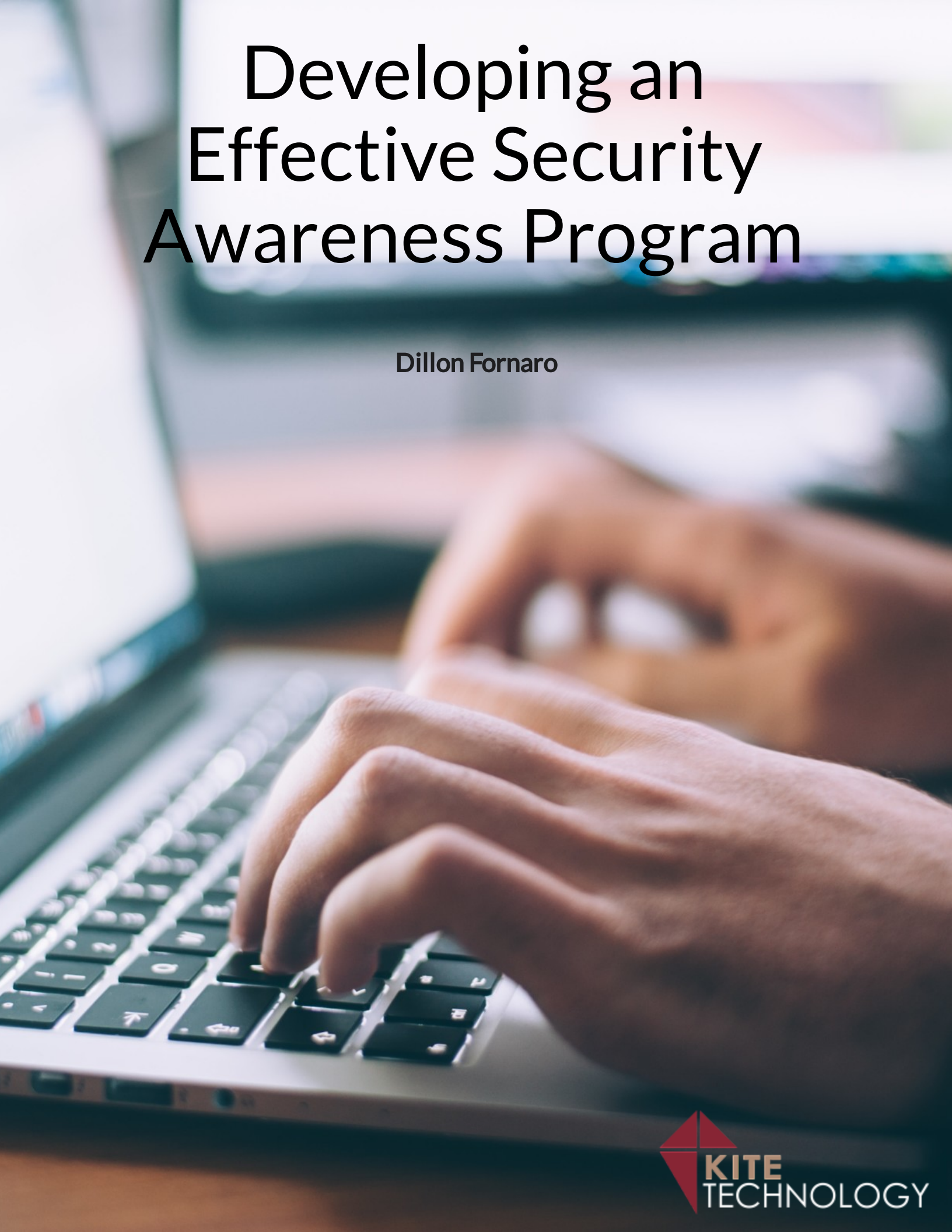
Developing an Effective Security Awareness Program

Dillon Fornaro



KITE TECHNOLOGY

Developing an Effective Security Awareness Program

Did you know that 81% of all reported data breaches are directly related to employee credentials? So how do you avoid becoming a statistic? It's by creating a highly engaging Security Awareness Program that educates your users on everything they need to know about recognizing and avoiding cyber threats. For it to be as effective as possible, your Security Awareness Program needs to be more than just watching a few videos here and there. It's no longer just training, but an entire program to undertake, develop, and deploy.

The goal of an effective security awareness program is for the information and education provided to resonate with your employees to create a certain posture and become more aware of cyber threats. By implementing an engaging Security Awareness Program for your end users, you'll be protecting them and your company's data.

There are three essential components that every security awareness program needs in order to be effective:

1. Training
2. Testing
3. Management/oversight

Training

Most of you have probably undergone some sort of security awareness training in the past. Whether it was watching videos like we talked about earlier or maybe even attending an online class- you probably don't remember much, right? How do we change that? Well, the first step is providing relevant and engaging training. Here are some tips:

1. Your training needs to be relevant

The educational scenarios and information that is included in your training should be something that is relevant the end user or their role. Before choosing your training modules, ask yourself these questions: What are the risks out there that would target our company specifically? Is there a specific world event going on that could be utilized by a malicious user to target our staff? Do we have remote workers that utilize public WIFI or mobile devices?

- Training should be specific to your type of business and your employee's roles.
- Should be used to help build security best practices into employees' everyday routines.
- Should be specific to cyber threats targeting your company/industry

2. Keep training fresh and engaging

Once you come up with the relevant information for your employees to learn, the next step is making sure it's engaging and worthwhile to the end-user. To someone who is learning something new, a good video with a good speaker goes a long way. Make sure to watch or take the training portion of your program yourself to see how engaging it may be. Also, make sure that the videos aren't too long. Multiple shorter videos can go a long way compared to an hour-long training session.

- Don't use out of date content
- Understand how people learn and tailor your program accordingly
- Use Gamification to make training modules more fun and competitive
- Offer bonuses of some sort for passing the test with the highest score or reward those who report the most phishing emails with gift cards to coffee shops, extra vacation time, etc.

3. Ask for feedback

I can tell you from experience that keeping your employees engaged in security awareness isn't always an easy task. You will have pushback and it may take some time to fine tune.. That is why you need to ask your users for feedback. If they aren't feeling good about what they are learning, you need to know why and act accordingly or explain to them the reasoning behind why you chose that certain video or article.

Ask employees to tell you why they feel the way they do: if valid, take their feedback into consideration.

4. Frequency of Training is Key

The true industry standard when it comes to frequency of training is to perform a campaign every quarter of the year with updated information. That seems like a lot, but with how many new emerging threats there are, it really is reasonable.

- Industry standard is 4 times a year but twice a year is a happy medium - only if done correctly
- If training is fresh and engaging, you shouldn't have pushback with the frequency of training.

5. What do you train YOUR employees on?

As stated earlier training will depend on your company's needs, but here are some recommendations to get started:

1. **Phishing-** Train your users to identify fraudulent emails. According to Statista, 306.4 Billion emails sent each day and 55% of those emails are considered spam. Since the most common attack vector into a network is email, training on phishing is important for everyone.

2. **Email Attachments-** Most of the time, just reading an email isn't going to do any damage. However, some have attachments. These attachments may contain malicious payloads: malware of all sorts, including ransomware/extortionware. So, teach your employees to always be skeptical about attachments, especially if they weren't expecting them. Lastly, teach them to call to verify – just because it's a legitimate email, doesn't mean the user hasn't had their account compromised.

3. **Websites and Domains-** Websites and domains are a popular way to trick users into thinking they're safe. Teaching your employees that the fundamentals of a domain is crucial to their understanding on how to keep their data secured. Just because it looks like you're on the correct website, doesn't mean you are. Verify the URL at the top of the page before entering any data. Is it spelled correctly? Was I brought here through a truncated URL? Did I confirm the address by hovering over the link sent to me in that email? All great questions to have your employees thinking about in a routine fashion.

4. **Physical Intrusion-** Physical security is often overlooked when it comes to a security awareness program. Ask yourself- Do you know who is entering your building? Do you have proper controls in place that will prevent someone that isn't supposed to be there? Have someone that isn't a familiar face to your employees put on a safety vest, grab a clipboard and a fake badge, and walk into one of your establishments with a nice story, a friendly smile, and see where they end up. You may be surprised on just how many people can get into your building and even possibly into your network. While this isn't something that happens as often as phishing, it's still worth training your users on to be skeptical of people entering your building that aren't familiar and implementing a check in/check out requirement goes a long way.

Testing

One of the most important and often overlooked component of a security awareness program is the testing portion. As much as we all hate to be tested on something, it's an extremely necessary step in creating a solid security awareness program. We're going to cover two of the main ways that you can test your users' ability to recognize and avoid cyber threats.

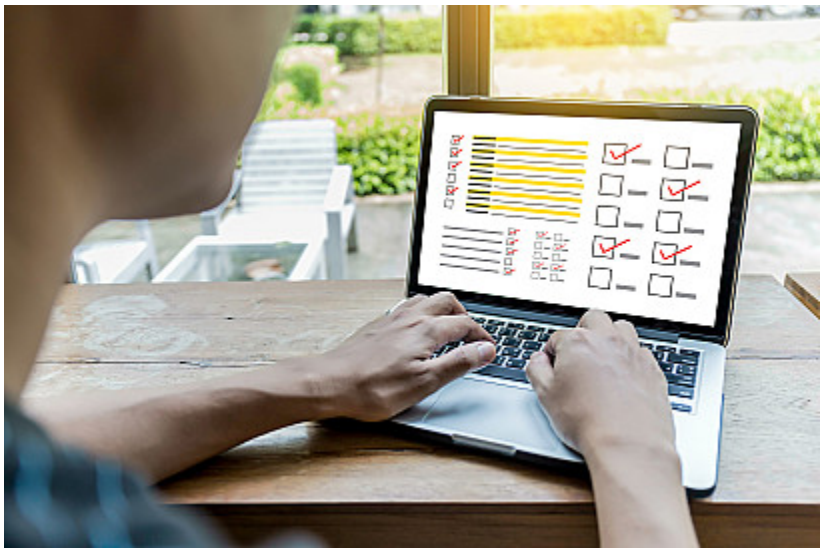
Simulated Phishing

Phishing is one of the most utilized methods today in attacks against companies. Simulating these attacks is extremely effective in helping the end user spot these types of emails. As a simulated phishing campaign takes off, it will send fictitious emails claiming to be from a bank, your IT department, or so on. More than likely, you would be using some sort of service for this which in return, will track if a user clicks on the email, downloads the attachment, or so on. With these features enabled, you will be able to see who is the most at risk in your company so that you can follow up with them to see exactly what went wrong. The follow up should never be a punishment. People make mistakes. That is why it is important to get to the root of the problem to educate that user on how to better prevent this from happening in the future.

Proficiency Testing

While this may not be the most effective way of gauging your employee's knowledge of what they have learned in regard to security awareness, it does still help, even if they're not proficient test takers. It's a good way to recognize whether or not someone may need some more training or maybe they just need an explanation on why they got a specific question wrong.

Again, following up with these employees who fail the testing is a huge priority for improving your end users' goal to learn which leads us to the final portion of a solid security awareness program: management & oversight



Management and Oversight

Management and oversight of a proper security program goes a long way in its effectiveness to teach your end users solid security posture. Whether it's familiarizing yourself with which employees are the most at risk to keeping up to date with the latest threats to incorporate into your training, there needs to be some sort of engagement between the one whom runs the program and those who participate. It's vital to create a "Culture of Security" where cybersecurity is prioritized, and your entire team is on board with taking the necessary steps to protect your organization.

1. Own Your Program

One of the most important aspects of the management and oversight component is someone has to **own** the responsibility of creating the program, push it out to their employees, and continue to monitor results. I see it all of the time. Someone is tasked with setting up their company's cybersecurity program which leads them eventually to the security awareness portion. The program is set up, pushed out, and forgot about. There is no follow-up. There is no incentive to complete the training. It's just there, waiting in the background because it was something they were told to do.

2. It's a Joint Effort

To ensure the success of your program, you must choose the right person to own the program. That can be someone in a leadership role or someone on your team that is passionate about security and willing to take this on. That person should understand that this as an ongoing project and one that is never finished because honestly, it never will be because of how the cybersecurity threat landscape is continually changing.

A solid security awareness program is a joint effort. Engagement between all parties; you, your employees, and the company as a whole which also includes management. The CEO of the company doesn't get to opt out of the Security Awareness Program. Everyone needs to participate for it to work effectively.

3. Evaluate Your Data

Last but not least, let's talk about using the results from your testing to evaluate the effectiveness of your training. This data will help you identify the users who would benefit from extra training or could use some additional incentives or encouragement to finish their training in the first place. Alternatively, the data will also help you identify those employees that are are completing the training on time and doing well which gives you the opportunity to reward them for their effort- which boosts morale and incentivizes others to do the same.

Data is one of the most important aspects of the training available to you as the owner of the program. Use it often and use it well to guide the development of your training and you will see an improvement in overall results.

Takeaways

1. An effective Security Awareness Program is one of the most critical tools that you can have in your cybersecurity toolbox. Remember, it's no longer just training, but an entire program.

2. Your company's Security Awareness Program will be more successful if everyone is involved and the program is built for your specific company and industry in mind. A cookie cutter approach won't be as effective.

3. Ongoing management and oversight of your Security Awareness Program is vital in ensuring that your program stays relevant and effective.

Making security awareness a priority is a necessity in today's age. Constant threats are looming and it's extremely important that you and your team understand and are aware of what's out there. Work together as a team to create a solid security foundation and posture- it will go a long way in protecting your organization and your clients!