KnowBe4
Human error. Conquered.

Obtaining and Maintaining Executive Support for Your Security Awareness Training Program

INTRODUCTION

We won’t sugarcoat it: executive support can make or break any program within your organization (security-related or otherwise). No support means no budget, no resources, no prioritization. In other words: no program.

> *For your security awareness program to be a success, the executive team must be convinced that the security mindset and culture created by security awareness training is the right thing for the organization.*

Security awareness training specifically can have its own set of hurdles. Cybersecurity programs have traditionally focused on software solutions designed to prevent, protect, detect, and respond to attacks. With security awareness training – a very human aspect of your cybersecurity program – the lack of executive support will likely be the deciding factor as to whether it is implemented or not.

It’s not just essential to ensure that you’ve got the backing to get the budget you need to create an effective and engaging training program. If the actions, habits, and cyber hygiene of the executive team don’t align with the message of your security awareness training program, the entire program can be undermined. For your security awareness program to be a success, the executive team must be convinced that the security mindset and culture created by security awareness training is the right thing for the organization and “talk the talk” and “walk the walk” when it comes to supporting this initiative.

Dealing with the complexities of internal politics, as well as gaining and maintaining executive support, can be a significant challenge for a variety of initiatives within an organization. However, this challenge is heightened when it comes to security awareness training, because the training and its impact aren’t always clearly linked to an organization’s bottom line.

So, how do you obtain and maintain the executive support you need?

In this whitepaper we’ll look at some of the questions you should ask when seeking executive buy-in for your program, as well as some of the things you can do to put yourself in the best possible position to get the support you need.

HOW IS YOUR STORY BEING TOLD WHEN YOU’RE NOT AT THE TABLE?

Most companies are unlikely to give those seeking to run a security awareness program a seat at the executive table or even an audience to present. As a result, effectively communicating your story to executives and highlighting the true value and benefits to the organization based on what you are planning to do become essential.

Here are a few questions to think about to ensure you can do this effectively:

- What is the story you’re telling and what do you want an executive’s takeaways to be when they think about the program?
- Do you even know the reasoning behind implementing a security awareness program? (While this may sound a little harsh, if you don’t fully understand the whys and wherefores of what you’re doing, you’re never going to convince your executives!)
- Does your story and value proposition make sense in presentation? (That is, if you listened to your own value proposition would it match up with what you are trying to get across? And if not, what are you doing to turn that around?)

Being able to answer these questions is a critical first step in the process. Your executive team will most likely be drowning in data from other sources, and you need to be able to cut through the noise. Therefore, your narrative needs to be clear and incisive. The project's value proposition must be effectively communicated – the executive team cannot be expected to magically understand the benefits of a bunch of charts and graphs. Don't leave anything to chance.

YOUR COMMUNICATION STRATEGY IS KEY

To get your message across effectively, you need to engage the story component of what you're looking to achieve. It's not just about numbers, percentages, and industry statistics, it's about telling the story of why security awareness training is a missing (and necessary) component of the organization's security strategy.

Any statistics presented need to be clearly tied back to what they mean for the organization and what you're trying to achieve. Never put yourself in a position where things are open to interpretation and where your executive team might put their own nuance on the message you're trying to get across.

Anytime you have a "What" you need to also answer the "So What" and the "Now What." Failing to do this leaves one or both of these questions open to interpretation, and that's a chance you cannot afford to take.

When you're putting your pitch together, always keep in mind this three-step process to ensure you get your points across effectively:

- What – every time you have a statistic or a number in your presentation, it should give rise to two other things:
  - So What? – what does this actually mean?
  - Now What? – what do we do in light of this information?

Anytime you have a "What" you need to also answer the "So What" and the "Now What." Failing to do this leaves one or both of these questions open to interpretation, and that's a chance you cannot afford to take.

Your communications strategy throughout this process is key. Be a storyteller, because telling stories is one of the best ways to embed concepts in our minds and make them memorable.

Ultimately, you want your pitch to become a morality tale of the value of security awareness. Sure, support that with charts, graphs, and numbers as you need to, but don't leave the actual moral of your story up for interpretation. Spell it out blatantly in all your communications. Otherwise your executives could flip through the details before your meeting, assume they know what you're talking about, and make a snap judgment before you even open your mouth and try to engage them in conversation.

CAPTURING EXECUTIVE TEAM ATTENTION

If there is a secret sauce to getting your executive team's attention, then it lies in these three things:

1. What's in It for Them

When you're addressing the "So What" elements within your pitch, make sure you also make clear what's in it for each member of your executive team. This means understanding what matters most to them when it comes to the outcomes of security awareness training.

You can hit this from both a positive and negative angle. You can talk about the pain that can be experienced when this isn't done right, such as data or people's accounts being compromised, or the organization looking bad. People always respond to fear. But you can also look at the positives, such as things like increased resilience, which can lead to greater stabilization of the environment, which in turn can give rise to increased employee productivity. These can then be tied to organizational goals and objectives that are important to the specific executives, for even greater impact.

2. Outline Clear Connections

Another part of answering the "So What" is showing a direct connection between the action of what you are trying to train on and what's important to the executive. Maybe that's a specific system or organizational outcome, project, or even a regulatory requirement. Creating clear connections to things that an executive is already concerned about for the organization makes the whole program more relatable for them.

3. Measurement and Stories

This is where you can really start to sell your program. Explain what will be measured as part of the program and then get into the morality side: "here are the things that will happen when we don't do this, and here are the things that will happen if we do this right." Don't be afraid to use all the facets of emotion here. While you need to steer clear of overtly selling FUD (fear, uncertainty, and doubt), you shouldn't be afraid to dip down into fear – every morality tale, story, or cautionary tale does this. Just make sure you use them in ways that are relevant and transparent.

WAYS TO ENGAGE YOUR EXECUTIVE TEAM

Here are some of the things you should focus on to get your executive team's attention:

- **Tie your program to compliance requirements –** Security awareness training is a requirement for most regulatory best practices. Don't be afraid to use this, and break down ways you want to do it to support your industry regulations.
- **Spotlight current events and stories about organizations that are similar to yours –** While you don't want to be seen to be fearmongering, relating your stories back to something or some organization that your executives can connect to will help to make the messaging more real. The closer to home and more real the threat becomes, the more your executives will feel they have duty of care to respond.
- **Map your program to established best practices –** Tying into things like the NIST Cybersecurity Framework, the National Association of Corporate Directors guidance on cybersecurity, or any industry-specific guidance that relates to your organization will show due diligence and the due care required to run this type of program.

USE A SMART GOAL-SETTING FRAMEWORK

Your executives need to know you have a plan to make your security awareness training initiative work. They will want to see you have intention behind what you're proposing. With intentional thought comes greater possibilities for success. The more methodical you are about how you approach pitching to your executive team, the greater the chances of success you'll have when seeking the buy-in you need.

But as the buy-in begins, there will be questions around how to measure the success of a security awareness training program. So, having some preliminary goals in mind will help provide executives with something tangible they can feel like they can hold you accountable to.

There are several goal setting systems out there, but if you don't have a favorite system already, then try looking at your goals in a SMART way. Your goals should be:

- Specific
- Measurable
- Actionable
- Relevant
- Time-keyed

What do we mean by this? Here's a couple of examples to get you thinking.

Saying "we want to reduce our Phish-prone™ Percentage" or "we want engaged employees so they are more aware of risk around phishing," may be true, but they're very non-specific.

However, saying "we want to reduce our Phish-prone Percentage from 30% to 15% within the next 3-4 months," is what you're after because it ticks all the SMART goal boxes. The goal is specific in that you can measure your progress, it's actionable by tying to steps in your overall proposal, it's relevant by relating to the goals of your executives, and by setting yourself a timeline it's time-keyed. Once you hit that SMART goal you will show a real impact for the organization. Presenting your program in this way will give you a far greater chance of getting your executives on board.

CONSIDER AN OKR FRAMEWORK

Another way you can show the executive team that you mean business is by using an Objectives and Key Results (OKR) Framework. Many organizational leaders will be familiar with these, and your executives will understand them – so you'll be talking to them in their own language. They allow you to set very specific objectives that can be measured by different key results.

Here's some example Key Results to help you build this into your program plan.

Objective (O): Reduce our overall simulated phishing test failure percentage from 22% to 2% in the next 12 months.

- **Key Result (KR):** Conduct a baseline phishing test to assess the organization's current level of phishing resiliency.
- **Key Result (KR):** Work with relevant teams to approve and schedule multiple phishing testing scenarios each month.
- **Key Result (KR):** Ensure that phishing tests are paired with just-in-time training opportunities or are followed up quickly with learning/correction opportunities.
- **Key Result (KR):** Assess and positively engage employee segments who are consistently more susceptible to phishing.
- **Key Result (KR):** Develop gamification, reward and recognition programs to create positive energy and positive social pressure.

BRAINSTORMING SPREADSHEET FOR GAINING SUPPORT

For each executive you're going to need to pitch to, you'll want to start thinking about how you are going to win them over. That means understanding what motivates them and what's important to them and their department. You need to understand their own specific value proposition and how you can tie your program to helping them achieve that. This is a serious undertaking and one you need to do up front before you get into the boardroom. This should also be done face to face because this is your opportunity to build a rapport with the people who can help get your project approved.

It's also an opportunity to find out where someone's concerns are and proactively answer any potential questions before you start pitching for budget and support. To help you do this, think about creating a spreadsheet with the following headings for each executive (remember this is just for you and not meant to be shared with them):

- Stakeholder name
- Title and department
- Primary drivers and needs
- Potential concerns, questions, etc.
- Departmental benefits if program is successful
- Stakeholder benefits if program is successful
- Other notes and comments (things to help you find common interest and build rapport)

IN CONCLUSION

Security awareness training is a marathon not a sprint. When you're pitching your security awareness training to your executive team, do not leave them with the impression that this is a one-time event, or it is like installing a firewall or other technical safeguard. Security awareness training is not a "set it and forget it," initiative. They need to understand that security awareness training is an ongoing management of a human security issue. If you're not reminding people regularly, they will default back to a "lazy norm" or baseline behavior.

Organizations need to commit to time and consistency with security awareness in the same way they would any other aspect of the business. Impacts won't be seen overnight. Security awareness is just as much about changing the security culture of an organization as it is about making it more secure. So, it's important to emphasize to executive teams that this is an investment that needs to be made with a modicum of patience.

Remember to be a storyteller and find analogies that you can use that will demonstrate the commitment that is going to be needed, and the benefits that will bring over time. The concept of compound interest leading to increased savings is a good way to demonstrate the benefits of consistent effort over time leading to a goal. Getting lucky with a one-time lottery ticket purchase is not a reliable way to save for retirement!

Security awareness is just as much about changing the security culture of an organization as it is about making it more secure.

Additionally, you need to find ways to measure the results of your program (that is, the changes in security behaviors) that work to establish that the security awareness program is successful. How you do this will depend on what you're trying to achieve. For example, an organization's susceptibility to being phished is easy to measure through simulated attacks. You can quickly set a baseline and then measure decreases in inappropriate user engagement with these simulations over time, demonstrating an improvement in organizational security. Also consider using the information from other tools such as security event management systems and endpoint protection systems. You can build a measurement process around almost anything that already tracks behavior in some form. After all, whether you get breached or not comes down to the behaviors of your employees, not just the information you presented to them.

Ultimately, successfully pitching your program plan is all about consistency. When you give promises and ask for support, be a realistic optimist. Talk about the benefits, discuss them at the individual level with each executive, be a storyteller, commit to persevere and talk about the benefits of doing your security awareness training program in the long term.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing attacks, and enterprise-strength reporting to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com