How To Get Leadership Buy-in for Cybersecurity

Adapted from: http://www.oriontech.com/how-to-get-leadership-buy-cybersecurity-awareness/

Obstacles to Buy-in for Cybersecurity

Seasoned cybersecurity professionals are all too familiar with the challenges of implementing cybersecurity programs within organizations, and many of them start with lack of leadership buy-in or a sponsor at the board level. According to a 2012 Law and Boardroom Study, data security was ranked by corporate Board members as their number one issue of concern. Yet, shockingly 75% of corporate boards are not actively involved in cybersecurity oversight.

How can these numbers be so far off? And why is support from the top such a big deal with this type of program? At Orion, we feel the challenges associated with getting an organization's leaders to really support Cybersecurity Awareness programs typically fall into one of four major buckets:

Budget Challenges

Determining the right security budget for an entire organization is not an easy task. There are a lot of factors to consider, and benchmarks vary drastically. The best way to set a budget that will actually hold up is to identify your company's specific needs and requirements. The sooner that top-level management is involved in this process, the better.

Change Management

Honestly, we could do an entire blog series on the challenges of change management within any organization. Since we aren't doing that today, the bottom line is that people don't like change. They want to continue doing things in the same way that they always have. Because,

let's face it, breakings habits isn't easy. When you have C-level and Board-Level support of a cybersecurity awareness initiative, all employees and team members will understand that compliance with training exercises or policies is not optional.

Lack of Understanding

There is no secret here, most company leaders will not sponsor initiatives they do not fully understand. While the past few years have made significant progress in highlighting the need to cybersecurity focus in light of headline-grabbing breaches constantly making the news, many members senior level management still view Cybersecurity as "ITs Problem" or "A Technical Purchase." This can make the task of selling Cybersecurity Awareness as an organizational strategy very difficult.

Lack of Time

Very few top-level business leaders have ample amounts of free time. In fact, most of them are juggling with a wide range of priorities. Because Awareness training can be viewed with a "we will handle it after we have an incident" mindset, it becomes difficult to make proactive programs a priority.

The importance to having all of these challenges overcome is that a cybersecurity awareness program that is supported and planned out effectively has the highest chance of success and providing value to the company. Without executive buy-in, it becomes difficult to channel the awareness levels that modern day security threats require, into an organizational goal and not just a personal one.

The Five B's of Buy-in for Cybersecurity

Once you understand the challenges that are keeping your executives from buying in, how do you go about overcoming them? Ideally, this is where we would post a checklist that can give you an immediate roadmap to getting the buy-in you need for your Cybersecurity initiative, but that is not the case. Remember that change takes time, and when it comes to changing how people perceive a business initiative, you have to start slow. So, instead of providing you with a quick-fix that may or may not work, our team decided to walk through several options that can support you in understanding how to get leadership buy-in for cybersecurity awareness programs.

Kirk Sievert wrote a blog post in which he calls out the "Five Bs of Executive Buy-in" which he argues lay a road map for helping implement change. According to Sievert, he names the Five Bs as:

1. Best Practices
2. Business Case
3. Be Specific
4. Be Assertive
5. Bring in an Expert

Drawing from that inspiration, we are going to walk you through the “Five Bs,” and help you understand how to apply them to a Cybersecurity Awareness campaign proposal.

Best Practices

Do your research and understand various examples of how other organizations have implemented Cybersecurity Awareness programs. This is critical to your being able to answer questions about Cybersecurity Awareness with confidence and credibility.

With regards to relevant data from the industry. there are two pieces of this that are important:

Check what your competition and partners are including in their programs- show them what others in your industry are doing.
How often are they promoting awareness campaigns?
How are they enforcing compliance?
Are they using video? Digital training resources?
What was the impact of the training and awareness programs?
Understand how will these various components work within your organization.
What are your biggest threats?
Tip: While Orion recommends understanding best practices and what is working in the industry, don’t get bogged down in “keeping up with the Joneses.” There is a big difference between using competitor research and industry benchmarks to inform your decisions, and allowing them to make your decision for you. Focus on what works best for your business and requirements.

The goal in this process is to become the subject matter expert for all things related to Cybersecurity Awareness in the eyes of your executive team.

Business Case

When determining how to position your business case it is important to highlight the various layers of threats that businesses face today. Every user, every laptop, and every smartphone is an endpoint that needs to be protected. When making this case to the board, make sure that you tie the implications of untrained employees to the bottom line.

Need an example of how to do this? Check out these numbers from a recent Ponemon Institute Study:

The Average 10,000-employee company spends $3.7 Million a year dealing with phishing attacks.
Companies who roll out training programs see improvements of between 26 and 99 percent in their phishing email click rates, with an average improvement of 64%
Adding in a 25% drop in retention, Ponemon calculated a phishing-related cost savings of $188 for the average company.
Note that the worst performing security awareness program still saved $77 per user.
Another tactic we have seen work time and time again is to conduct an exercise that shows management actual vulnerabilities within an organization. Luckily, there are a lot of free resources you can use to present risk to leadership. Here are a few that we recommend:

- Workplace Security Risk Calculator
- Online End User Security Awareness Quiz
- Online Identity Risk Calculator
- How Secure Is My Password? Password Checker
- Technology Checklist For Businesses
- MediaPro Awareness Program Maturity Assessment Quiz
- FCC Small Biz Cyber Planner

This line of thought will help you to driving home business value when selling your leadership on Cybersecurity Awareness programs.

Be Specific

It is critical to remember when talking to the board that you are addressing people who in most cases come from business backgrounds and not security or IT backgrounds. In all of your communication plans, be specific.

Tip: When board members are asking about threats, personalize the risks for them. Example: Start off by asking them how many of them have their work email on their smart phone? Then ask if their smartphone software is up to date. Or if they have ever accessed their emails on public Wi-Fi.

Once you have their attention on the threats, dive into what you want the cybersecurity awareness program to entail. Make sure that you answer:

Whom will need to be involved?
How will you communicate the awareness campaign?
How often will you hold events and promote awareness?
How much of a budget will be needed to support the event?
How will you measure progress after various awareness events?

Be Assertive

When attempting to get leadership buy-in for any initiative, it is critical that you be prepared for some push back. After all, while the business case for Cybersecurity Awareness has certainly been made, you are still talking about taking money and time of all employees in order to fix something that they may not believe is broken.

You have done the research, you understand what is needed, now you just need to make your case until you have them convinced. One of the ways we recommend presenting this information in a confident manner is to present them with a solution. Do not spend the entire meeting talking about problems or various instances where someone made a mistake. Continue to point out how you can drive progress forward.

Bring in an Expert

Sometimes, you reach a point where the leadership just needs to hear it from someone else. Maybe, you have been trying to get them convinced for too long. Maybe they have questions

that they are just not communicating to you. One of the things that we highly recommend is to go ahead and interact with an expert. This allows the leadership to hear the case for Cybersecurity Awareness expert whom can provide a different perspective and possibly lead them to that “ah-ha” moment that had previously been lacking. Another benefit of bringing in an expert is that they will have the independence to challenge traditional thinking and call out weaknesses that exist in the current system and provide a neutral perspective on the situation.