DYOPATH

CULTURE BEFORE TECHNOLOGY: TAKING A HUMAN-CENTRIC APPROACH TO CYBERSECURITY

One of the biggest mistakes companies make is thinking of cybersecurity purely in terms of tools, strategies, and numbers — and completely forgetting about the people involved.

In reality, the success of your security depends heavily on the people in your organization and the culture you are able to build. The best tools and most cutting-edge solutions in the world are useless without a strong culture of awareness and understanding to underpin them.

Here's the bad news — very few companies are getting this right. In a report by ISACA, only 5% of companies said their cybersecurity culture was where they wanted it to be.

So how do you go about building and strengthening a culture of security in your organization? In this white paper, we'll show you.

We'll include insights from Eric Anderson, the Vice President of Channels and Sales at Symbol Security — a company that specializes in fixing the human element component with social engineering — and Sam Bourgeois, the Director of Cybersecurity Services for DYOPATH.

A Big Shift in Cybersecurity

Until relatively recently, most people viewed cybersecurity as the sole domain of IT and security teams. These branches of the organization would take care of the company's security, and everyone else would focus on their own jobs.

But a shift is gradually taking place. More and more people are beginning to understand that security is an organization-wide effort that demands engagement from everyone. Companies that view security as a shared concern are much safer and more resistant to various forms of attack.

Social engineering attacks are the clearest example of the importance of this. Phishing, pretexting, and business email compromise are just a few ways attackers target individual humans within an organization to gain access to data and assets. Each individual team member now has a role to play, and a responsibility to be educated, vigilant, and careful.

Leadership has to change to reflect this. Company leaders need to actively guide cultural change and give employees all the training, information, and resources they need to play their part in security.

Building a Strong Culture of Security

How do you go about building a strong security culture in your organization? There is no quick fix here — it's an ongoing process that needs to be tackled from multiple angles. In this part of the white paper, we're going to look at a few of the steps organizations can take to build a safer, more security-aware company.

Security Starts at Home

Eric says, "At Symbol, we are big believers in the idea that security starts at home. If you're more secure at home, you're going to be more secure at work."

The 2020 Twitter attack was a clear example of this, as its success depended in part on targeting the personal emails and devices of company employees. And it's not the only one — attackers are increasingly going after individual employees in their personal lives.

If you build the right security habits at home, they'll transfer to your professional life. And in a work environment that's increasingly distributed, with the lines between home and office often blurred, those secure habits need to be in effect 24/7.

So what can employees do to stay safe at home? Here are some good places to start:

- Set strong passwords, and regularly change them. Password management tools can be a big help when it comes to moving away from basic, easily memorized passwords. Bonus points for going passwordless!
- Have two-factor authentication set up and turned on for every app and platform you use, not just those related to work. Bonus points for using an app-based feature instead of using the text message option.
- Make sure all your hardware devices like laptops, phones, and tablets are kept updated. When you get a notification about a recommended software update, install it.
- Be careful about the security of the Wi-Fi networks you use, especially when accessing public networks in places like coffee shops and airports.

Following these steps doesn't just help employees build stronger security habits for the workplace — it also protects them and their families in their personal lives.

Speak the Language of Your Employees

Too many security teams focus excessively on technical language and security-focused risk factors when they try to educate their co-workers. A much better strategy is to focus on the consequences of not being vigilant. Clearly explain the specific risks that come about when people are careless with their personal security.

A common hurdle here is the widespread objection to being monitored or observed — for example, when it comes to personal smartphones. This is where inclusivity is important. Companies have to make sure employees are part of the security process so they fully understand why specific security actions are taking place and feel like active participants in their own security rather than subjects to be monitored.

Simplify & Explain

Another part of the solution here is building understanding. Sam says, "We've created this kind of mysticism around cybersecurity, so people, they think that they can't understand it — well, they can. It's actually quite simple."

You don't need years of high-level experience in cybersecurity to understand the basics of how threats work and how to defend against them. Almost anyone can grasp the fundamentals, and when they do, they'll be far more engaged in the security process — and much safer.

The goal for leaders is to focus on simplifying and explaining key security concepts instead of making cybersecurity seem complicated, daunting, and scary. One useful technique here is to use personal stories.

"Personal stories matter," says Eric. "Leaders, or anyone in the organization, can share a personal story around a time that they fell for a phishing scam, or how they dealt with a data breach. It makes it relatable, and it humanizes cybersecurity and makes it feel real and urgent, and shows that we're all in this together."

Stay Positive

All too often, companies fixate on the negative when it comes to cybersecurity. They will be quick to call attention to mistakes, weak points, and bad habits. It's understandable — there's a lot at stake. But part of building a healthy culture around cybersecurity involves calling out the positive moments, too.

Make a point of celebrating wins. If someone on your marketing team successfully identifies a phishing email, call attention to it and treat it as a victory for the whole organization. Showing recognition when individual team members do the right thing is a great way to encourage and reinforce more engagement with security.

Some companies might even put incentive programs in place to reward employees when they consistently take the right steps with security.

Education in the Right Doses

Many organizations treat their cybersecurity education as a one-and-done process. They'll expect their teams to go through one single onboarding process and then consider it finished.

This is a bad way to approach education. Sam says, "Good training needs to be just in time, just enough, and just for me." In other words, focus on educating your teams on an ongoing basis via small, relevant snippets of learning.

Did your employee just click a suspicious link in an email? A short, personalized message to show them why this is risky and how to avoid it in the future is far more effective than overwhelming them with all the information at once.

Learning is most effective when it happens over time, with spaced repetition. It's unrealistic to expect your employees to retain everything — or even the majority of the information — from a three-hour-long safety lecture. Instead, educate them gradually.

Keep Training Relevant

Generic, cookie-cutter training is always going to have limitations. This kind of approach can still work — it's certainly better than nothing — but your best results will always come from customized training that is relevant to the circumstances and challenges your employees work with every day.

For example, training around phishing emails should actually look like the email programs your company uses. Ideally, your training will refer to the specific tools and platforms that you use, so your employees can understand and internalize the lessons much more easily.

Lead From the Top

Big, lasting cultural changes need to be championed by your leadership. If you want to permanently improve the way your teams think about security and bake in habits and attitudes that stand the test of time, you need enthusiastic buy-in from your leaders.

If company executives see security as a frustrating chore — and talk about it accordingly — their co-workers will be far less likely to take security seriously. On the other hand, if your leaders are aware of the importance of strong cybersecurity habits and make a point of following the right steps in their own lives, other company members will take note.

Don't Get Fixated on Compliance

Compliance is important. Today's organizations are expected to adhere to a huge — and constantly growing — set of regulations and frameworks specific to their industry and region.

But it's important to keep in mind that your team members aren't going to resonate deeply with the need to check boxes and comply with lengthy compliance processes. Instead, your training should emphasize what matters to them — the need to keep their assets, devices, and families safe from cyber criminals.

Sam says, "End users are regular people. They want to do the right thing — help them do the right thing. Do it at their speed, at their pace, when they're ready for it. And they'll come along."

Be Human-Centric

With cybersecurity, it's easy to get caught up in technical language and rely heavily on statistics and data. While this is important, it's usually not enough. If you want to drive lasting cultural change across your entire organization, you need to complement the data with a more human approach.

This is another area where stories can play a role. If a certain employee is making the same mistakes consistently — for example, regularly clicking through suspicious email links — try reminding them that this kind of thing can also endanger them at home on their personal devices. Bringing a human element into education can make security seem more real and relatable.

People First, Tools Second

If you want to build a strong, lasting culture of cybersecurity in your organization, you need to start with your people. This isn't to say tools aren't important — you'll still need the right combination of technologies and solutions to defend your organization — but your toolset needs to be built around your people and their needs, not the other way around.

Without the right culture in place, your tools won't be worth anywhere near as much.

> "It's important to get that culture right, to build the foundation so everyone is rowing in the same direction, and then layer the toolset on to make life a little bit easier." — Eric Anderson, Symbol Security

On the same note, the best approach to tools is usually a simple one. Sam says, "If you can do it with three tools instead of five, do that. If you can do it with one tool instead of three, do that. Try to simplify as much as possible, because it has to be easier to do it right than to do it wrong."

DYOPATH & Symbol Security

Symbol Security is dedicated to changing the way organizations manage their cybersecurity training. Their solution helps companies build training programs around immersive simulations and gamification so employees engage more and respond better to what they learn.

Now, every DYOGUARD user will get free cybersecurity training as a result of our partnership with Symbol Security. It's our way of helping you and your employees develop better habits and become more security-aware, both in the office and at home.

To learn more about DYOPATH, DYOGUARD, and this new partnership, schedule a demo with us.

If you want to learn more . . .

Visit our Website

☎ Call us at (866) 609 - PATH

✉ Email us at solutions@dyopath.com