HOW TO DEVELOP A CULTURE OF SECURITY

Security in the workplace has become a global headline. I'm sure you have heard about the attack on Costa Rica, Uber, multiple healthcare providers, Twitter, Marriott and many others. These types of attacks are going to continue into the foreseeable future, and we have to create a culture of security with a new and heightened level of awareness and scrutiny within our organizations. These attacks are hitting schools, community colleges, universities, businesses of all sizes and types. I've had many business owners say to me something like, "Surely I'm small enough that they won't care amount me?" However, that is simply not true. They are hitting 10 user networks, 2 user networks, global powerhouse organizations, and everyone in between. Everyone is a target. So, how do we build a culture of security?

1. **Have a candid conversation with your team** stating, "It might be us next!" The bad actors are most likely to get in through people and social engineering. The best security in the world will not be enough if a teammate lets the bad guys in. If you would like someone from the JMARK team to come in and speak with your organization about best practices, please contact us here. We're happy to come in (virtually or in person) and provide context of how serious the threat is, why individual vigilance is so important, and how they can keep themselves and your organization safe.

2. **Make sure that you have the right partner to help create a security strategy.** This needs to include many layers of protection. You can find the JMARK checklist here. A single IT department, an "IT Guy" or even a small MSP cannot have the necessary subject matter expertise and/or resources to deal with all the unique threats against different technologies.

3. **Designate a Security Director in your organization**. They should have the responsibility to check out third party integrations, current vendors, develop the business continuity and disaster recovery plans and more. They should also provide a security update to both the executive team and the board of directors. If you would like help with this role, please contact us here.

4. **Discuss security often**. The CEO or senior leader should bring up security in every company meeting. Take 5 minutes, read a story, play a video, share a real-world experience about how the bad actors are shutting down businesses, costing them hundreds of thousands and sometimes millions of dollars. Many organizations cannot handle being down for weeks and paying $400k or more, even with insurance in place. Make the message real and personal and show how all the hard work of the team can be lost in a matter of hours through a simple click on a link in an email. Security management is ***everyone's*** responsibility.

5. **Be consistent and intentional**. In addition to the CEO sharing about the threats in meetings, we encourage you to have other leaders bring it up in team standups or departmental meetings. The team needs to be reminded from all levels within the business. Additionally, we recommend that you tie employee review scores to their security awareness. We don't want to create an atmosphere of fear of stepping up when a mistake is made. In fact, you should cultivate the opposite. Your employees should be commended and rewarded for stepping up and saying, "I think I made a mistake.". As a part of the

review process, the supervisor should verify that all training has been completed, discuss if the user is helping others to be mindful, and stepping forward if they suspect an issue.

6. **Engage your team.** From our checklist, you'll see that having Multi-Factor Authentication (MFA) and User Awareness training are high on the list. However, this should not be seen as a guarantee or provide a false sense of safety. MFA is awesome, but bad actors can deploy malware into an environment with as little as a click on a link. Awareness training and MFA together make a big difference but keeping your team vigilant and engaged in the security process is vital.

If you would like to learn more, we'd love to share. Just book a call here.