Creating a Cybersecurity Culture

Employees are an organization's first line of defense against cybercriminals. For this reason, they are also commonly targeted. In fact, the vast majority (88%) of data breaches are caused by employee mistakes, according to Stanford University. Unfortunately for organizations, a single mistake can result in costly losses, reputational damage and lost or stolen data.

In order to keep your organization safe from cybercriminals, cybersecurity must become an integral part of company culture—something that is valued and upheld by every member of the organization. Cybersecurity should be top of mind for every employee when choosing whether to click a link, open an email or download documents from the web.

This article contains tips for improving employee engagement and creating a cybersecurity culture that will help protect your organization against cybercriminals.

Cybersecurity Culture Explained

An organization's security culture will not grow on its own. To transform security training into everyday practices, organizations must invest in their security culture and constantly nurture it. A strong and resilient cybersecurity culture can benefit an organization in a number of ways, including:

- Protects the organization against cyberthreats and data breaches
- Strengthens customer trust and loyalty
- Improves brand reputation

Although many organizations recognize the benefits of having a cybersecurity culture, they may fail to successfully create one for multiple reasons. One of the most common reasons is a lack of employee buy-in. In fact, one survey found that 60% of organizations don't believe they have successfully achieved employee buy-in for cybersecurity practices. Lack of executive buy-in is also a common cause of failure. This may result from outdated thinking that cybersecurity only belongs to the IT department or a lack of understanding about the pervasiveness of the issue.

Fortunately for organizations, the main stumbling blocks to creating a thriving cybersecurity culture can also guarantee success if leveraged effectively.

Best Practices

When cultivating a cybersecurity culture, organizations should consider the following best practices:

- **Engage the C-suite.** Senior executives are sometimes resistant to adopting good cyber hygiene. This has to change if your organization is going to create a successful cybersecurity culture. Employees need to see management leading by example if they're going to buy into a healthy cybersecurity culture. Encourage leaders to join the conversation and reinforce that cybersecurity is every employee's responsibility.

  Additionally, senior executives are one of the biggest targets for cybercriminals. Ensure they are doing their part in upholding cybersecurity values by teaching them how to identify and defend against targeted cyberattacks.

- **Inspire ownership of cybersecurity.** Clearly communicate what's at stake to your employees and explain that your organization needs their help. It's not enough to simply explain changes to security protocols. Ensure employees understand why these changes have been made

and what you're trying to do to protect the organization. It's imperative that employees understand that no security system is foolproof and, therefore, it's up to them to minimize threats and avoid unnecessary risks.

- **Create engaging cybersecurity programs.** Cybersecurity training should not be presented as a one-off occurrence. If you want your employees to embrace cybersecurity as part of their culture, provide fun training based on real experiences. Consider leveraging discussion forums, online games, in-person training and mock phishing exams as part of your holistic approach to cybersecurity learning. Brief and frequent lessons will also be more digestible and remind employees that cyber awareness is part of their corporate life.
- **Bring back the basics.** When discussing cybersecurity, many organizations make the mistake of skipping basic training. This can cause confusion and prevent core cybersecurity values from resonating with employees. According to one survey, 50% of all employees haven't had formal cybersecurity training, and 96% keep passwords saved on their devices for easy access. When creating and teaching good cyber hygiene, don't forget basic principles such as strong password policies, two-factor authentication and limits on security, downloads and network access.
- **Make it easy.** Ensure employees know where to report suspicious emails and how to check the authenticity of work-related communications. Whenever possible, encourage open lines of communication between your employees and the IT department. This will help encourage employees to proactively reach out to IT for help or to report mistakes.
- **Celebrate success.** Make cybersecurity part of performance reviews and reward systems. It is also beneficial to acknowledge employee successes one-on-one by expressing appreciation or offering rewards for their commitment to your organization's cybersecurity goals.

Conclusion

When workplace cybersecurity is treated as a simple check-the-box exercise, costly mistakes can occur. Teaching employees to value and take responsibility for their actions can help organizations reduce their chances of becoming a victim of a cyberattack.

Contact us today for more cyber guidance.