Cybersecurity: 5 Ways to Combat Threats in Your Organization

Headlines about security breaches, malware and hackers have become an everyday part of our personal and professional lives. That doesn't mean we give up or give in to cyber threats. As digital citizens, we – and our employees – dig in.

October marks the time of year known as National Cyber Security Awareness Month (NCSAM), a joint effort by DHS and the nonprofit National Cyber Security Alliance (NCSA) to educate Americans about cyber threats and share tips and best practices for staying safe online. Here are five ways your organization can promote cyber safety this month.

1) Share Tips and Resources with Employees

Cybersecurity is the responsibility of every employee in your organization, not just the IT professionals. We all have a role to play in keeping our internet-connected devices free from malware and infections. Remind employees to regularly scan for viruses and spyware. Keep software up to date.

For employees with home offices, provide guidance for protecting you and your clients' data. With family members using the internet to engage in social media, adjust the thermostat and shop online, your employees must ensure that their networks and devices are secure.

Share these and other NCSA tip sheets with all employees, regardless of their work location:

- Safety Tips for Mobile Devices
- Keep a Clean Machine
- Passwords and Securing Your Accounts

2) Assessing and Developing Cybersecurity Competencies

When you're conducting competency assessments, be sure to assess cybersecurity skills appropriate for each job role. Every employee needs to master at least a basic set of cybersecurity core competencies. IT professionals, of course, will need more specialized cyber skills and competencies.

This month, encourage employees to close cybersecurity skills gaps by taking a course that shows them how. An interactive learning experience will be more effective in shaping employee behavior than a simple tip sheet. And there are many courses that touch on online safety. In fact, one of the most popular courses that Avilar offers through our content partners is *Protecting Your PC from the Bad Guys*. It's a timely course that shows participants how to practice safe computing to minimize the chance of infection from malicious software.

By delivering employee learning, you'll be closing skills gaps, better protecting your organization and tapping some of the secondary benefits of learning, such as improved employee engagement and retention.

3) Showcase your Cybersecurity Professionals

In its ratings of top cyber threats, Forbes includes a "Lack of Skilled Cybersecurity Workers." Both public and private sectors are having difficulty finding, paying for and keeping employees with cybersecurity skills.

NCSAM is the perfect opportunity to put a spotlight on your employees whose job it is to protect your IT infrastructure and company devices from the cyber bad guys. If you have a monthly newsletter, include a photo of the team with a "thank you" message. Write an article or blog on one or more of your cyber professionals about why they chose a career dedicated to fighting cyber threats. What do they love about their jobs? What have they learned about cybersecurity since joining your organization?

Your efforts will reinforce your messages about cyber best practices, while recognizing valuable team members that you want to keep.

4) Support Local STEM Programs

The pipeline for future cybersecurity professionals is made up of children interested in Science, Technology, Engineering and Math (STEM). Even if cybersecurity is not core to your organization's mission, you can benefit from supporting local STEM programs.

Encourage your IT employees to speak at local schools or serve as a guest teacher at a STEM camp. Celebrate all employees who help out at a local robotics competition or coding hackathon. Increased company involvement leads to higher employee morale, stronger relationships with potential future employees, and more goodwill in the community.

5) Engage in the #CyberAware Social Conversation

Regardless of whether you're a NCSAM Champion, engage in the #CyberAware social conversation. Share posts from others on the importance of cybersecurity. Create your own posts about any NCSAM activities you're doing this month. Tag resources such as the DHS Cybersecurity initiative (@Cyber), National Cyber Security Alliance (@StaySafeOnline) and their Stop Think Connect cybersecurity education campaign (@StopThinkConnect).

Since hashtags are useful for finding topics people care about, include relevant hashtags in your posts, including these:

- #CyberAware
- #CyberMonth2018
- #cybersecurity
- #CyberThreats
- #NCSAM2018
- #onlinesafety

Is Your Cybersecurity Plan Up-to-Date?

Cybersecurity is a serious topic. With so many people talking about it this month, it's a perfect time to generate some engaging and empowering activities to get people involved. It's one of the best ways to protect your employees, clients and organization.

Looking for ways to strengthen your cybersecurity competencies within your organization? Read our whitepaper, *Advancing Cybersecurity with Competency Management*. Or contact us. We're always ready to support the good guys!