6 Steps for Building a Cybersecurity Culture

Cybersecurity has become a top priority, with responsibility generally handed over to IT and cybersecurity groups. But is that the right way to go? Probably not. A more effective approach would be to instill the entire organization with a cybersecurity culture, where protecting critical assets is a shared responsibility across all functions and levels.

Why aren't your cybersecurity strategies working?

Your network security systems aren't keeping pace with growing threats. Your cybersecurity team is plagued by increasingly frequent, sophisticated and costly threats. Having witnessed industry debacles such as last May's WannaCry ransomware, the recent Equifax disaster and the 2016 breach in the U.S. Voter Database, C-level executives in all sectors are justifiably nervous and frustrated.

Looking at the big picture, cybercrime cost the global economy $450 billion in 2016. At the same time, the Hiscox Cyber Readiness Report 2017 found that 53 percent of study participants were ill-prepared for common criminal tactics – from phishing emails and weak passwords to malware packaged in JavaScript attachments and social media attacks.

Looking at the public sector, fully 28% of Americans are not at all confident that the federal government can protect their personal information. And with good reason. According to a 2016 report by Privacy Rights Clearinghouse, federal and state government agencies

publicly disclosed a total of 203 data breaches over the last five years, resulting in nearly 47 million records being stolen, exposed or otherwise compromised.

So who or what is to blame: The security system? The IT group? You may have top-notch security technology and competent staffing, but without C-Suite leadership, vision and action, other defense strategies tend to fall short.

A true cybersecurity culture starts at the top.

Cybersecurity has become a top priority, with responsibility generally handed over to IT and cybersecurity groups. But is that the right way to go? Probably not. A more effective approach would be to instill the entire organization with a cybersecurity culture, where protecting critical assets is a shared responsibility across all functions and levels.

Creating this culture shift requires leadership involvement at the uppermost levels. But where to start? October is National Cyber Security Awareness Month (NSCAM), the ideal time for C-Suite executives to become fully engaged in creating a cross-functional cybersecurity culture.

Here are 6 ways for the C-Suite to transform the organizational culture:

Be proactive: Take a forward-looking, strategic approach to cyber defense that balances tools, process and people.

Include security in the C-Suite: Ensure that cybersecurity has a prominent voice. Consider adding the role of CIGO (chief information governance officer) or CISO (Chief Information Security Officer) to the C-Suite.

Get educated. Start by learning about the acknowledged weakest link, employee behavior on networked computers and devices. Dig into

behaviors, incidents, associated risks and protection against phishing emails — the number one attack vector, social media attacks and other pitfalls.

Allocate adequate resources: Provide for sufficient cybersecurity staffing and expertise. Invest in a collaborative, end-to-end cybersecurity solution such as the Fortinet Security Fabric.

Insist on full participation: Require, support, participate in and reinforce company-wide cyber policies that include training, testing and accountability.

Review cybersecurity status: Take part in regular examinations, at least yearly, of data security and privacy processes determine if the right systems and people are in place.

A cybersecurity culture requires C-Suite leadership, security expertise and strong endpoint security. As a partner of Fortinet, Proactive Network Management Corporation (PNMC) offers the expertise and best-of-breed cybersecurity technology you need to reinforce the efforts of your cyber-aware workforce. Contact us to learn more.