How-to


Getty Images

SECURITY > THREAT MANAGEMENT

# Building an Effective Cybersecurity Culture

You can have a top-notch cybersecurity defense in place, but if employees aren't taking their responsibilities seriously, your organization will still be at risk. That's why a strong cybersecurity culture is a must.

Karen D. Schwartz | Jul 08, 2021

Having the right tools and good security specialists goes a long way toward creating a secure organization, but it's really only half the battle. If your employees don't take cybersecurity seriously, you've still got a big problem. From apathy to

Increasingly, companies understand that the culture around cybersecurity has to be cohesive and effective. A report from Osterman Research found th security and IT leaders say developing a strong cybersecurity culture is extremely important. About three-quarters of those leaders say employees are as important or more important than technology in keeping organizations secure.

Yet few are getting it right. A KnowBe4 report, for example, found that employees working in a poor cybersecurity culture will share credentials 52 times more than employees working in a good security culture. Kai Roer, a security culture researcher at KnowBe4, said the company has found that no industry sector reached what it defines as a good security culture.

While the situation may seem hopeless, that's far from the case. Here's how to attack the problem:

**Take your company's cultural temperature**. Finding out how employees classify their cybersecurity hygiene, how they perceive cybersecurity at the company, how they see their role in organizational cybersecurity, how well they adhere to policies and security practices, and how willing they are to learn more and change is an important first step in making changes. Many companies use one of the available cybersecurity culture surveys, such as the Infosec IQ Cybersecurity Culture Survey or KnowBe4's Security Culture Survey.

Donna Gomez, a security risk and compliance analyst in Johnson County government in Kansas, is a big fan of these types of surveys. She's led surveys of the county's 3,800 employees numerous times over the past several years and finds them valuable. "These surveys really help gauge what we're delivering and whether it is meeting the objectives," she said. "It helps us provide the right tools and education to make them less of a victim."

**Eliminate blame.** Many security issues are caused by user error, but blaming

culture of blame, people won't step forward," she said. "Instead, it should be about helping people avoid those mistakes in the future. They have to kn rewarded for honesty, not penalized."

**Develop security awareness training programs based on your organization's specific weaknesses.** "We see the security awareness program as a way to improve virtually all cultural security issues," said Megan Sawle, Infosec's vice president of marketing and research. "It's about delivering content that can built toward the more ambitious goals of building trust, increasing engagement and changing the way people feel about the outcomes of security incidents." It's important to make the training engaging, as opposed to the PowerPoint approach, she added.

It's also important to target the training at specific users who exhibit specific issues. That's important, Roer said, since everybody's psychological triggers for action are different.

"Some employees may be tricked by one kind of phishing attempt but not by others. By identifying what kinds of phishing work on each employee, you can help train specific employees on their specific issues," he said. In addition to improving outcomes, it also makes the process more pleasant, since employees won't have to sit through sessions that may not be relevant to them.

**Create incentives**. Many companies find that the carrot-and-stick approach can work wonders. Gomez, for example, is using some of the simulation games provided by Infosec, such as "Choose Your Own Adventure," scenario-based training disguised as a game. Nair uses a different type of incentive approach for her company by setting up simulated phishing attacks and publicizing employees who don't take the bait. "Basically, it's about creating heroes, which gives people positive recognition for doing something good. This builds the culture you want."

are tougher, and you have to keep trying to reach them," Gomez said.



0 COMMENTS

## RECOMMENDED READING

### US Accuses China of Using Criminal Hackers in Cyber Espionage Operations
JUL 20, 2021

### Microsoft: Israeli Firm's Tools Used to Target Activists, Dissidents
JUL 16, 2021

### Attackers Exploited 4 Zero-Day Flaws in Browsers
JUL 16, 2021

### SonicWall: Ransomware Attacks Targeting End-of-Life Appliances
JUL 15, 2021