Cybersecurity at MIT Sloan

THE WALL STREET JOURNAL.

September 8, 2022

THE WALL STREET JOURNAL.

JOURNAL REPORT | TECHNOLOGY

How Leaders Can Create a Cybersecure Workplace Culture

Everyone pays lip service to the idea of creating a cybersecurity-resilient organization. But few leaders know how to actually make it happen.

It certainly isn't easy. New vulnerabilities emerge every day, as malicious cybersecurity actors find fresh ways to attack or infiltrate organizations. Technology can help, but it can only do so much. Just as important is a culture where all employees fill in the gaps—by noticing anomalies, questioning things that might look legitimate but are slightly off in some way, or stopping compromised processes that would otherwise proceed.

But how do you get employees to absorb the values crucial to creating a cybersafe organization? For several years, we have been studying companies that have managed to do just that, and we have identified seven actions that corporate leaders can take to make sure that every employee participates in keeping the organization secure.

Shine a light on cybersecurity routinely: The more a leader highlights the importance of cybersecurity, the more employees will pay attention. In the organizations we studied, we learned that when employees know that cybersecurity is important to their supervisor or higher up the food chain, they develop an attitude that it's something worth spending time on.

In one company, employees regularly heard the CEO praise the cybersecurity team in all-hands meetings, and explain why cybersecurity was important. That inevitably filtered down the ranks. Employees we spoke to had little doubt that cybersecurity wasn't just an empty catchword, and they found ways to contribute.

In another company we studied, some employees were asked to create a short video of a cybersecurity issue—such as keeping documents private, or how to protect credentials—and share it with their team members. The research these team members put into the creation of their video not only benefited them, but also created a library of short, fun videos for all team members to learn from.

Use the right language: In one company we studied, the leaders emphasized the importance of "data protection," rather than calling it "cybersecurity" in their communications and training. That may sound trivial. But we learned that employees found "cybersecurity" too nebulous. They knew it was important, but didn't really know what it meant or how they could contribute. When the focus changed to "data protection," it created a monumental shift in their attitudes. They knew what data was, since they worked with it all the time. Protecting data was a value they could rally around, and they did.

Make it fun, or at least easy: The less friction a company creates around cybersecurity, the more likely employees will take the appropriate actions. For example, in several companies we studied, the security team had added a button to their email client that made it easy for employees to forward suspicious emails to security. What happened next was no surprise: Employees were more likely to forward suspicious emails in those companies than in companies where employees didn't have as easy of a way to do this.

In another company, the cybersecurity culture leader used well-known games, movie clips and songs to instill cybersecurity messages. These were so popular that employees eagerly awaited the next one, and in the course of having fun, their attitudes—and cybersecurity behaviors—changed. **...**

TO CONTINUE, SCAN QR CODE

Dr. Pearlson *is the executive director of the Cybersecurity at MIT Sloan (CAMS) consortium.* **Dr. Madnick** *is the John Norris Maguire professor of information technologies, emeritus, at the MIT Sloan School of Management and the founding director of the CAMS research consortium. They can be reached at reports@wsj.com.*

THIS QR CODE WILL DIRECT YOU TO THE CAMS WEBSITE
https://cams.mit.edu
SCAN ME

THIS QR CODE WILL GIVE YOU ACCESS TO A DIGITAL COPY OF THE ARTICLE
SCAN ME