THE WALL STREET JOURNAL.
English Edition ▾ | Print Edition | Video | Podcasts | Latest Headlines

BUSINESS JOURNAL REPORTS: TECHNOLOGY

How Leaders Can Create a Cybersecure Workplace Culture

Bosses can start by highlighting the importance of cybersecurity—as often as possible

September 8, 2022

By Keri Pearlson and Stuart Madnick

Sept. 8, 2022 10:00 am ET

Everyone pays lip service to the idea of creating 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 an 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.

Make heroes out of those people who have the values you are hoping to instill in all employees: When you see someone doing something to make the environment more secure,

make sure everybody knows. One company we studied offered electronic badges to employees who went above and beyond by demonstrating cybersecurity values. The rewarded employees could put the badge into their email signature, and they did. Those e-badges signaled to everyone else that this was a "cyber-hero." Hokey? Maybe. Effective? Definitely. These heroes became the go-to informal leaders within their teams, reinforcing cybersecurity values. The more heroes in your team, the more secure your team will be.

Focus on rewards as well as training: Many organizations implement training programs and awareness campaigns to instill cybersecurity values. Those are important to set a baseline, but they aren't enough. We asked employees what they remembered from their training or awareness campaigns. Often, employees could only tell us *when* they had their latest training class, not *what* they learned. They had only done the class (usually online) because it was required. They often were doing their email or other activity on the side, because the training happened when the organization needed them to do it, rather than when it was the optimum time for the employee. Little wonder that long-term retention was low or nonexistent.

Organizations that were more successful went beyond training and awareness. In several organizations, leaders offered rewards for security activities. One leader in a bank we studied offered a chocolate-chip cookie to the first 100 employees who responded to a list of activities he created to foster a cybersafe culture. He ran out of cookies within the hour. Another organization offered incentives such as company-branded swag that could be earned by completing tasks, and fun titles (such as Password Knighthood) for those who entered friendly competitions between teams. A third company included a cybersecurity evaluation in the employee's annual review, and that drove the attitude that cybersecurity was both important and rewarded.

Follow the money: Leaders who invest in cybersecurity initiatives send the message that this is important, and those who consistently overlook funding cyber-initiatives send the opposite message.

When we talked to product designers and developers, they regularly told us that cybersecurity was important, but also often said it wasn't their job to build secure offerings. They clearly had gotten the message from their bosses that they should give priority to meeting, say, time-to-market schedules or design elegance. Cybersecurity features were low on the priority list.

In fact, we heard that designers were never praised for secure designs, but were regularly praised for elegant or functional designs. Managers could intervene here by making it clear

that customers increasingly value cybersecurity, in some cases refusing to even consider doing business with a company that wasn't viewed as cybersecure. In one company, developers met with key customers to understand why cybersecurity was so important to them. At this company, managers not only told designers to give priority to cybersecurity but also followed through by praising them for doing so.

Extend the cybersecurity attitudes to employees' personal life: Today's hybrid work environment is accompanied by a bigger blending of home and work life. Cybersecurity follows this, too. Assisting employees to have a cybersecurity attitude at home is another way companies can build the beliefs they want in the office.

One company we studied invested in password managers for the office and a second copy for employees to use for their personal credentials. Another company regularly shared stories about cyber-breaches and discussed the potential personal impact. These activities demonstrated to employees that the company was supportive of their personal cyber safety, which, in turn, shaped beliefs that being secure wasn't just something the company wanted done to keep itself safe, but was both personally and professionally important to the employees. The result was that employees didn't have to shift their thinking when they went from home to the office or from office to home. They thought about it all the time. And that made everyone a lot more secure.

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.

Next in Journal Reports: Technology