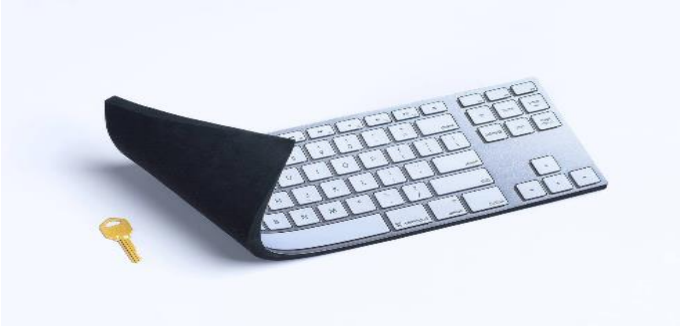
JOURNAL REPORTS: LEADERSHIP

How Companies Can Create a Cybersafe Culture at Work

Employees know hackers are gunning for them. Yet they still keep falling for their tricks. Companies can change that.



Unfortunately, most of the things companies are doing to change their cybersecurity culture simply don't work.
ILLUSTRATION: KEVIN VAN AELST FOR THE WSJ

By Stuart Madnick
May 29, 2018 10 12 p.m. ET

As technical defenses against cyberattacks have improved, attackers have adapted by zeroing in on the weakest link: people. And too many companies are making it easy for the attackers to succeed. An analogy that I often use is this: You can get a stronger lock for your door, but if you are still leaving the key under your mat, are you really any more secure?

It isn't as if people aren't aware of the weapons hackers are using. For instance, most people have heard of, and probably experienced, phishing—emails or messages asking you to take some action. ("We are your IT dept. and want to help you protect your computer. Click on this link for more information.") Although crude, these tactics still achieve a 1% to 3% success rate.

Then there are the more deadly, personalized "spearphish" attacks. One example is an email, apparently sent from a CEO to the CFO, that starts by mentioning things they discussed at dinner last week and requests that money be transferred immediately for a new high-priority project. These attacks are increasingly popular because they have a high success rate.

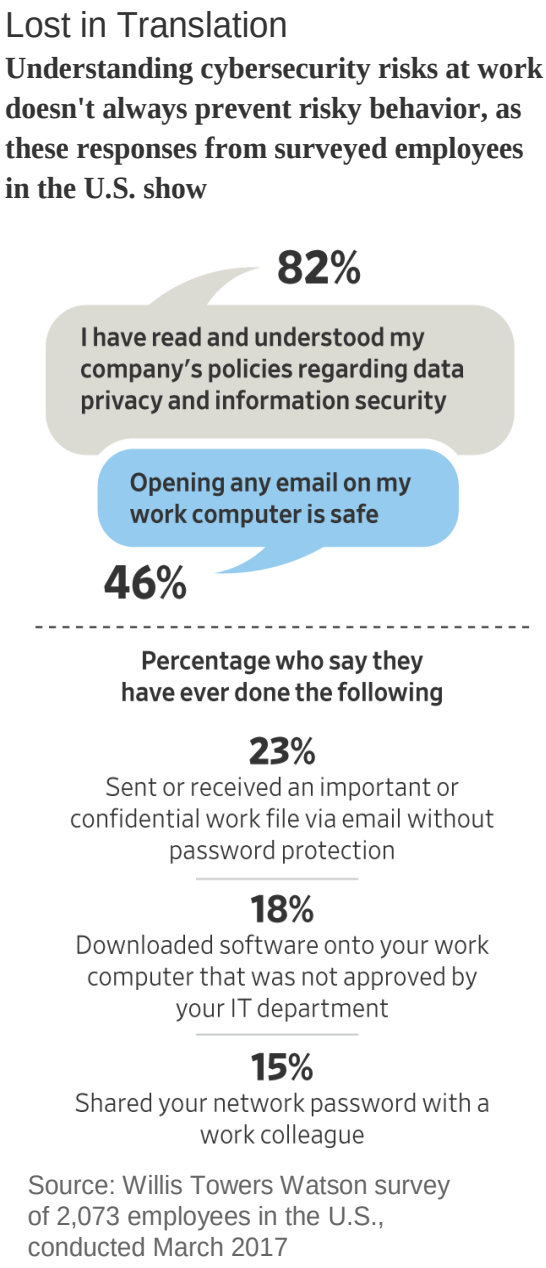
The common element of all these kinds of attacks: They rely on people falling for them.

Too much information

Such gullibility, unfortunately, is a self-inflicted wound, the result of a cyberculture where people are willing to share all kinds of information and try new things all the time. There are lots of good things about that, but also much that is dangerous. So now is the time for companies and institutions to change that culture. It won't be easy, and it will take some time. But it's crucial if we want our companies and information to be safe from cybertheft. We have to start now, and we have to do it right.

Unfortunately, most of the things companies are doing simply don't work. In our studies, we have found that such typical initiatives as distributing fliers about cybersecurity, sending people to a one-time training class, or asking them to view a 30-minute video are pretty much worthless. People do them, but they don't retain enough information and they don't change their behaviors.

To understand what does work, it's helpful to learn from some prior successful efforts to change our culture. A good example is smoking. When the U.S. Surgeon General came out with his report in 1964 outlining the dangers of smoking, things didn't change immediately. Photos of lungs blackened by smoking, though disturbing, had little impact, with responses like, "It is my body, leave me alone." Over time, though, what had more impact
regarding smoking was society's reaction. It is not just about you, but about the others that your action affects. It's about how your smoking damages your family.



Out of curiosity

To better understand how far we have to go in creating a cybersafe culture, consider this: If you were taking a tour through a nuclear plant, and there was a big red valve with a sign on it that said "Do not touch," how many of you would turn it? None, I would guess. But in a phishing test conducted at a major financial-services firm, one of the test emails actually said: "This is a Phishing Test. Clicking the link below will cause harm to your computer." At least one executive clicked it! When asked why, he said, "I was curious to see what it would do." To me, that is pretty strong evidence that people are generally unaware of the dangers that they expose themselves, and their organizations, to on a regular basis.

So, how do we go about creating a cybersafe culture? What are the key elements? My colleague, Dr. Keri Pearlson, our executive director, and the rest of our Cybersecurity at MIT Sloan research team have interviewed many companies working toward just such a culture. Here's a look at approaches and actions that we have found most effective.

Get everyone involved: This seems like such a simple concept. But most companies aren't there yet. At too many companies, cybersecurity is still seen as a technology issue, or the responsibility of the IT department or, at best, management. But cybersecurity requires the active efforts and cooperation of everyone in the business.

The need for leadership: Having said that, individual motivation doesn't appear automatically or magically. There needs to be strong attention and support from top management and a clearly designated manager and team who are responsible to help develop, support and sustain the cybersecurity culture.

Passive solutions: These are things that require minimal, or even no, conscious action from the employee, such as segregating the network used by personal devices, such as your smartphone, from the corporate network, or requiring two-factor authentication to connect to the corporate network.

Another tactic: Filter emails and put suspicious emails in a separate folder. In this way, it highlights the fact that employees should make sure they know who the email is from and what the attachment is before they open it.

Active reminders: Culture is not a once-a-year, or once-a-month, event. It must be continuous and integrated into daily life.

At the entrance of many factories, for instance, you will see a sign, such as: "542 days since last industrial accident." Do you want to be the person to reset that number to zero?

But have you ever seen a sign at a data center or office that said: "5 minutes since last successful cyberattack"? Probably not, but you should. Companies should regularly remind workers how many attempted cyberattacks their organization had today, and how many were successful, and if things are getting better or worse.

Along those lines, companies should implement phishing tests, whereby potentially dangerous emails are sent to employees to see who will fall for them, with feedback to the careless employees, and reminders that suspicious emails or events should be reported.

Simulations of cyberattacks, similar to fire drills, can significantly increase awareness and understanding of the complexities of an attack.

Another active reminder is a note added to each email that someone receives that says, "This email has an attachment. Be sure you know who it is from before you open it. We don't want to aid a cyberattack."

What's more, we need to make sure people understand that this isn't just about them. It's about everybody they work with. I recently observed a large poster on the scaffolding of a construction site near my office. It was of a worker holding a photo of his family. The caption was, "I know why safety is important." The point is: His family relies on him, and he owes it to his family to be safe at work. That was the same message that finally got through to smokers. And that's the same message that we need to get through to employees about cybersecurity dangers. Companies have to make it clear that clicking on just that one phishing email can open up the entire information system to the bad guys, shutting down many other systems, or worse, holding the systems for ransom.

Engaging and fun: This is where there are the most opportunities for both creativity and benefits. Most companies are effective at conducting market research to understand their customers and how to influence them. But they aren't nearly as diligent about understanding their employees.

Yet understanding what motivates their specific employees is key in finding the most effective cybersafety strategies. We have seen engaging and funny videos and songs that connect with employees, as well as badges for "responsible cyber-defenders." What may be hokey for one company can be highly effective in another one. In one organization, there is a "cybersecurity superhero" who travels around the company and personifies and promotes the organization's commitment to cybersecurity.

It's a team effort: It is hard to change the culture of a single individual or have an immediate impact on an entire large organization. That's why the group—however defined—is so crucial.

Using the smoking example, having the spouse repeatedly say, "Please do not smoke, you are endangering me and the children," provides significant impact. Similarly, having a colleague talk about how a careless employee is putting the rest of the group in danger of cyberattacks puts a lot of peer pressure on the employee to change his or her behavior. We have seen companies run periodic phishing tests where the results of the overall group, as well as individuals, are posted—with recognition rewards for the most cybersecure groups. Do you want to be the one who lowers the score for your group?

Another example is to have a "cybersecurity moment" at the beginning of each team meeting where the group briefly talks about a way to be secure or discusses a recent incident—anything to raise awareness and promote cybersecure behaviors.

We have found it's also crucial that each team has a cybersecurity leader who brings and shares skills and ideas back to the rest of the team.

Measurement and accountability: Best practices need to be built into the regular daily work processes, not just be afterthoughts. Success stories, such as those emerging from group activities, should be highlighted, publicized and encouraged.

As is often said, "if you cannot measure it, you cannot manage it." There need to be ways to measure the organization's cybersafety level—and how it is changing over time. Cybersafety effectiveness needs to be a valued part of everyone's skill set and incorporated explicitly into performance and bonus reviews.

For instance, employees who repeatedly fail a phishing test can be disciplined or even terminated. Nothing changes behavior faster than rewards and consequences.

In the end, it's crucial that support and enthusiasm for increasing cybersafety be visible at every level of the organization, from top executives and middle management to the individual. It needs to be integrated into how employees are trained, managed and rewarded. It needs to be a way of life.

Dr. Madnick is a professor of information technologies, MIT Sloan School of Management, and a professor of engineering systems, MIT School of Engineering. He can be reached at reports@wsj.com.

Appeared in the May 30, 2018, print edition as 'How Firms Can Create A Cybersafe Culture.'