Why Companies Should Stop Scaring Employees About Cybersecurity

If they want workers to be more vigilant, fear doesn't work. Fortunately, there are alternatives.

By Karen Renaud

Dec. 7, 2020 1:00 pm ET

Companies often turn to a powerful emotion to get employees to be vigilant about cybersecurity. They scare them.

If you do *this*, or don't do *that*, something awful will happen. Click on phishing messages, and the company's network will be exposed to hackers. Use simple passwords, and your personal files will get stolen.

The problem: Fear doesn't work. Sure, it may get people to act in that moment. But scare tactics don't get people invested in security over the long term, as Marc Dupuis of the University of Washington and I discovered in research last year.

In fact, it can do the opposite. That is because fear can leave employees in a constant state of anxiety, which makes them unable to think clearly about threats. Alternatively, such heavy-handed, scare messaging can make employees disgruntled and uninterested in security, thinking that the threats are exaggerated—and that bosses don't trust them to do the right thing.

But fear not. Although scaring employees may not be an effective way to keep them vigilant, there are other tools that *do* work. First, let's dig deeper into why fear doesn't work.

WHY FEAR FAILS

Fear is a short-term emotion.

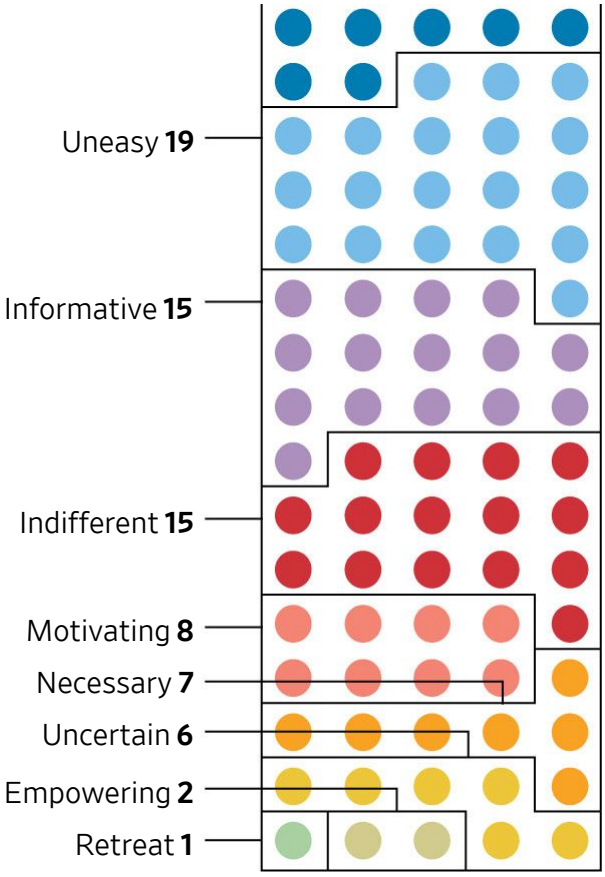
There is no question that fear can work to get people to perform a one-off action, like installing antivirus software. But long-term behaviors are where the problems come in—and long-term vigilance is the real point of cybersecurity. After the initial surge, fear will

wear off and convert to an underlying state of anxiety, which makes people unlikely to get people to commit to frequent actions such as choosing strong passwords.

For example, consider that Jane is told during cyber-awareness training that any email could be a phishing message. If she clicks on an embedded link or opens an attachment, she learns, malware could be installed, and she will lose all the files on her machine and precipitate a major cyber incident at her place of work.

The Fear Factor

Many of the 400 workers in a study indicated they don't feel it is necessary to induce fear for the sake of company cybersecurity.



*Multiple responses allowed
Source: Marc Dupuis and Karen Renaud, Ethics and Information Technology, Oct. 20, 2020

All of this will leave her in a permanent state of uncertainty. Her productivity is likely to plummet because she mistrusts every email that arrives in her inbox, and she isn't sure if links in messages are safe to click on.

In other words, a fear-based approach doesn't encourage genuine watchfulness. Once someone is in a state of heightened fear or anxiety, their brains are fully occupied in dealing with the emotion, making measured and thoughtful action unlikely or impossible, according to Paul Brown, Joan Kingsley and Sue Paterson in their book "The Fear-Free Organization." That means Jane might be so anxious that she can't make informed choices about messages and instead works entirely by impulse.

People don't believe fear appeals.

People have many things to fear in their lives—especially in 2020—and they resent people leveraging even more fear against them. Prof. Dupuis and I recently surveyed 400 people, and one of the issues that emerged during the study was that while many people might believe in fear-based appeals too much—as with Jane in the above example—others think that such appeals exaggerate the risk to give the message more power. We found that only 20.6% agreed that these fear appeals were necessary—so, people are suspicious and reject the entire message.

The crimes come with punishment.

Very often, fear appeals are coupled with harsh punishments for making security errors. Organizations do this for very understandable reasons: If people have an immediate, tangible personal stake in following the rules, the logic goes, they are more likely to stay on the straight and narrow.

One U.K. organization fined employees heavily if they opened attachments on test phishing messages the organization sent out itself. These fines were significant, up to 50% of employee salaries. Another company had a policy of firing staff who fell for such messages three times.

Yet another company posted a photo of people who fell for a phishing message on the communal fridge to embarrass them.

David Rock suggests in his research into the neuroscience of collaboration that an employee who is singled out this way already feels bad about being deceived—and will now experience the equivalent of physical pain at being shamed. One employee of a company using this kind of tactic told me that if she fell for a phishing message, she feared that it would be brought up during her yearly performance review and affect her chances of being promoted—leaving her in a permanent state of anxiety.

These organizations don't seem to understand the harm that they do to employer-employee relations with these campaigns. An organization needs workers to be committed to securing the organization's devices and information. This can't be achieved by eliciting fear and imposing sanctions.

Fear puts employees in a bind.

Companies that rely on fear often make a demand of employees: Deal with the problem yourselves by following the rules. But those fixes are often difficult, at best. And might be impossible. So, in essence, workers are told the dire consequences of not following rules that they *can't* follow.

For example, it is common for password policies to instruct employees to (a) choose strong passwords, (b) not write them down and (c) not reuse them anywhere else. But, given that most people have tens if not dozens of passwords, this rule is impossible to follow—so it is likely that employees will end up in a state of long-term anxiety or simply give up on following the rules altogether.

WHAT WORKS BETTER

So, what is the alternative to fear? Creativity and trust. Giving employees more leeway and support works a lot better than infusing their lives with anxiety and creating an aversion to anything to do with cybersecurity.

Here's a more productive three-pronged approach—drawn from the works of Prof. Sidney Dekker at Griffith University in Australia; former submarine captain and current leadership expert David Marquet; speaker and author Wouter Hart; and my own research with Verena Zimmermann at TU Darmstadt's Institute for Psychology in Germany.

Create a buddy system.

Don't put people in a room and talk at them for hours about security. Give them a "buddy" who's there to help them in the office every day to help them carry out the actions you want.

In the system, instead of trying to train *everybody,* one employee in each department is appointed to serve as cybersecurity expert. This employee is close by to support colleagues day to day, available to answer questions about things like potential phishing messages. If a message does turn out to be a phish, the buddy can warn the rest of the department immediately. Or the buddy could help somebody with a question about how to send files outside the company securely.

Not only does everybody get less stressful support, but they get the message that cybersecurity isn't a solo sport but a team effort.

One company I spoke to uses a tactic along these lines, assigning an employee to be a contact for other workers about potential phishing messages. First, he always thanks them for consulting him. If the email isn't a phish, he will let them know it is safe to click the link or open the attachment. If it is a phish, he praises them for their alertness.

He told me that since this policy has been implemented, people have become far more confident in their ability to spot phishing emails, so most of the queries he now receives are about genuine threats, and he can warn all other employees in time. The organization has had zero successful phishing attacks since it implemented this policy.

Provide adequate resources.

Instead of relying on people to take multiple complex steps to ensure security, give them tools that can help them or automate the job entirely.

For instance, if you want people to have strong passwords, give them a password manager.

It can generate passwords for them and remember those passwords. Or if you want people to spot phishing messages, put a messaging system in place to warn everyone immediately when your organization is being targeted—as opposed to alerting by email, which might go unread for hours. The first person to spot the message lets everyone else know.

What's more, the alert can also explain how to spot similar messages in the future. The entire workforce gets trained on the spot and gains confidence in spotting phishing messages instead of living in a state of fear that they are going to click on something by accident.

Remove obstacles.

A lot of the fear-based cybersecurity messages involve telling people what tools they can't use in the office. But instead of banning such tools, companies should figure out how those tools can be used securely and effectively.

For example, many organizations forbid the use of USB memory sticks. At the same time, they don't provide a feasible way for people to transfer files to others they are collaborating with. When people improvise—such as emailing the files to other people—they also put the information at risk.

Far better to issue encrypted memory sticks that authenticate using fingerprints (no risk of forgetting the password or using a weak one, or being tempted to write it on the drive itself). Yes, it is more expensive than banning the use of memory sticks in general, but it is better to spend a bit more to get actual protection, instead of engaging in what security expert Bruce Schneier calls "security theater"—thinking that banning every possible insecure action is going to work.

The idea is to work with your employees rather than against them. There is no short-term solution to the cybersecurity conundrum. We have to play the long game and find a better way—treating our employees with respect and dignity, and not as the *problem*, but as part of the solution.

Dr. Renaud is professor of cybersecurity at Abertay University's Division of Cybersecurity in Dundee, Scotland. She can be reached at reports@wsj.com.

Corrections & Amplifications

Marc Dupuis is an assistant professor at the University of Washington. An earlier version of this article incorrectly said he was from Washington University. (Corrected on Dec. 8, 2020)