Harvard Business Review | Digital Article

Managing Organizations

Your Employees Are Your Best Defense Against Cyberattacks

by Fabian Muhly, Jennifer Jordan, and Robert B. Cialdini

Your Employees Are Your Best Defense Against Cyberattacks

by Fabian Muhly, Jennifer Jordan, and Robert B. Cialdini

Published on HBR.org / August 30, 2021 / Reprint H06IGS

Illustration by Delphine Lee

According to the FBI, cybercriminals scammed $26 billion between October 2013 and July 2019 with the "Business Email Compromise" scam that, using deceptive and manipulative social engineering techniques, lured employees and individuals into divulging their credentials and eventually making unauthorized transfers or funds. In 2017, MacEwan University in Canada was defrauded of some $11.8 million when a cybercriminal impersonated one of the university's staff members and requested changing the bank account information of one

of its vendors. Another report covering 31 countries — 60% of world population and a corresponding 85% of global GDP — estimated the financial loss of online scams in 2019 to be €36 billion.

In addition to direct financial losses, security-based offenses disrupt a company's productivity — and its public reputation. For example, when 130 high-profile Twitter accounts were hacked in 2020, it was an embarrassing black eye for the company: a startling weakness in the company's security, which was exploited by a 17-year-old's low-tech attack. The vulnerability made the company look silly and caused its stock price to plunge by $1.3 billion (if only temporarily). It could have been much worse, too: Security breaches can also have legal and liability consequences for directors and senior managers.

Individual behavior flaws play a major role in all of these hacks. Attackers take advantage of people's willingness to trust certain requests and to mindlessly click on links or open virus-laden attachments. The human factor is assumed to be the ultimate attack target in 99% of breaches. In a five-year study, researchers successfully penetrated 96% of the security systems across 1,000 banks using human psychology alone.

So, how do business leaders reduce this human-based liability? Leaders logically rely on their security department when it comes to securing an organization's information and investment decisions about the correct tools to do so. But this approach is too narrow. For a truly security-aware culture, all members of the community must be sincerely and wholeheartedly committed — beyond just doing the one- to two-day security training that most companies mandate. Creating such a security-aware culture is facilitated when leaders can influence their team members to adopt certain mindsets and behaviors.

Cialdini's research on the principles of influence has shown that there are six principles that, if harnessed, encourage people to comply with requests or move in a desired direction.

1. People act consistently with the behavior they have shown in the past. Formal and informal commitments lead to similar future behavior.
2. People are influenced by the opinions and behaviors of the social majority. When uncertain how to think or act, people look to the outside world for cues.
3. Reciprocity (or giving something to someone with seemingly no obligation for requited behavior) is one of the best ways to elicit return favor-giving.
4. People want what is rare or seemingly scarce and will make extra efforts to get these things.
5. People are influenced by those who are like them or those they find likeable – that is, people flock to birds of a similar feather, as well as to "feathers" they find appealing.
6. People are more likely to comply with requests when these requests are issued by someone in an authority role (or even by someone with the mere accoutrements of authority – badges, white jackets, business attire, etc.).

Based on Cialdini's principles, we recommend the following six strategies to fortify the human firewall against the deceptive techniques of criminals and foster a security-aware organizational culture.

1. Ask employees to sign a security policy.

Demonstrating commitment, such as signing a code of ethics, makes people more likely to follow through and leads to greater cognitive and behavioral adherence with codes of conduct. These policies are written commitments that state an employee will, for instance, treat all

sensitive corporate information (e.g., customer and contractual data) confidentially, proceed in the best interest of the organization during on- and offline activities, and report suspicious incidents immediately to the respective internal point of contact. Employees also acknowledge that they will not disclose any sensitive corporate information to any external parties.

Within the policy, it's useful to clearly state which kind of information is sensitive and which is not. (E.g., you can't ask an employee to not complain about the company's cafeteria food on social media but you can ask them not to disclose client lists).

For example, CISCO requires its employees to annually sign a code of business conduct that reminds them how to protect the company's intellectual property, as well as confidential information assets. The company requires that its employees not share confidential or proprietary information with people who have no legitimate business need for it and to commit to reporting any observed breaches of such requirement. A corporate culture of blame can discourage employees from reporting suspicious activities, but ensuring they understand the rationale and asking them to sign a policy that signals their responsibility to report suspicious activities can circumvent this issue.

It's important that signing a commitment like this is voluntary — if it's forced, the subsequent internal impulse to commit will be weaker. But the act of signing fosters personal (inside) and interpersonal (outside) consistency pressures, which makes it more likely they will adhere to the company's standards. And it's best if the employees can sign it in the presence of co-workers; once a commitment is public, employees feel obliged to act consistent to the commitment, lest lose face in front of their esteemed colleagues.

2. Lead by example.

In situations of uncertainty, people look around them for cues on how to think and act. On the one hand, this behavior can be framed as conformity, but on the other, it can be seen as a way to help people grasp a common understanding of correct or normative behavior. Looking to others for cues helps to reduce uncertainty — especially when those others are in respected social positions.

Senior leaders, therefore, should lead by example and promote best-practice behavior.

For instance, they should emphasize the importance of security behaviors like not leaving one's PC unlocked, not holding open doors at company site to people without verifying their legitimacy, and not exposing company documents, be they physical or digital, in public spaces. We recommend that leaders also provide contrasting examples of security-violation incidents where either they themselves had been careless or where careless behavior was reported. Doing so will help reduce the "it won't happen to me" feeling of invulnerability amongst the employees.

3. Elicit reciprocity.

There is a pervasive social norm that dictates if someone gives us something, we feel obliged to return the favor. This urge tends to be true even if the original gift was not requested or even if what is requested in return is far more valuable than what was originally given. The norm of reciprocity is important because often the returned favor is done unconsciously.

Senior leaders should be aware of this powerful influencing technique and use it to strengthen a security-aware culture in the organization.

Taking moves to secure an employees' own data or identity, like providing them with secure and encrypted flash drives or with a customizable digital photo frame that displays security reminders can be meaningful first steps to elicit reciprocity.

4. Leverage scarcity.

People find objects and opportunities more attractive if they are rare, scarce, or difficult to obtain. Senior leaders can make use of this psychological tendency when promoting the organization's rare and exemplary security accreditations, such as accredited information security processes (e.g., ISO 27001), that stand to be jeopardized by a security breach.

By doing so and unequivocally communicating to the workforce both the organization's attractiveness as a great place to work due to the security culture, as well as what would be at stake were its security to be compromised (i.e., what one could potentially lose), senior leaders will strengthen employees' commitment to a security culture. Moreover, senior leaders should promote the installation of a classification system that separates innocuous from sensitive information. Employees will acquire a sense for the scarce — must-be-protected — information, which keeps them attentive in competently protecting the holy jewels of the company, instead of the illusionary task to protect all information regardless of its criticality.

5. Be like those you lead.

Security professionals emphasize the importance of an empathetic mindset for achieving compliance in interpersonal situations. People are most influenced by others with whom they identify and like, and leaders can build trust with the workforce when they act with humility and empathy. Leaders who show vulnerability are likely to receive

empathy and sympathy in return. This reciprocal exchange can indirectly foster compliance with senior leaders' directives in terms of ideal security behavior. Sharing their own struggles or storytelling about their own mistakes related to a security culture and how they learned from these mistakes can make them more approachable and identifiable, thereby increasing the chances that others will follow their lead.

6. Leverage the value of authority.

Usually, organizations oblige their employees to take an annual digital security training. There is the real risk that employees click-through the activity but don't connect the contents to their daily behavior. When senior leaders, who employees see as the ultimate organizational authority, personally instruct their workforce to comply with corporate information security, they will be more likely to get the desired outcome. But there's a catch: Leaders need to be seen as a trusted source in addition tobeing the boss. It's the difference between merely being "in authority," ordering the workforce what to do, and being perceived as "an authority," knowledgeable of the topic. Having both is the most effective combination.

Senior leaders need to prove their expertise and educated understanding of information security issues to effectively enforce their instructions and mandates. They can achieve this by preserving a strong relationship to their information security team and regularly keeping themselves and the workforce informed about the latest security advancements. Subscribing to newsletters, such as the ones from SANS, is a good starting point. This recommendation might seem in contrast to the one immediately above (*Be like those you lead)*. But leaders can exercise their authority while at the same time being humble and empathetic.

Scammers and social engineers regularly use influencing tactics to deceive employees, threatening the value and reputation of your organization. The above six recommendations are an easy and cost-effective way for leaders to counteract those information security risks with proven principles based in human psychology.

FM

Fabian Muhly is a researcher in criminology at University of Lausanne, Switzerland, focusing on the topic of social engineering fraud, and is co-founder of Leo & Muhly Cyber Advisory LLC.

Jennifer Jordan is a social psychologist and a professor of leadership and organizational behavior at IMD. Her research and teaching focuses on the leadership challenges of the digital age.

RC

Robert B. Cialdini is the Regents' Professor of Psychology at Arizona State University and the author of Influence: Science and Practice (Allyn & Bacon, 2001), now in its fourth edition. Further regularly updated information about the influence process can be found at www.influenceatwork.com.

