Four Things Consumer Businesses Need to do Now to Protect Themselves Against Cybersecurity Threats

By David Trepp

After years of being able to fly below the radar, consumer businesses now have to deal with being victims of cyberattacks. The relative ease of ransomware, invoice-related fraud and other common cyberattacks has made consumer businesses lucrative targets. As many cyberattacks rely on duping employees via social engineering, training employees is paramount to protecting the company. The question is, then, how do we effectively train our employees? Many companies already employ cybersecurity trainers and offer online trainings as well as heaps of reading materials and videos to their employees. So why do hackers still enjoy so much success with social engineering attacks?

The answer is that protecting against social engineering attacks requires a different kind of diligence. Social engineering preys upon our society's norms governing polite human interaction. Additionally, unlike denial-of-service, SQL injection and other attacks that IT personnel are responsible for detecting, social engineering tactics are generally employed directly against people who have little or no training in cybersecurity.

Stopping these lines of attacks, therefore, requires participation from everyone, and that in turn often requires a major change in company culture. With that end in mind, here are four strategies your company can implement now to reduce your risk and start becoming a "cybersecurity-first" organization.

1. Structure your cybersecurity efforts from the top down

The first and most important step in an effective employee awareness training program is to start with the board and C-level employees. Not only are people in these positions high-value targets who need to be extra cautious, but they are also the folks who set the tone for the entire company. It's the C-level executive and board members who establish a culture of cybersecurity, and as the saying goes, culture eats strategy for breakfast. Setting a security-aware example allows company leaders to exemplify behaviors others will emulate. Conversely, C-suite executives who take a nonchalant approach to security awareness are teaching their subordinates to do the same, thus dooming their organizations to hacks and headlines.

2. Hold training sessions regularly

The next awareness training concept that's important to understand, is that training and testing has to be repeated. One Fortune-50 firm has determined that the average employee falls for a social engineering attack four times before becoming "inoculated" against such attacks. Regularly training, followed by testing employee awareness, is thus key to protecting your organization. Many companies are starting to "gamify" awareness training, holding competitions to see which individuals and teams perform the best in training and testing situations. By awarding prizes for winners, the gamification of training encourages good awareness habits and can also serve the ancillary function of bringing the entire company closer together.

3. Make your cybersecurity tools easy to use

Beyond simply training employees, your IT staff must also provide employees with powerful, user-friendly tools to protect themselves. Starting with clear, easy-to-understand policies and procedures, the organization's security program should provide clear guidance. Additionally, technical tools, such as strong email and web filters, password safe applications and easy-to-use multifactor authentication solutions can halt attacks, or at least make them far less impactful.

4. Empower your employees

Lastly, your organization must empower its employees. Everybody is the security officer, and they must be empowered to make security decisions. Give employees simple, easy-to-remember responses to potential email, phone and in-person interactions and authorize them to call a time-out during which they

can contact IT security to explore the possibility that the interaction may be some kind of scam. Thank them for their efforts and make sure they know that this isn't just some new way to make their lives miserable. After all, security is everyone's concern from the CEO to the janitor. Using these techniques, everyone pulling together can ensure a safe cyber future for the company.

Call to action: As a consumer business, becoming the victim of a cybersecurity attack can deal a permanent blow to your company's reputation. BPM's professionals in the IT Assurance Group leverage their extensive expertise to create a strategy tailored to the unique structure of your business. To learn more, please contact David at DTrepp@bpmcpa.com

About the author:
David Trepp is partner in the IT Assurance practice at BPM, one of the 50 largest public accounting and advisory firms in the country. With offices in the Bay Area, Oregon, India, Hong Kong and the Cayman Islands, BPM helps clients succeed around the world.