August 13, 2018

# If Only Those Employees…

CYBERSECURITY, TECHNOLOGY
BY MATTHEW DUNN

One of the most common sentiments that I come across as an information security professional is that employees are the ones making the organization less secure: *If only everyone was as smart as IT, or a security professional or of high intelligence, no one would click on those phishing emails or get malware from social media sites.* The logic in that type of thinking is flawed and can actually be detrimental to the security of an organization. Let's talk about why that is and what to do about it.

The goal should be to protect our employees as much as possible from cyberattacks, not to waste time blaming the victims.

First, let's get rid of the notion that IT, security and "smart people" in general are immune to phishing and other social engineering attacks. EVERYONE is vulnerable. It isn't just employees in marketing and sales that get phished. As a penetration tester I can tell you this with certainty. We frequently are able to get IT and sometimes even security staff to click on phishing emails and open malware hidden in support tickets. A good phish can trick about anyone, and attackers are much better at phishing than they used to be.

Now, that isn't to say that we need to stop educating our employees about safe computing practices. Employees need to know to lock their computer when they walk away, use strong but easy-to-remember passwords, watch out for suspicious emails, and etc. Let's be honest though. An accountant's job is accounting, an HR associate's job is HR. We can't expect everyone to be an expert outside of their field. For instance, I am great at security consulting, but you wouldn't want to hire me to do your company's taxes. We can't rely on our employees to be experts at defending themselves from cyberattack, but we can help them out.

It is true that currently employees are one of the softest targets, but that is often due to an organization's security and IT controls. Most frequently on our penetration tests, we gain access to a client's network by guessing weak passwords that meet complexity requirements (and that is possible to prevent) or phishing employees, which may require evading antivirus products and other security controls. Once we are on a network, it is often those weak passwords, password reuse, and overly permissive user accounts that allow us to move from victim zero to full control of a network. Employees take the blame, but most often, what it comes down to is corporate culture.

Often, organizations want to make things easy for employees and for the IT team, so they avoid technical controls that make attackers lives' much more difficult. However, there are many technical controls that are mature and, while they may take time to implement, they don't add much complexity for an employee and provide a great deal of added security.

Everyone has a firewall and traditional antivirus and you need those things, but they do little to stop many attackers. To more effectively stop and limit an attacker's impact we need to do things like: ensure that two-factor authentication is used on all possible externally accessible resources, limit administrative credential assignment on a least privilege model, have separate administrative accounts from those accounts that are used for day-to-day work, segregate network traffic (Tom's workstation doesn't need to talk to Janice's

workstation or the backend database server), block bad passwords (even those that meet complexity requirements) and have a better understanding of who/what is on our networks and what they are doing. I have yet to see any organization doing all of what I just listed.

The security controls I presented are not million-dollar appliances that take a team of three or more people to operate. Some are difficult to implement, but many are not. We all want the easy button, and spending money is often easier, but the best things in life don't come without effort. If we put in a little elbow grease with our IT and security practices, we can stop putting so much of the blame on our employees. With that I pose a challenge*: Instead of blaming victims, try to do more to protect them.*

## You've heard our thoughts… We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.