Winning The War On Cybersecurity By Preparing Our Future Leaders

During my time in the cybersecurity industry, I have learned that there are three very important laws to consider. First, if you have data, you have cyber risk. Second, if there is a vulnerability, it will be exploited. And third, humans are far more vulnerable than technology.

In IBM's annual X-Force Threat Intelligence Index 2018, it was determined that "inadvertent insiders" — or employees who accidentally cause security incidents through human error – exposed billions of records between 2015 and 2017. This may help explain why cybercrime keeps getting worse despite the fact that the spend on cybersecurity technologies keeps increasing year over year.

Looking closely at the digital forensics of many breaches, the acquired evidence often points to a similar root cause — people are getting tricked into doing things they shouldn't be doing. Year after year, millions of people simply can't resist the temptation of clicking on those interesting phishing emails, not to mention a wide range of other cyber no-nos. It is clear that hackers are hacking people and not technology. People's tendency to leave personal information on social media that hackers can use against them can make spear phishing attacks worse. The latest edition of Symantec's Internet Security Threat Report found that 71% of the targeted attacks detected in the report used spear phishing to get the targeted user's credentials.

Part of the problem is that we rely on cybersecurity technologies to protect us, but we have not kept our own security awareness skills up to date. We love living in a digital world, and most of us share digital information every day. Even so, many of us, as individuals and as organizations at large, ignore the first law of cybersecurity. We often think, "Who would come after me? I've got nothing anyone wants." And even those of us that believe in and observe the first law of cybersecurity may ignore the second and third by thinking, "It's ok if I do something wrong, like click on this link I'm not sure about. I've got a firewall, I'm protected."

To add to this problem, as organizations and people in general look to others for assistance in this confusing world of cybersecurity, they discover firsthand that there's a massive and still growing cybersecurity skills gap. One 2018 cybersecurity workforce study found that 63% of people surveyed said their organizations had a shortage of dedicated cybersecurity staff, and 59% said that their organizations are at moderate or extreme risk of a cyber attack as a result.

One way I believe we can at least make progress on these issues is by instilling cybersecurity knowledge and awareness in the next generation of internet users.

Let’s talk to our future leaders, the ones currently in grade school and teach them how to determine whether or not certain information is sensitive and how it needs to be protected. Let’s help them understand what a corrupt link, website or attachment looks like and where they are most vulnerable to hackers. We can also teach them about the benefits of joining the cybersecurity industry and how they can find purpose in helping others prevent and detect threats brought on by the digital age.

When you attempt to educate a younger audience (or any audience in the world of cybersecurity), it is best to start with the first law that I mentioned above. Everything in cybersecurity begins and ends with the understanding that if you have data, then you have cyber risk. If your audience truly does not believe their data is at risk, your lesson will fall on deaf ears. If you’re instructing someone, start your lesson with stories and case studies on how real this problem is and make them specific to your audience. A high school audience, for example, may not put much thought into statistics on cyber breaches that negatively impact the healthcare industry, but they will certainly pay attention when they know how it connects to them. From there, move on to the second and third laws, essentially explaining to the audience that their actions have serious consequences.

In the digital world we live in, information is the new currency, and that currency needs to be protected. Good cybersecurity awareness is not just for organizations and not just for governments — it’s for individuals everywhere. In a connected world, we each have a responsibility to protect ourselves and the people we interact with.

The outcome of our new cyber war all depends on how well we train the next generation of future leaders.

By Danny Pehar