Human Factors and Cybersecurity

Steve Durbin, Managing Director of the Information Security Forum (ISF), explains that "Cybercriminals have a deep understanding of human psychology and stress-related pandemic issues. In 2020 alone, Google registered a record two million phishing websites whereas ransomware attacks increased by sevenfold."

Some of the obstacles to security sound organizations, related specifically to people and not the technology, include the disruption of following secure protocols, the perception that security personnel fit a certain model with specific coding and computer science backgrounds, an organizational culture that does not invite or encourage critical thinking, treating every job and person as having the same needs, and investing in training that embraces participation and reinforce desired security outcomes.

While companies invest in security via their IT department, Durbin stresses the critical failings of such a shortsighted approach to preventing cyber breaches, and explains in numerous articles the need to address the entire organization, specifically the human factors aspect of cybersecurity. We highlight some quotes from his, Security of the Workforce, ISF Podcast:

"There's one thing that never changes and that is your ability to correctly predict how people behave. So many people have tried, and many people have failed. And, many people will continue to follow that same road, and I think that from this security standpoint, if you look at what security tries to do, security loves things that are predictable – things that it can anticipate, ideally. And, so people fit outside that realm. And, you hear a lot about zero trust, and all that kind of thing, is the way to go from a security standpoint, but you can't apply that to people. So, if you zero trust any of your people then you might as well pack up and go home. You have no business.

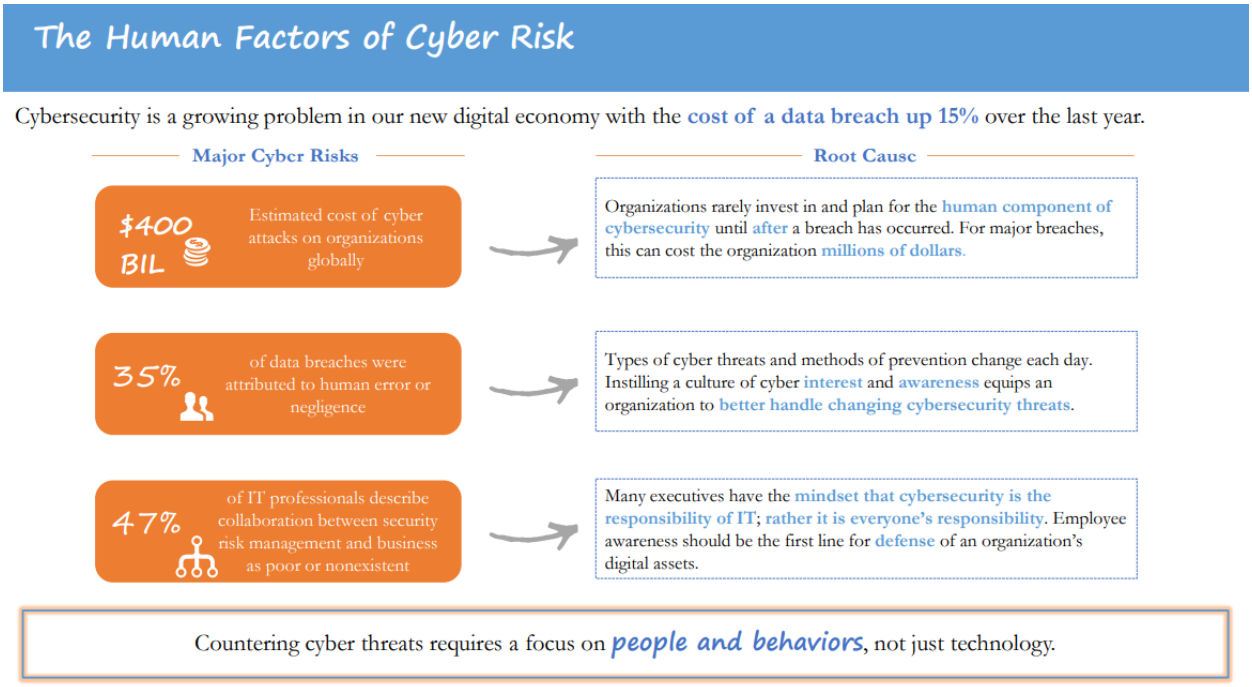
Steve Durbin
Managing Director, ISF

And, of course, you know zero trust doesn't mean that you don't trust. It just means that you make an assumption that something that can go wrong, will go wrong. But, even then, within a people environment that does work well. It doesn't sit well with my view of a trusting culture, a flexible culture, a culture that has a broad mix of generations that's highly diverse, that's agile, that encourages people to question, to challenge. Because that's how you build a thriving business, in my view."

“For me, everything begins and ends with people. Even if you introduce a high degree of artificial intelligence and machine learning into your processes, you will still have to deal with people, in some way, shape, or form. It’s a constant and that’s why I keep coming back to it. Because, we haven’t cracked it. I don’t think we ever will. And, I think we have to keep working at it.”

“If you’re going to have security being recognized as adding value to your business, then you have to move away from a reliance on pure technology to get your message across, so you have to be able to articulate the value that you bring to the business – not just in the boardroom but in every single department that you touch. And, so an understanding of the way people operate, the way that people take on board messages, the way that they like perhaps to be involved, understanding the dynamic of an organization becomes increasingly more important.”

47% of IT professionals describe collaboration between security risk management and business as poor or nonexistent. Many executives have the mindset that cybersecurity is the responsibility of IT; rather it is everyone’s responsibility. Employee awareness should be the first line for defense of an organization’s digital assets. https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.



Karen Heumann

G2M Communications