CEP Magazine - May 2020
Learning to slow down in the Internet of Things era

By Mark Lanterman

Mark Lanterman (mlanterman@compforensics.com) is the Chief Technology Officer of Computer Forensic Services and a professor at the Saint Thomas School of Law in Minneapolis, Minnesota, USA.

Time and again, organizations and individuals alike approach me having been made victim to one of the most commonly deployed, and often incredibly destructive, cyberattacks—the dreaded phishing email. With just a click, a link in an email can produce all kinds of damage. Financial, reputational, legal, operational—the threat of a phishing risk comes with myriad consequences. As a type of social engineering attack in which cybercriminals capitalize on the human element of security, efforts at prevention take on a much more complicated dimension. However, a simple piece of advice may just be the difference between staying secure and falling prey—slow down. In fact, these words may help strengthen every element of an organization's security posture as the Internet of Things (IoT) and unprecedented use of technology infiltrate the status quo.

More convenience brings a higher risk for human error

The IoT is commonly understood as this amazing web of interconnected devices—ranging from complex mechanical systems to our washing machines—that can communicate via a network. The potential range of benefits of this kind of technology is hard to even encapsulate, especially within organizational settings. But, simply put, it makes most tasks easier. From automating processes formerly requiring human input to allowing for instant communication and data gathering, the impact the IoT has had on our lives is beyond significant. With all of the benefits and potential uses—and as the IoT expands and improves and new devices are integrated—organizations are feeling a constant need to take stock of what can be adopted. In other words, organizations are frequently feeling the pressure to speed up, often without fully considering the risks.

When it comes to phishing, cybercriminals tend to do whatever they can to get people to speed up. "You're going to be arrested today if you do not respond to this request for information!" "This is your boss—start the wire transfer immediately!" Often assisted by the process of doxxing (the buying, selling, sharing, or gathering of an individual's personal information online, often with malicious intent), cybercriminals are getting better and better at personalizing their attacks to get your attention and get you to act. Unfortunately, people's personal information is much easier to hack than the security technologies in which organizations often invest. By slowing down, taking the time to follow up in person, typing in an address instead of clicking on a link, and being a cautious and well-informed user in general can be the deciding factor in protecting yourself against a phishing attack. Our approach to the IoT should come with the same admonition.

My cybersecurity mantra—Where we gain convenience, we lose security—may be overused, but it's for a good reason. With every benefit that the IoT presents, it subjects you to an inverse, proportional risk. Bring your own device policies involve an increased, often difficult to fully control, number of points of vulnerability. Automated procedures lead to operational failure in the event of a cyberattack. The larger our use and reliance on the IoT, the greater the risk to our cybersecurity. With this in mind, slowing down becomes just as critical in considering the IoT within our organizations as it is when we are presented with unknown email links.