Executive Summary

As new devices continue to become available on the market, people expect that companies are improving all features, including security. However, as users continually add personal information to every device they own with emails, addresses, shared passwords, and shared accounts, the possibility of a data breach only increases. While companies do work to enhance security measures on devices, user security awareness is stagnant. There are also faults in the architecture of IoT devices that allow hackers to access personal data and a lack of security standards across countries.

User security awareness is arguably the most important aspect when it comes to slowing data breaches. Unsuspecting users are nothing short of a dream to hackers – they click on malicious links, emails, and ads without a second thought; all of which allows hackers to infiltrate data on the device. In response, some companies have begun to develop enhanced cybersecurity training, sometimes requiring their employees to take the training multiple times a year.

Faults in the architecture of IoT devices lie in the different layers that make up the device – the perception layer, network layer, and application layer. These layers all contain issues that are difficult to overcome, such as DoS attacks, man-in-the-middle attacks, tampering, eavesdropping, virus attacks, and many more.

Most countries have their own cybersecurity strategies in place, even though cybersecurity is a global problem. Companies that want to market their products in multiple countries either have to form two separate products with different software builds or attempt to incorporate multiple security policies into one device. If there were global regulation, governments might be in a better position to make the cyber-world more secure.