Educating the Internet of Things (IoT) Users on Cybersecurity Risks

Submitted by Calvin Nobles, PhD

Cybersecurity Policy Fellow at New America Think Tank

The IoT consists of many commonly used devices such as smartphones, wearable devices, kitchen appliances, home security systems, smart cars, military equipment, intelligent devices, and medical apparatuses (Lindqvist & Neumann, 2017). The IoT is interconnected devices with sensors and actuators enabling apparatuses to share information, analytics, and creative application across ubiquitous platforms (Stojkoska, & Trivodaliev, 2017). Researchers and practitioners are forecasting 100 billion interconnected devices and $11T contribution to the global economy by 2025 (Rose, Eldridge, & Chapin, 2015). Concerns deriving from IoT are (a) security risks, (b) privacy implications, and (c) data gathering, (d) lack of governing policies, (Rose, Eldridge, & Chapin, 2015) and (e) no existing platforms to educate IoT users. Rose, Eldridge, and Chapin (2015) accentuate that some IoT devices lack adequate security and pose significant risks and vulnerabilities that cyber threat actors can exploit and gain control to conduct malicious activities. The security vulnerabilities associated with IoT devices directly impacts privacy and data as cyber threat actors are prone to exploit these known security weaknesses to gain access to sensitive data (Rose, Eldridge, & Chapin, 2015). Therefore, it is imperative to educate IOT users on the security risks and vulnerabilities stemming from these devices. The lack of educational platforms exacerbates the problem as many IoT users are unaware of the IoT cybersecurity risks and vulnerabilities.

The benefits and use cases of IoT in developing and less developing countries are endless (Rose, Eldridge, & Chapin, 2015); however, the lack of policies and educational resources need to rise to the forefront of IoT discourse. According to the U.S. Government Accountability Office, no federal institution in the U.S. regulates IoT (U.S. GAO, 2017). The proliferation of IoT by personal and industrial uses require users to become educated in which public and private organizations can partner to provide educational courses on risks, vulnerabilities, and threats of the IoT. Through informative, educational programs, users can take proactive actions to prevent devices from becoming bots during a major cyber-attack. Failure to educate users on how cyber threat actors exploit internet-enabled devices and to gain access to sensitive personal data or use the devices to conduct cyber-attacks perpetuates the on-going cybersecurity threats to IoT.

This presentation is the result of research and critical analysis of the IoT and the lack of consumer education on cybersecurity threats, risks, and vulnerabilities associated with common Internet-connected devices and appliances. The presentation will provide recommendations for educating consumers on IoT, governing policies, and regulatory actions to improve the security of IoT devices. The attendees will leave with a questioning attitude and desire to resolve IoT weaknesses and risks. The practical takeaways are:

a. The need for federal policy identifying a lead IoT agency

b. Educational programs on IoT and cybersecurity risks

c. The need to advocate for IoT devices with better security

d. When and when not to trust IoT devices

References

Lindqvist, U., & Neumann, P. G. (2017). The future of the Internet of Things. *Communications of the ACM*, *60*(2), 26-30.

Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The Internet Society (ISOC)*, 1-50.

Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, *140*, 1454-1464.

United States Government Accountability Office, (May 2017) Center for Science, Technology, and Engineering Report to Congressional Requesters, GAO-17-75, TECHNOLOGY ASSESSMENT Internet of Things Status and implications of an increasingly connected world. http://www.gao.gov/assets/690/684590.pdf