Internet of Things (IoT) Security Policy Platform

14 November 2019

It is the view of the IoT Security Policy Platform that the Internet of Things (IoT) carries significant potential to change our world for the better. Projections for the impact of IoT on the Internet and the global economy are impressive, forecasting explosive growth in the number of IoT devices and their use in a wide variety of new and exciting applications. The following statement is directed to all the governments, citizens and organisations with an interest in realising this potential of IoT.

With billions of IoT devices, applications and services already in use, and greater numbers coming online, IoT security is of utmost importance. Many of these devices lack basic security features, and vulnerabilities or compromised devices can be forced to serve as entry points for cyber attacks, jeopardising sensitive data and threatening the safety of individual users. These are risks that users and businesses adopting IoT must contend with.

Significant work is already underway to address risks and identify the opportunities of IoT as enhancing security will enable consumers to realise the benefits of IoT. Given the Internet's global reach and impact, it is important to join efforts to improve IoT security.

To date, our governmental agencies and organisations have created or are in the process of developing strong IoT security frameworks through intense research, collaboration, and multi-stakeholder fora. The members of he IoT Security Policy Platform, are raising the bar for IoT security practices in their respective fields. Our goal is to enhance the security of the global IoT ecosystem.

Though these frameworks are not exactly alike, each attempts to meaningfully increase security through the lens of its own regional and national context. These frameworks target various applications (consumer, industrial, etc.) and parts of the IoT ecosystem (networks, devices, etc.), as well as explore different approaches to action recommendations and best practices. And yet, these frameworks hold certain principles in common, including:

- Ensure that security is incorporated in all stages of the design, development, and life-cycle, including risk assessments, security testing and evaluation;
- Ensure that personal and critical data is protected; and
- Make it easy for users to delete personal data.

These principles can be achieved through a variety of means, including:

- Implement a vulnerability disclosure policy;
- Make it clear to consumers what the minimum length of time for which a device will receive software security updates;
- Provide mechanisms to securely update software;
- Manufacturers build devices with unique passwords or credentials;
- Protect the communication of security-sensitive data [such as, via encrypted data streams]; and
- Securely store credentials and security-sensitive data.

But these frameworks are only a first step. The IoT Security Policy Platform, with its members, are working together to address the challenges that are faced globally, particularly fragmentation, as part of efforts to create international alignment on IoT security.

Moving forward, the Platform with its members should all continue to work together to harmonize and develop these frameworks when needed to ensure they keep pace with a constantly evolving technological world to enhance trust and raise awareness of security safeguards associated with IoT devices.