Rethinking the cybersecurity of consumer Internet of Things (IoT): how to incentivise companies to produce cyber-secure consumer IoT products

Joo Ng

Technical Report

RHUL–ISG–2019–2

27 March 2019

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

EXECUTIVE SUMMARY

The current widespread use of poorly secured consumer IoT products has been causing menace to the overall security of the Internet (or cybersecurity). This project contributes to the exploration for an alternative and more plausible solution by rethinking the problem from a different and more fundamental perspective. This project report investigates and analyses how innate psychological factors influence consumers' thinking process when making judgement about the cybersecurity risk of IoT, and how this perception eventually leads to economic externalities that cause market failures in the provision of cybersecurity. The insights gained are then applied to formulate a plausible solution model that would incentivise enterprises to design and make consumer IoT products that are more cyber-secure.

Based on these insights, I advocate and recommend a self-regulatory model that incorporates supervision from national governments to ensure robust governance and strict compliance. The model incorporates mandatory and universal adherence to well-founded baseline cybersecurity principles for IoT products traded in the global consumer market. It entails imposing mandatory cybersecurity certification on all IoT products traded in the global consumer market. A global framework for internationally recognised certifications and cybersecurity markings that are based on international standards would provide information transparency about the security quality of IoT products. This would reduce information asymmetry about the cybersecurity of IoT products in the market and enhance consumer trust. This approach would also provide a level playing field for competition and eliminate the economic reason for free-riding in the first place.

The proposed model should also include a more global, standardised, and integrated eco-system for the responsible disclosure and sharing of vulnerability information, and for promptly repairing known IoT defects. The timely availability of accurate, consistent, and relevant information to decision makers in the global market is necessary to fundamentally address the problem regarding inadequate public information about cybersecurity vulnerabilities and incidents. The improved quality and availability of cybersecurity information enables more accurate management and allocation of security risk, as well as better decision-making and policy-making.