Atlantic Council

Security in the Billions:

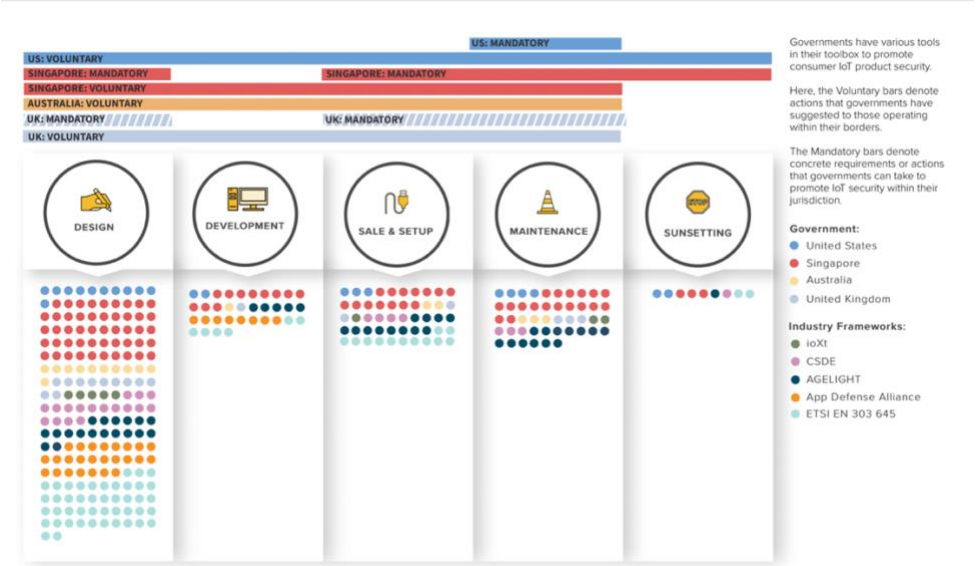
Toward a Multinational Strategy to Better Secure the IoT Ecosystem

By Patrick Mitchell, Liv Rowley, and Justin Sherman with Nima Agah, Gabrielle Young, and Tianjiu Zuo

From business efficiencies to personal convenience, the physical world's growing connection to an internet-enabled digital layer promises many benefits. But fully realizing the potential of the internet-of-things (IoT) requires addressing its worst failing: widespread insecurity. Among other consequences, insecure smart products have been used to spy on unwitting consumers, hijacked to form botnets that deliver paralyzing denial-of-service attacks on internet infrastructure, and provided the initial entry point to compromise corporate and government networks.

In the consumer IoT segment, the problem is particularly acute. Companies routinely design and develop IoT products with poor cybersecurity practices, including universal default passwords, weak encryption, limited security update mechanisms, and minimal data security processes on devices themselves. Buyers often deploy these products without adequately understanding the risk they are assuming. These deficiencies—rooted not merely in technology but, more so, in economic incentives—means that policy intervention is merited. Yet as governments begin to take more forceful action, there is another potential pitfall: fragmented regulatory approaches that add unnecessary cost and confusion while failing to deliver greater security.

In this report, the Atlantic Council offers a multinational strategy to enhance the security of the IoT ecosystem. It provides a framework for a clearer understanding of the IoT security landscape, mapping the guidelines promoted by various governments, standards development organizations, industry groups, and consumer advocates across the entire product lifecycle. It highlights four case studies—Australia, Singapore, the United Kingdom, and the United States—that we believe are well-positioned to make an outsize impact through their coordinated action.



For more on this project, find us on the web:
https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/

The framework's first goal is to reduce fragmentation between policy approaches by highlighting their contributions and limitations. Second, it aims to better situate technical and process guidance into cybersecurity policy. The framework highlights that the IoT security approaches in the countries studied focus on the design, development, sale, and setup phases of the IoT lifecycle, with significant gaps in security actions and policies for the maintenance and sunsetting phases of an IoT product's lifespan.

Next, the report describes a multi-tier system that aims to (1) rid the world of IoT's most glaring vulnerabilities and (2) harmonize international efforts to make it easier for firms to manufacture and sell products with even stronger security features. This multi-tiered scheme would ensure that minimum security standards are met, give consumers easily digestible ways of understanding the security of a product, and allow manufacturers that invest in higher security to advertise it understandably. To this end, we recommend that governments:

1) Implement regulatory measures to **enforce a mandatory security baseline on manufacturers selling in their markets**, as the UK's Product Safety and Telecommunications Infrastructure bill proposes.
2) Follow the "reversing the cascade" philosophy and **put pressure on domestic suppliers and retailers to prioritize selling devices that meet a minimum security baseline**—who may, in turn, put their own pressure on manufacturers.
3) Support the creation of a **voluntary, higher tier of security requirements, indicated via labeling programs** in their markets, like Singapore's Cybersecurity Labelling Scheme and programs currently being explored by DHA in Australia and NIST in the United States.
4) Use government purchasing power to support IoT products conforming to this higher tier by **setting more stringent security requirements for products used by public sector agencies**, as demonstrated by the US's IoT Cybersecurity Improvement Act of 2020.
5) In the short term, reach agreements to **mutually recognize each other's cybersecurity labels** to ease the burden on firms applying for certification, like the pact that Singapore and Finland recently signed.
6) Over the longer term, **compare results** of national labeling programs and move towards a **single global model for communicating security characteristics** of an IoT product.
7) Pursue **outcomes-based approaches to consumer IoT security** rooted in agreed-upon basic security principles and maintain similar definitions of products considered in-scope.
8) Collaborate with industry to regularly **review and update their tiers of security outcomes**.
9) Develop additional **guidance around the "sunsetting" phase** of the IoT product lifecycle.

The report concludes with country-specific implementation plans to operationalize these recommendations and push towards a stronger, more cohesive multinational approach. Despite the perennially crowded global to-do list, reducing the threats from insecure consumer IoT products is overdue, attainable, and worthy of our attention. As more and more objects in the physical world become susceptible to the threats that have long plagued the digital world, we need processes, norms, and global standards that are fit for this new reality.

For more on this project, find us on the web:
https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/