Atlantic Council

Security in the Billions

Toward a Multinational Strategy to Better Secure the IoT Ecosystem

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

Implementation for the United Kingdom

The purpose of this is to demonstrate how the United Kingdom should act to help develop a multinational strategy to better secure the IoT ecosystem.

Tier 1. Set the Baseline of Minimally Acceptable Security:

Of the four countries examined in this report, the UK is closest to creating a mandatory baseline for a broad range of IoT products sold in its market. The PSTI Bill will set minimum security requirements for manufacturers and couple them with potent enforcement mechanisms. By empowering the DCMS secretary to set these guidelines, this baseline can keep pace with technological change without the need to constantly rewrite legislation. The UK government should take the following actions:

- **Pass the legislation**. The most obvious and immediate next step is for parliament to enact the PSTI Bill. Thus far, the proposed law has made its way through the legislative process with its core provisions intact. While it does not address everything on the wish list of security advocates, it is an ambitious effort that lawmakers should approve. The House of Lords has recommended a sensible amendment that will also protect security researchers conducting legitimate vulnerability research from intimidation and lawsuits by manufacturers.[1] Given that the countdown for firms to comply with the new law begins one year after the bill receives Royal Assent consideration of further amendments should take into account the additional time they will add to the process.
- **Identify a regulator**. While the DCMS will define the cybersecurity provisions that manufacturers must abide by, it will not be the agency that enforces them. At the time of publication, the UK government had not publicly named the regulator responsible for enforcing the baseline product requirements. In its 2021 consultation, the DCMS sought recommendations on agencies well-positioned to serve in this role. Multiple respondents highlighted Trading Standards and Ofcom, the UK's communications regulator.[2] The DCMS has also consulted with the Office for Product Safety and Standards in the Department for Business, Energy, and Industrial Strategy, another consumer product safety

[1] Alex Scroxton, "Lords Move to Protect Cyber Researchers from Prosecution, *Computer Weekly*, June 2022, https://www.computerweekly.com/news/252521716/Lords-move-to-protect-cyber-researchers-from-prosecution.
[2] "Government Response to the Regulatory Proposals for Consumer Internet of Things (IoT) Security Consultation." United Kingdom Department for Digital, Culture, Media & Sport (DCMS), February 2020, https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation.

regulator.[3] This report does not have a specific recommendation as to the best-positioned agency to assume this role, but the government should announce this decision and begin to build out the key elements of its enforcement capacity.

Tier 2. Incentivize Above the Baseline:

Unlike the other three countries profiled in this report, the UK government has for now explicitly rejected the approach of device labeling, choosing to initially focus the bulk of its efforts on setting the first tier of a mandatory baseline. Despite the challenges with cybersecurity labels, the team views them as the best option for encouraging manufacturers to invest in greater security as well as providing consumers with accessible information. In partnership with NCSC, the DCMS should:

- **Provide "forward guidance" on provisions that it aims to mandate next**. Like a good central bank, the DCMS should provide predictability in its intended future actions while remaining flexible to change in the face of new information. While the UK plans to begin with the so-called "top three" measures in its initial list of mandatory requirements, one of the key design principles of its approach is the ability to gradually ratchet up the baseline with new provisions. Through public announcements and meetings with industry, DCMS can telegraph where regulation is headed and allow security-minded firms to bring their products into compliance before the measures become mandatory. For starters, the DCMS should look to the World Economic Forum (WEF) statement that highlights two additional ETSI principles as the logical next steps: ensure that products communicate securely and safeguard personal data.[4] Other impactful measures could include a guideline requiring manufacturers to provide security updates for a minimum period consistent with the average length of time consumers use a product, which can vary by product category. The DCMS could go even further by publishing the planned effective dates of new security requirements years in advance. These provisions can change as cybersecurity threats and commercial considerations change.
- **Study the impact of cybersecurity labels in other markets and be prepared to reevaluate if they achieve results**. Thus far, research on cybersecurity labeling for smart devices remains largely limited to surveys about consumers' hypothetical willingness to pay more for products that have an indicator of greater security. Now that several countries have introduced labeling programs, users should begin to see "real world" data on their performance, both as it relates to changing consumer behavior and in addressing the downstream ills of insecure devices. If it becomes apparent that one or more of these labeling approaches are achieving success—or gaining traction as an international standard—the UK government should remain open to adopting it in its market.

---

[3] "Proposals for Regulating Consumer Smart Product Cyber Security – Call for Views," United Kingdom Department for Digital, Culture, Media & Sport (DCMS), October 2020, https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views.

[4] "IoT security: How We Are Keeping Consumers Safe from Cyber Threats," World Economic Forum, February 2022, https://www.weforum.org/impact/iot-security-keeping-consumers-safe/.