ITI Promoting Innovation Worldwide

IoT Security Policy Principles

The growth of network-connected devices, systems, and services comprising the Internet of Things (IoT) creates immense opportunities and benefits for our society. To reap the benefits of connected devices and to minimize the potentially significant risks posed by malicious actors seeking to exploit them, these devices need to be secure and resilient. Unfortunately, as the number of connected people, businesses, and devices grows, so does the potential for malicious attacks. Today, the destructive potential of cyber attacks can increase exponentially when such attacks leverage massive quantities of connected IoT devices.

As risks to the global digital ecosystem, including IoT, continue to grow, so does our need to restore trust and confidence in connected devices and the IoT and larger ecosystems to advance not only security but economic growth and innovation. To help policymakers and stakeholders better ensure the security of the IoT ecosystem, ITI recommends using the following policy principles as a guide.

1. Focus Beyond the Device

It is imperative that all stakeholders collaborate to take a thoughtful, holistic approach to securing the various parts of networks and complex ecosystems that make up the IoT. An inclusive process must focus on end-to-end security, including security-by-design techniques and secure development lifecycles.
As global concerns regarding IoT security — including concerns about sophisticated automated and distributed threats such as botnets that exploit insecure IoT devices — have continued to grow, policymakers have disproportionately focused on IoT product security without addressing the broader issues related to securing the IoT ecosystem. Many policy proposals have narrowly focused on individual components of the ecosystem, rather than focusing on ecosystem security as a whole**.** For instance, some policies propose that internet service providers (ISPs) should simply shut down all botnets, or that manufacturers of billions of devices should make them universally secure. Such overly simplistic solutions fail to address the fundamental need to secure the ecosystem. Regardless of which security measures are taken at the device, network, or software level, if these components of the ecosystem are addressed in isolation, efforts will ultimately fail. Taking a holistic view is therefore a superior approach.

2. Lead With Industry-Driven Core Baselines and Standards

While ecosystem-wide security is important, there is a need to develop a consensus around baseline security capabilities for IoT devices. Developing a common set of best practices and secure capabilities that are broadly applicable across all IoT devices with varying levels of complexity and are driven by market demand will help to improve all new IoT devices' cybersecurity.

Building broad industry consensus around an IoT security baseline will also facilitate more effective government-industry collaboration on this issue, helping to drive interoperable IoT security policies worldwide. In addition, establishing a core baseline will promote globally interoperable standards and advance innovation worldwide to improve IoT security. Governments should continue to encourage open and international security standards to maintain the long-term viability of the IoT and to foster solutions that are interoperable and reusable across a variety of use case deployments, vendors, sectors, and geographies.

Noteworthy multistakeholder efforts to develop core IoT baselines include the Core Device Cybersecurity Capability Baseline in Draft (2nd) NISTIR 8259, Recommendations for IoT Device Maufacturers, which incorporates references to multiple international IoT security standards, and the industry-driven C2 Consensus on IoT Security Capabilities. Driving global alignment around a core IoT security baseline effort that garners significant consensus can serve as a critical tool to advance global IoT security.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

3. Avoid Regulatory Fragmentation and Duplication

To fully realize the benefits offered by IoT, governments should promote policies that help break down barriers to connecting devices and correlating data while protecting privacy and security. Government bodies should examine the technologies underlying the IoT and assess where current authority, oversight, and regulation already exist and avoid siloed, sector-specific regulatory approaches.

Policymakers and regulators should reinforce private-public cooperation on IoT issues to help identify cybersecurity solutions and better coordinate the many IoT security-related policy efforts currently in progress across the U.S. government and globally. In the United States, the National Institute of Science and Technology's (NIST) ongoing commitment to industry outreach in developing an IoT security framework provides an excellent example of such cooperation.

The viability of security labels as effective and efficient tools for consumers requires further discussion, particularly since there is currently no consensus amongst policymakers and industry stakeholders regarding the benefits and drawbacks of such a scheme. For example, providing consumers with clear information about critical security features in IoT devices may foster market competition based on security, build trust in the security of IoT products, and help consumers fulfill their role in maintaining security. However, such a scheme may communicate a false sense of security and if made mandatory, would only serve to further fragment markets and raise the cost of compliance. Policymakers should proceed carefully on this front, ensuring that any contemplated scheme is voluntary and carefully considered.

4. Promote Global Harmonization

Mandatory IoT requirements published by individual states or municipalities, sector-specific agencies, or countries will unhelpfully fragment the global IoT security landscape. Such fragmentation may ultimately limit the growth of a secure IoT by reducing the efficiencies of scale in development, manufacturing, support, training, assessment, and identification of secure IoT products. It will also make it more difficult for industry to comply with such divergent requirements, hampering global business and trade.

The long-term security and resilience of the internet and communications ecosystem requires a global and holistic approach involving the adoption of baseline security practices by stakeholders in many different countries, industries, and segments of the ecosystem. To combat an increasingly divergent policy environment, policymakers should prioritize global harmonization and regulatory cooperation to support a voluntary, industry-driven consensus around core baseline capabilities for IoT security that are grounded in global standards.

Finally, stakeholders must understand that connecting IoT devices or equipment to the Internet is a long-term commitment, not a one-time design and manufacturing cost. IoT security demands dynamic, flexible market-driven solutions that are nimble and adaptable to evolving cyber threats, including those specific to the proliferation of IoT devices, rather than regulatory compliance mechanisms that differ by local or national jurisdiction.