Cybersecurity policy for the Internet of Things

Microsoft Policy Papers

The security challenges of the Fourth Industrial Revolution

Around the world, organizations and individuals are experiencing a fundamental shift in their relationship with technology. This transformation, often called the Fourth Industrial Revolution, has been characterized as a fusion of the physical, digital and biological worlds, with far-reaching implications for economies and industries, and even humankind. The Internet of Things (IoT)[1] is a key element of this global digital transformation.

It is not just the sheer number of IoT devices that will have an impact, but how they connect the physical and cyberworlds. IoT breaks the confines of traditional computer networks, as it allows for "things" to connect to the Internet, ranging from the significant - airplanes, elevators, solar panels, medical equipment - to the mundane - toys, soap dispensers, and porch lights.

To the extent that IoT is an extension of current platforms and networks, many of the same risks to the confidentiality, integrity, and availability of data still apply. However, many connected devices will be deployed into environments with older legacy systems that cannot be easily managed and updated, or they may fall under multiple regulatory jurisdictions with different requirements, or into consumer environments with fewer resources for significant security management.

Moreover, given the broad applicability of IoT technologies across relatively different types of communities, the cybersecurity concerns of IoT users will also differ. However, it is nevertheless important to understand them to make sense of IoT security issues and enable the development of more responsive technological and policy approaches. Microsoft therefore recommends looking at IoT security through the lenses of three core groups of users – consumers, enterprises and governments. We believe this approach will result in better security solutions, guidelines and requirements overall.

These challenges provide ample reason to bring governments and the technology industry together to increase the security of IoT networks and devices generally, and to ensure an adequate security baseline that addresses all IoT elements. It is clear to us that dialogue is the most important ingredient for meaningful progress in IoT cybersecurity policy. Policymakers have significant opportunities to create spaces where challenges can be explored and solutions identified, whether through public consultations led by governments or non-governmental organizations, collaboration across stakeholders towards common frameworks or standardized approaches, or other forums.

What is IoT?

There is no universally agreed-on definition of IoT, perhaps in part because the term IoT does not simply describe a new type of technical architecture, but a new concept that defines how we interact with the physical world.

The US National Security and Telecommunications Advisory Committee (NSTAC) has defined IoT based on three shared common principles:

Devices: Devices within a network are instrumented so they can be addressed individually.

Platforms: Devices are interconnected by way of a shared platform, such as a cloud service.

Intelligence: Devices may perform functions adaptively, on their own or with other devices and applications, based on programming and inputs from the physical world.

At the same time, it is important to remember that the relevant stakeholders, implications of potential policies, and indeed, the relevant technologies themselves are still evolving. Policymakers must therefore take a long-range view of problems and solutions, while moving with agility in the face of a changing landscape.

[1] IoT definition: The President's National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the Internet of Things, Nov. 19, 2014, Appendix E, https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf

Government role in securing the IoT environment

The changes introduced by IoT create both new opportunities and challenges for policymakers, as traditional governance frameworks and models have to be reconsidered for a different world. As stewards of societal well-being and the public interest, governments have a special role to play in delivering the vision of a secure IoT and supporting its development. They also have unique capabilities to convene stakeholders to address shared challenges, promote best practices through guidance, and intervene as regulators. In particular, they can:

- Raise awareness of best security practices and guidelines: Not every business has the knowledge and expertise to make smart decisions about security when developing and deploying IoT devices and services. Governments can enable better security outcomes by promoting best practices that range from security by-design principles to sector-specific product development and risk assessment guides.
- Develop enhanced guidance for safety critical sectors: Greater investments in cybersecurity and system resilience apply in particular to devices that support human life, critical infrastructure, and other essential functions, whose inability to function and lack of resilience could have dire consequences.
- Invest in IoT security training, education, and raise public awareness: Government investments in workforce development and awareness-raising campaigns can help increase the scale and impact of industry-led efforts.
- Encourage collaboration between the public and private sector: IoT policy issues are often driven by IoT's unprecedented scale, which can impact a diverse range of stakeholder groups in new ways. For example, realtors may face new challenges in marketing and selling a smart home if its connected elements cannot easily be transferred over to a new owner. Including a broadly representative group of stakeholders can be useful in developing, updating, and maintaining IoT security guidance.
- Create an inter-ministerial task force to coordinate security efforts: The impact of breakdowns in cybersecurity cuts across organizational boundaries, so creating an interagency or inter-ministerial IoT task force can balance perspectives on security and risk management. Such a task force could develop policies and coordination efforts that address these cross-organization security issues.
- Promote the development of secure, open, consensus-based standards: As new IoT technologies develop, there will be an increasing need to ensure interoperability between new IoT systems and legacy technology systems. While some Internet protocols can be adopted from existing standards, IoT has specific security requirements that must be addressed separately. Governments can encourage the development of open, voluntary, consensus-based, and globally relevant standards that foster greater interoperability.
- Harmonize approaches to IoT security across national borders: Manufacturers of IoT devices want to market their devices worldwide, no matter where the underlying code was developed or the devices were manufactured. Governments are in a position to reduce the possible costs for small and medium-size IoT manufacturers to meet IoT security requirements by harmonizing them across countries.

Looking forward, IoT cybersecurity policy will only increase in importance as the world grows more connected and reliant on the efficiencies and opportunities that IoT brings. IoT users and policymakers will face new IoT use cases, including situations where users may not even be aware that they are interacting with a connected device, which will prompt new questions about how to manage security needs alongside opportunities for innovation.

Microsoft looks forward to supporting the growth of a secure IoT ecosystem through advancements in technology and policy, in partnership with stakeholders from across the public and private sectors.