Strong Cybersecurity Protections Support a Safe and Secure Product Infrastructure

Cybersecurity risks presented by Internet-capable devices require a strong regulatory framework to protect consumers which includes third-party conformity assessment, certification, and labeling. The third-party conformity assessment industry has the necessary capabilities and consumer trust to serve in this role.

The market for consumer products capable of connecting to the internet (e.g., IoT devices) is growing exponentially, thanks in part to innovation and the unique ability of these devices to address consumer needs. As reported in the TIC Council Value of TIC Study[1], the size of the global IoT consumer market is expected to grow from $53bn in 2019 to an estimated $188bn in 2027.

Consumer products with internet capable functionality present unique hurdles for consumers who may not have the technical understanding or access to expertise to protect their homes and loved ones from cyber criminals.

The independent third-party TIC sector, representing testing, inspection, certification, and other conformity assessment activities, can play a unique role in evaluating and confirming that internet capable devices meet requirements for cyber security and that the manufacturers that produce them have implemented appropriate mitigation strategies[2] to address these risks.

The third-party TIC sector has established cybersecurity assessment, certification, and labeling programs which to date are offering consumers the information needed to support their buying decisions and understand the cybersecurity requirements of products. A regulatory framework which supports the continued growth of these programs, including the mandatory use of third-party TIC industry marks is critical.

Manufacturers and Suppliers – In April 2021, the U.S. Government learned that hackers had breached multiple U.S. Federal agencies through a vulnerability in a widely used remote access product called Pulse Connect Secure[3]. The hacking group exploited vulnerabilities in Pulse Connect Secure products allowing hackers to bypass passwords and multifactor authentication to access agencies' data.

A similar breach to a manufacturer or supplier system without the necessary safeguarding, would jeopardize the security and safety of all consumer products within that infrastructure. The use of Independent third-party conformity assessment to confirm that appropriate testing, risk-evaluation, and mitigation strategies are deployed, providing regulators and consumers with needed confidence that such hacks could be prevented or mitigated.

Product Development – Products with IoT functionality benefit from risked-based evaluation and testing, supporting a security-first development process to address risks created by the introduction of internet capabilities. Ensuring

[1] "Value of the Testing, Inspection and Certification Sector," Final Report, December 2020. Contact americas@tic-council.org to receive a copy on the date of publication.

[2] The Internet of Things (IoT) and Consumer Product Hazards, IFIA's recommended guidelines for ensuring the safety of connected devices, https://www.tic-council.org/application/files/5015/5679/7564/IFIA_Recommended_Guidelines_IoT_2018.08.23_RO.pdf

[3] "Federal Cybersecurity: America's Data Still at Risk" Staff report, Committee on Homeland Security and Government Affairs, United States Senate, Page 3.

security passwords can be set on devices, that products include necessary labeling and consumer instructions,[4,5] and other steps can reduce the likelihood of intrusions and are a commonsense safety measure. Independent third-party TIC organizations are uniquely skilled to support manufacturers during the design process and also to evaluate end products to ensure key performance functions, such as the setting of passwords and partitioning of devices on networks, are available to consumers.

Product Lifecycle – Software updates to IoT capable devices have the capability of compromising compliance with applicable rules and standards, and introducing unknown hazards to consumers. Consumers may be unprepared to evaluate and address security issues produced by such updates. Third-party TIC organizations can support consumers (and secondary consumers) by evaluating product updates and products after update to confirm that products continue to comply with requirements for secure performance.

Why Independent third-party conformity assessment?

There are one million TIC employees (often in high-wage STEM jobs) scattered in more than 160 countries around the globe offering conformity assessment services.[6] The TIC industry supports manufacturers with a highly skilled workforce and capabilities that manufacturers may not have the capital and resources to maintain in-house.

Third-party TIC providers are highly trained in thousands of standards, rules, and regulations and in their application to a wide range of products. This makes them uniquely qualified to evaluate immerging and innovative products not yet encountered on the market.

Independent third-party TIC organizations, by their nature as independent and impartial evaluators, can provide consumers with a level of confidence in products that would not be achieved to the same extent by conformity assessment services performed by first parties.

Independent third-party TIC organizations, such as those represented by the TIC Council, accredited to international standards such as ISO/IEC 17025 for testing and ISO/IEC 17065 for certification, provide an extra layer of confidence for consumers and regulators that TIC competencies and capabilities have been evaluated by an independent external body.

Incorporating the use of independent third-party TIC organizations into cybersecurity programs for internet capable devices is the cost-effective strategy to support consumer confidence and to protect the safety and security of consumers.

Contact person: Karin Athanas (kathanas@tic-council.org)

TIC Council is a global association representing over 90 international independent third-party testing, inspection, certification and verification organizations. The industry represents an estimated one million employees across the world with annual sales of approximately USD 200 billion

[4] Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/cybersecurity-labeling-consumers-internet-things

[5] Improving the Nation's Cybersecurity, Executive Oder 14028, https://www.federalregister.gov/d/2021-10460

[6] "Value of the Testing, Inspection and Certification Sector," Final Report, December 2020. Contact americas@tic-council.org to receive a copy on the date of publication.