TIC Council Recommendations for a Robust Cybersecurity Framework in India

Introduction

It is evident that digital technologies are becoming an integral part of the society with applications ranging from Industry 4.0, smart cities, smart homes, connected vehicles, agriculture to healthcare .

Therefore, a strong cybersecurity system supports national security, builds trust in digital transactions, protects sensitive data, and promotes economic growth, allowing India to pursue its goal of becoming a developed country.

This paper provides recommendations to further strengthen the cybersecurity ecosystem in India and discusses how the Testing, Inspection and Certification (TIC) sector can play a pivotol role to support the stakeholders to achieve the desired objective. You may find our recommendations in short here:

Recommendations

a) **Adopt a risk-based approach to conformity assessment:** Cybersecurity policies should leverage a risk-based approach which emphasize the identification and prioritization of the most critical cybersecurity risks, followed by the application of controls to mitigate them. A risk-based approach to select the conformity assessment procedure for each type of device category would consider the device's intended use, foreseeable conditions of use, vulnerability and would apply specific security requirements, including tested methodologies for all assurance levels. Also with the continously evolving technologies, alongwith risk-based approach, the key focus should also be on "thinking out-of-box", and "evaluation of latest technology solving special attacks". In this context, involving third parties having relevant expertise and experence in the conformity assessment for cybersecurity of devices should become critical.

b) **Inclusive engagements for developing policies and regulation around cybersecurity:** In this highly connected environment that includes, consumers, critical infrastructure operators, industry and service providers, any regulatory efforts should include all relevant stakeholders and take into consideration current programmes. The TIC sector should be included in these stakeholder discussions, since it plays a critical role in helping ensure products' compliance with cybersecurity requirements and other rules.

c) **Ensure a global holistic approach for cybersecurity requirements:** In view of the global pervasiveness of digitalisation across industry sectors, it is important to establish a common framework protecting all users which would increase awareness and promote the use of harmonised global standards. The regulatory framework should make use of internationally established risk classification systems and standards which offer a common global approach to security requirements for products. Globally harmonised standards and regulatory frameworks (i.e. conformity assessment) minimise regulatory barriers, facilitate trade across borders, and reduce the cost of implementing regulations for governments and industry. Global TIC organisations having global expertise in the cybsecurity domain can back the authorities in establishing the desired specifications and requirements for a robust cybersecurity framework.

d) **Leverage private third-party TIC players:** Incorporating independent third-party TIC organizations into cybersecurity programmes enables speed to market, gives choice to manufacturers, requires less direct oversight by the regulatory authorities, and results in the desired levels of consumer safety and security.

TIC Council India
UL Quality Assurance Private Ltd, Plot No. 12, Block A, Infocity, Sector 33 and 34,
Gurgaon, Haryana, India
+91-9811606820 | india@tic-council.org

e) **Adoption of security-by-design principles:** It is important to implement security-by-design principle during the design phase of the product devlopment cycle itself. Security-by-design and security-by-default shall be fundamental priciple for all the product development processes. Adoping these principles significantly lowers the number of exploitable flaws in products before such products are introduced to the market for public use and consumption.

f) **Foster cybersecurity culture:** As the country embraces the new technologies and innovation, it is essential to prioritise the cybersecurity and resilence of our digital infrastructure. By prioritising cybersecurity awareness, fostering collaborations, developing a robust cybersecurity infrastructure as well as a skilled cybersecurity workforce, countries can confidently navigate the digital landscape while ensuring the security and privacy of citizens and critical assets. Private TIC organisations with relevant expertise can play a critical role by guiding the relevant stakeholders including government authorities to foster a cybersecurity culture in the country.

TIC Council India
UL Quality Assurance Private Ltd, Plot No. 12, Block A, Infocity, Sector 33 and 34,
Gurgaon, Haryana, India
+91-9811606820 | india@tic-council.org

ANNEX: Importance of a Robust Regulatory Framework for Cybersecurity

Cybersecurity is the application of technologies, processes and controls to defend computer systems, servers, networks, electronic systems, programs, devices and data from malicious cyberattacks. It aims to mitigate the risks of cyberattacks and protect against the unauthorised exploitation of systems, networks, and technologies by cybercriminals who intend to gain unauthorised access to these systems and are constantly looking for new ways to exploit individuals, organisations and even governments.

It is absolutely vital thattechnology utilised in critical operations be protected and safeguarded. Any cyberattack on critical infrastructure (eg. power grids, telecom networks, banking and healthcare systems) can bring the entire system to a halt and lead to crippled communications, huge financial and data loss and even endanger the health and safety of citizens.

Geopolitical instabilities as well as more frequent cyberattacks, in terms of means and scale, requires countries to reconsider their international strategies and include cybersecurity or else cyberattacks may bring catastrophic consequences to vital sectors.

In this regard, India has also witnessed numerous incidents of cyberattacks in last few years, wherein some cases power grids and critical infrastructure have been targeted. Over 1.3 million cyberattacks were reported across India in 2022. This was a significant increase as compared to 2019. The country was among the top five in the world with the highest number of cybersecurity incidents that year[1].

One example of a major cyberattack in India was in November 2022, when India's premier medical institute, All India Institue of Medical Sciences (AIIMS) faced a major cyberattack and its server went out of order, which caused major disruptions to its sevices. On another instance, in February 2021, hackers broke into Air India's database to steal the personal information of 4.5 million Air India customers.[2]

Nevertheless, a majority of the products being built only address operational performance, price and time-to-market objectives[3].

Therefore, we recommend that devices are built according to pricincples deveoped and shared by the cyberommunity. For instance, the principle of "security by design", is a critical element for having a proactive approach on identifying all necessary security contingencies from the outset. Integrating them into the entire life cycle would preventively close security gaps and mitigate cyber threats, much more needs to be done.

Secondly, many cybersecurity issues revolve around the lack of harmonised regulatory framework and common cybersecurity standards. Regulations are formulated at a slower pace than the deployment and adoption of connected technologies. This has led to uncertainty in the minds of users as well as providers of these services concerning the operation and security of connected devices. These concerns are rinsing due to increasing fears around data privacy as well as frequent malicious attacks that have been disrupting the critical operations of users, organisations and governments.

A transparent and comprehensive regulatory framework for cybersecurity testing and certification would surely be beneficial to all stakeholders including consumers, industry and authorities alike. The emerging standards landscape as well as the increasing number of security incidents are good indicators that such a framework is critically needed.

[1] https://www.statista.com/
[2] https://etinsights.et-edge.com/top-7-data-breach-incidents-in-india/
[3] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

TIC Council India
UL Quality Assurance Private Ltd, Plot No. 12, Block A, Infocity, Sector 33 and 34,
Gurgaon, Haryana, India
+91-9811606820 | india@tic-council.org

Regulatory Landscape Around Cybersecurity in India

In recent years, the government of India has undertaken several initiatives to build and strengthen a robust cybersecurity framework for the country. In the budget for 2023-24, the Ministry of Electronics and Information Technology (MeitY) has been allocated a sum of USD 75 Million to improve the country's cybersecurity infrastructure.

To promote the culture of cybersecurity in organisations and amongst the public, several cybersecurity initiatives such as Cyber Surakshit Bharat and Cyber Swachhta Kendra etc. have been introduced by the government.

In 2020, the National Cybersecurity Strategy was conceptualized by the Data Security Council of India (DSCI), headed by a National Cybersecurity Coordinator. This strategy aims to ensure a safe, secure, trusted, resilient, and vibrant cyberspace for India. The final strategy as well as implementation timelines are yet to be announced.

In October 2021, the Telecommunication Engineering Centre (TEC) issued the "Code of Practice for Securing Consumer Internet of Things (IoT)" as a baseline requirement, in alignment with global standards and best practices. This document provides baseline requirements in line with the Cybersecurity for Consumer Internet of Things: Baseline Requirements mentioned in ETSI EN 303 645. This is applicable to all stakeholders in the IoT sector including device manufacturer, IoT service providers/system integrators, mobile application developers and retailers, etc. Currently, this Code of Practice is intended for voluntary adoption by the stakeholders only. Furthermore, the Communication Security Certification Scheme (ComSec scheme) has also been announced by National Centre for Communication Security (NCCS). This scheme involves mandatory testing and certification of security parameters as per the Indian Telecom Security Assurance Requirements (ITSAR) defined by NCCS. In the initial phase, only IP Routers and WiFi CPEs have been included under the scope and IoT devices are expected to be covered in upcoming phases.

Also, in August 2023, the Digital Personal Data Protection (DPDP) Act 2023[4] was granted assent by the President of India, transforming it into law. The provisions of this Act apply to the processing of personal data collected within the territory of India as well as the processing of digital personal data outside of India, if the processing is in connection with any activity related to the offering of goods or services to individuals within the territory of India. This Act will function as a proactive defense mechanism in the field of cybercrime and data protection, strengthening organisations' resilience to cyber threats by adopting robust data security practices such as encrypted communications and security breach reporting.

In current context, as there is no mandated policy, standards or governance structure in India, it is imperative to fasten the release of strategy, regulation and procedures pertaining to the cybersecurity controls. It is important to establish testing and security mechanism so that the devices/products can be tested and certified in accordance with globally accepted standards and requirements ensuring safety, security and desired performance of the devices as well as overall connected ecosystem.

Furthermore, as the cybersecurity applications are not limited to a particular industry segment and is adopted by all, it is critical that a conisistent approach be followed by ministries and relevant authorities while formulating the policies and regulations around cybersecurity. A central working group with sub-committees

[4] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

TIC Council India
UL Quality Assurance Private Ltd, Plot No. 12, Block A, Infocity, Sector 33 and 34,
Gurgaon, Haryana, India
+91-9811606820 | india@tic-council.org

can be constituted with participation of ministries, authorities and other stakeholders such as manufactures, testing laboratories, academia etc. from relevant segments.

Role of TIC Sector in Ensuring A Robust Cybersecurity Ecosystem

Governments, manufacturers, standards developers and conformity assessment providers have a role to play in ensuring a robust cybersecurity ecosystem in the country. In particular, the TIC (testing, inspection and certification) sector can, through Independent third-party certification , help meet this need in a reliable and efficient manner.

The TIC sector provides complete testing, inspections and certification services for hardware and software implementation into connected devices and services, malicious code and penetration testing, cybersecurity connectivity, safety and electromagnetic compatibility among other requirements.

Manufacturers often engage TIC companies to provide a comprehensive review of cybersecurity due diligence processes throughout the device lifecycle. The TIC sector therefore contributes to manufacturers' "security-by-design" approach, which means that security is not only part of the final product but an end-to-end approach throughout the entire supply chain, including development, production, delivery, retail, personalization and use right until end-of-life.

Leveraging private third-party TIC players also reduces the burden on the respective regulatory authority pertaining to the cumbersome process of audit and review of technical documents, process, and other related requirements. Private third-party TIC players also enable speed to market, giving choice to manufacturers, requiring less direct oversight by the regulatory authorities, while still resulting in desired levels of consumer safety and security.

Incorporating the use of independent third-party TIC services into cybersecurity programmes especially for connected devices is an effective strategy for ensuring consumer confidence and protecting the safety and security of consumers. Independent assessment by a third-party through product testing, verification and certification, along with cybersecurity rating demonstrates diligence and that the products and the system conforms to defined standards. In addition, this makes product security more transparent and accessible to customers as well as offer confidence and facilitating purchasing decisions. Such cybersecurity security rating also enables manufacturers to gain competitive differentiation.

TIC Council India
UL Quality Assurance Private Ltd, Plot No. 12, Block A, Infocity, Sector 33 and 34,
Gurgaon, Haryana, India
+91-9811606820 | india@tic-council.org

Contact person: *Dr Seema Shukla, Executive Director, TIC Council India*
Address: Block No 12, Plot A, Infocity Sector 33 and 34, Gurgaon, Haryana India.
tel: *99107018003*
email: *india@tic-council.org*
Editor's Note About TIC Council

TIC Council is the global trade federation representing the independent third-party Testing, Inspection and Certification (TIC) industry which brings together about 100-member companies and organizations from around the world to speak with one voice. Its members provide services across a wide range of sectors: consumer products, medical devices, petroleum, mining and metals, food, and agriculture among others. Through provision of these services, TIC Council members assure that not only regulatory requirements are met, but also that reliability, economic value, and sustainability are enhanced. TIC Council's members are present in more than 160 countries and the wider TIC sector currently employs more than 1 million people across the globe.

The Value of TIC Report

To learn more about TIC Council and its member's activities, the landmark report on the Value of the TIC sector, developed jointly by the international law firm Steptoe and the London-based consultancy Europe Economics is now available to read. This report illustrates, by using data and case studies, how the TIC sector benefits a variety of stakeholders and industries around the world. You can find the study here, and we welcome you to share it with anyone who might be interested.