Cybersecurity and Connected Products: Reviewing the Regulatory Landscape

Prepared by:
Rebeka El Hadad, Regulatory Analyst, Compliance & Risks

June 2021

1. Introduction

Global dependence on connected products has led to an immediate need for laws and regulations to protect information on the devices from online theft or manipulation. A few countries have taken bold steps to enact cybersecurity regulations, but most have taken only tentative action.

Industry 4.0 (also known as the fourth industrial revolution) can be defined as utilizing smart technologies and automation to assist with traditional manufacturing. These machines are often interconnected and connected to the internet, which presents an increased security risk, especially as cybercriminals can easily access full networks through vulnerabilities of individual devices.

This white paper will give an overview of cybersecurity regulations and standards around the world, with a focus on the EU, UK, USA, Australia, China, Brazil and South Africa. It will also shed light on some of the most common requirements for manufacturers of connected products.

2. Regulatory Overview

Below is an overview of recent cybersecurity regulations around the world, representing a snapshot of the regulatory landscape and how countries are adapting to the everchanging cyber world. The examples below are in no way exhaustive.

2.1. European Union

The EU launched its cybersecurity certification scheme (EUCC) Version 1.1.1 on 25 May 2021. The scheme will act as a successor to the SOG-IS MRA that is already in place in the field of information systems security and common information technology security evaluation criteria.

The scheme will be implemented by the European Union Agency for Cybersecurity (ENISA) using the Common Criteria ISO/IEC 15408. The European Cybersecurity certification framework will consist of several schemes expected to gradually increase trust in ICT products, services and processes certified under these schemes and reduce the costs within the Digital Single Market.

The EU is currently also reviewing the General Product Safety Directive 2001/95/EC to look at online selling and new technologies. With the increase in implementing AI and smart components in comparison to when it was originally released in 2001, the existing Directive is not able to sufficiently cover the full scope of modern products. The revision is specifically looking into the definition of products, and the new risks of having a product that is open to security threats.

Cybersecurity cannot be mentioned without also mentioning the General Data Protection Regulation (GDPR) of 2016. The concern is the large amount of data collected by connected devices, in addition to the sensitive nature of some types of data (home security cameras, smart assistants and fitness wearables). Therefore, GDPR has given consumers more control over their personal data.

2.2. United Kingdom

The UK government launched a public consultation for connected consumer products regulations in July 2020. In April 2021, the UK Minister for Digital Infrastructure Matt Warman MP published the government's response to the consultation.

The response confirmed plans to introduce new laws that will contain mandatory cybersecurity requirements for connected products. The response also stated that "the regulation will apply to all consumer connected products such as smart speakers, smart televisions, connected doorbells and smartphones. A number of devices will be exempt due to the specific circumstances of how they are constructed and secured, including desktop computers and laptops. The security requirements will align with international standards and are familiar to all manufacturers and other relevant parties across the industry."

2.3. United States

The California State Legislature has issued Bill 327 on the Security of Connected Devices, that is also known as the California IoT Law. This law has been in force since January 2020, and it requires manufacturers of connected devices "to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified."

The US National Institute of Standards and Technology (NIST) has also issued a number of guides and reports, including the NIST Cybersecurity Framework. The framework "is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders."

In May 2020, NIST issued an interesting document that is addressed to manufacturers: Foundational Cybersecurity Activities for IoT Device Manufacturers. The document "describes recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers. These foundational cybersecurity activities can help manufacturers lessen the cybersecurity-related efforts needed by customers, which in turn can reduce the prevalence and severity of IoT device compromises and the attacks performed using compromised devices."

2.4. Australia

In September 2020, the Australian Department of Home Affairs issued a voluntary Code of Practice document: Securing the Internet of Things for Consumers. The document "represents a first step in the Australian Government's approach to improve the security of IoT devices in Australia." This code of practice contains 13 principles and is intended for a business audience, but can also be browsed by consumers to encourage healthy security behaviours, and to increase awareness. “The Australian Government recommends industry prioritize the top three principles because action on default passwords, vulnerability disclosure and security updates will bring the largest security benefits in the short term.” Among the principles are the following:

- No duplicated default or weak passwords
- Implement a vulnerability disclosure policy
- Keep software securely updated
- Securely store credentials
- Make systems resilient to outages
- Make it easy for consumers to delete personal data

2.5. Brazil

In January 2021, the Brazil National Telecommunications Agency (ANATEL) published Act No 77/2021 regarding the minimum cybersecurity requirements for telecommunications equipment. The Act seeks to establish a set of cybersecurity requirements for telecommunications equipment to minimize or correct vulnerabilities through software/firmware updates or configuration recommendations. This Act enters into force on 4 July 2021. The act refers to international standards, including ISO/IEC 27402 — Cybersecurity — IoT security and privacy — Device baseline requirements [DRAFT], ETSI EN 303 645 v2.1.1 (2020-06) - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements, and ETSI TS 133 117 V16.5.0 (2020-08) - Universal Mobile Telecommunications System (UMTS); LTE; Catalog of general security assurance requirements, but it does not specify which standards must be followed for compliance.

The Act requires steps be taken to enable the use of appropriate encryption methods, according to international standards, for the transmission and storage of sensitive and personal data, and users must be able to easily delete their stored data without risks of exposure of personal information. §5.1.7 is responsible for the ability to mitigate potential attacks.

2.6. China

China has various cybersecurity and data regulations that are issued by different authorities. Among these regulations is the Cybersecurity Law of 2016. The Law aims to guarantee cybersecurity, safeguard cyberspace sovereignty, national security and public interest, and to protect the lawful rights and interests of citizens, legal persons and other organizations.

The Law comprises 79 articles in seven chapters and covers: collection, use and protection of personal information, protection of critical information infrastructure, clarification of responsibilities of network operators, and certification of critical equipment and special cybersecurity products.

2.7. South Africa

In April 2021, the South African Department of Communications and Digital Technologies issued a draft National Policy on Data and Cloud. The following objectives of the policy are outlined, to:

- “Promote connectivity and access to data and cloud services
- Remove regulatory barriers and enable competition
- Ensure implementation of effective cybersecurity privacy, and data and cloud infrastructure protection measures
- Provide for institutional mechanisms for the governance of data and cloud services
- Support the development of small, medium, and micro enterprises (SMMEs)
- Provide for research, innovation, and human capital development."

3. Cybersecurity Standards

There are various standards that are concerned with cybersecurity around the world, including:

ISO/IEC 27000-series is a group of standards that were developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The series acts as guidance to companies and organizations to help them enhance their security measures and prevent data breaches. They outline information security management system (ISMS) requirements and the steps necessary to prove compliance. They also cover information security controls that a company can implement.

ETSI EN 303 645 - Cyber Security for Consumer Internet of Things: Baseline Requirements. According to the European Union Agency for Cybersecurity (ENISA), this standard "establishes a common baseline across the European and wider global market, raising the security bar for all consumer IoT devices from near-zero to a good level" and "every major, at scale, attack involving consumer IoT seen to date is covered."

ISO 22301 - Security and resilience - Business continuity management systems - Requirements. According to the International Standards Organization (ISO), this standard contains "requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise."

ISO/IEC 15408 - Information technology — Security techniques — Evaluation criteria for IT security. This standard "is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality."

GB/T 25070-2019 Information Security Technology technical requirements of security design for classified protection of cybersecurity. This Chinese national standard outlines security requirements for new technologies such as cloud computing, mobile internet, Internet of Things, industrial control and big data, and the requirements for personal security protection in new application areas.

4. Manufacturer Requirements

The requirements that manufacturers of connected products must adhere to are still hazy and they differ greatly from one country to another. There is no global model for cybersecurity requirements; however, most of the regulations focus on:

Data protection: the need to ensure that consumer data is secure, and that consumers are informed of what exactly is being collected and how it is stored. Consumers must also be able to easily delete their stored personal data without risk of their data being retained without their knowledge.

Security: understanding vulnerabilities, detecting security breaches, and putting measures in place to prevent an incident before having to react to it.

Testing: which will include passing various cybersecurity standards depending on the country and its requirements at the time.

Certification: this is not yet widely implemented, but countries have started to develop cybersecurity certification schemes, even though there is no global model so far.

Reporting: most of the regulations require companies to report any security breaches within a short time period after becoming aware of one.

5. Challenges

There are inconsistencies between countries with regard to cybersecurity terminology, goals and scope of regulatory coverage. There is also no global consensus when it comes to cybersecurity regulations and there is no common model that all countries follow. Most countries agree on the importance of protecting consumer data, but there still is no agreement on what exactly needs to be included in a cybersecurity regulation.

New technologies are developed and introduced constantly, so it is hard for regulations to stay up to date with each new development and to include provisions that would cover each invention.

6. Conclusion

The aim of this paper was to present a brief overview of recent developments in cybersecurity regulations and standards around the world.

Although many countries are committed to cybersecurity regulation, they have found it difficult to match appropriate regulations with each new technology that is introduced. One thing is for certain: clear cybersecurity regulations are becoming a necessity with the increase of smart and connected devices.

About the Author

Rebeka El Hadad

Regulatory Analyst, Compliance & Risks

Rebeka is a Regulatory Analyst with the Global Regulatory Compliance Team. She is responsible for monitoring and researching regulatory developments in the Arabic speaking countries of the Middle East, as well as advising on regulations related to Cybersecurity and connected products.

She holds a Bachelor's Degree in English Language & Literature from the University of Gaza and a Master's Degree in Translation & Interpreting (English - Arabic) from Durham University, UK.

About Compliance & Risks

Compliance & Risks helps manufacturers, retailers and their supply chain partners monitor and manage requirements, regulations and standards for a cleaner, safer and better world. It creates business advantage for clients by providing reliable legislative information, insights and actions through C2P, its compliance knowledge management platform, consulting, market access, managed services and other solutions.

The company is recognized as the end to end global regulatory solutions provider across the technology, consumer goods and retail, industrial goods and life sciences sectors. Headquartered in Cork, they also have offices in Brussels, California, London and New York. For more information, please visit www.complianceandrisks.com

Important Notice: All information provided by Compliance & Risks Limited and its contributing researchers in this report is provided for strategic and informational purposes only and should not be construed as company specific legal compliance advice or counsel. Compliance & Risks Limited makes no representation whatsoever about the suitability of the information and services contained herein for resolving any question of law. Compliance & Risks Limited does not provide any legal services.