Compliance for FA Products with Cyber Related Laws, Regulations, and Standards Such as Cybersecurity

Author: *Mitsushiro Fujishima**

**Nagoya Works*

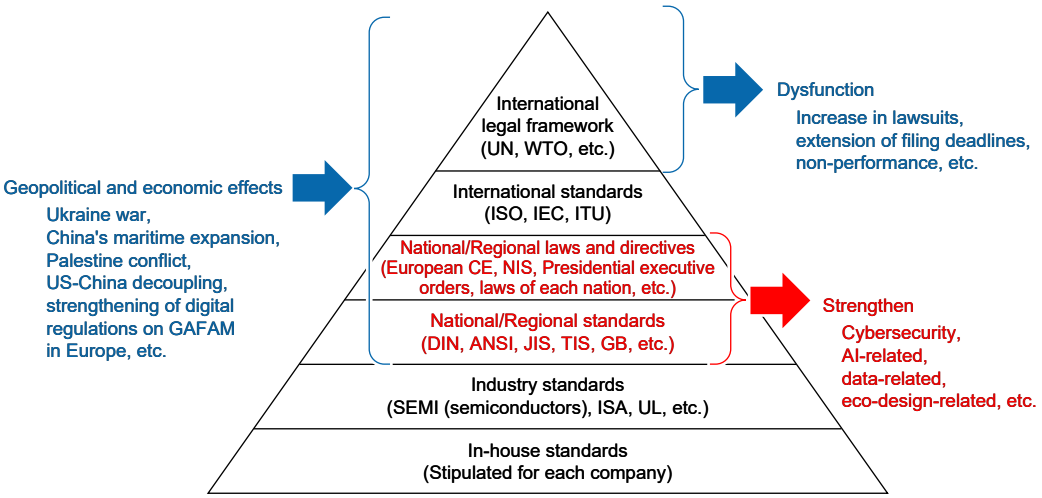
Abstract

At many companies marketing products or services in overseas markets, systems and human resource development are in place for compliance with traditional physical-matter-related laws, regulations, and standards, such as electrical safety laws and the European Directive on the Restriction of the use of certain Hazardous Substances in electronic equipment (RoHS). However, these systems and human resource development are not really adequate for digital-matter-related (hereinafter referred to as “cyber-related”) laws, regulations, and standards in fields such as cybersecurity and AI. This situation poses a risk of escalating into problems that could destabilize corporate management in today’s era where violations of laws, regulations, and standards become major news stories.

Furthermore, promptly and seriously addressing cyber-related laws, regulations, and standards in each country and region can raise the level of corporate competitiveness through various transformations.

1. Introduction

Currently, efforts are underway to digitalize information in factories and offices all over the world through initiatives such as manufacturing Digital Transformation (DX), the industrial Internet of Things (IoT), and the Fourth Industrial Revolution. This digital information can be shared in real-time via the Internet, and that is driving transformations in manufacturing and business models. And social transformation is advancing toward solving environmental issues and realizing well-being—i.e., pursuit of human happiness—through frameworks such as Society 5.0 and Sustainable Development Goals (SDGs).



ISO: International Organization for Standardization, IEC: International Electrotechnical Commission, ITU: International Telecommunication Union, CE: Conformite Europeenne, NIS: Network and Information Systems Directive, DIN: Deutsches Institut für Normung, ANSI: American National Standards Institute, JIS: Japanese Industrial Standards, TIS: Thailand Industrial Standards, GB: Guo jia Biao zhun, ISA: International Society of Automation, UL: Underwriters Laboratories Inc.

Fig. 1 Changes in the impact of laws, regulations, and standards

Amid such major transformations on a global scale, it is essential to establish cooperative frameworks through globalization transcending nations and regions. However, as shown in Fig. 1, recent events such as the Ukraine war, China's maritime expansion, the Palestinian issue in the Middle East, US-China decoupling, and application of the European Union General Data Protection Regulation (GDPR) to the American firms Google, Amazon, Facebook, Apple, and Microsoft (GAFAM) in Europe have intensified the trend of deglobalization driven by geopolitical and economic effects. Critics have also pointed out dysfunction of the United Nations and the World Trade Organization (WTO), which are meant to mediate international conflicts and trade issues.

Amid this international situation, China enforced the Cybersecurity Law of China (hereinafter referred to as the "Chinese CS Law") in June 2017, based on the idea that the Internet too has borders. In addition, cyber-related laws, regulations, standards, and requirements such as the European Cyber Resilience Act (CRA), AI regulation proposals, data laws, and digital product passports are being considered one after another for establishment or enhancement in 2024 and beyond.

In recent years, with the widespread use of social media and the resulting social environment where information spreads rapidly and can lead to public backlash, it goes without saying that even if there are no issues with product quality, a tarnished corporate image due to violations of laws, regulations, standards, or the like can have an extremely large damaging impact on a company's management.

This paper provides an overview and background of the Chinese CS Law, which has already come into effect, and the European CRA, which will come into effect in the future, while also discussing issues that will arise going forward.

2. Chinese CS Law

The Chinese CS Law is a law signed and issued by the President of the People's Republic of China himself to ensure national security by addressing issues such as cyberattacks from overseas, leakage of corporate secrets within China, and the leak of personal information. Many related laws have also been issued, and there has been particular emphasis on three related laws: the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law.

This law also includes a "reporting obligation," and violations may result in corrective recommendations, warnings, fines, revocation of business licenses, as well as fines or criminal liability for "individuals involved in violations." The Chinese CS Law is also related to national defense, and thus overseas companies cannot ignore the impact of the recently strengthened Counterespionage Law and must comply to ensure the safety of employees working within China.

2.1 Investigative background of the Chinese CS Law and issues

The draft of the Chinese CS Law was issued in June 2015. It was passed and promulgated by the Standing Committee of the National People's Congress in November 2016, and came into effect in June 2017. Products in Mitsubishi Electric's FA field were also included in the Catalogue of Critical Network Equipment and Network Security-specific Products (2017 No. 1, revised in July 2023), which was released at the same time, and Mitsubishi Electric started preliminary research (Table 1).

The biggest challenge for our company at the time was that national standards (Chinese GB standards) had not yet been established for the relevant products under this law, and furthermore, the criteria and assessment organizations for cybersecurity conformity assessment, the organizations ultimately responsible for granting certification, and other details were unclear.

In-house, we had established systems and developed human resources for hardware-related (physical) laws, regulations, and standards, such as electrical safety laws and the European RoHS Directive, which regulates hazardous substances. However, when it came to software-related laws, regulations, and standards for the latest cyber-related technologies such as cybersecurity, our systems and human resource development were still insufficient.

Table 1 Catalogue of Critical Network Equipment and Network Security-specific Products (excerpt from the 2017 No. 1 issue)

Category	Equipment/Product name	Required scope
Critical network equipment	Routers	Throughput (bidirectional) ≥ 12Tbps, Routing table capacity ≥ 550,000
	Switches	Throughput (bidirectional) ≥ 30Tbps, Packet switching rate ≥ 10Gpps
	Servers	Number of CPUs ≥ 8, Number of cores for a single CPU ≥ 14, Memory capacity ≥ 256GB
	PLC	Basic operation processing speed ≤ 0.08μs
Network security related products	Data backup machines	Backup capacity ≥ 20T, Backup speed ≥ 60MB/s, Backup time interval ≤ 1h
	Firewalls	Throughput ≥ 80Gbps, Maximum simultaneous number of sessions ≥ 3,000,000, Number of new sessions per second ≥ 250,000
	Web applications, firewalls	Throughput ≥ 6Gbps, Maximum HTTP concurrent sessions ≥ 2,000,000,
	Intrusion detection systems	Maximum detection speed ≥ 15Gbps, Maximum concurrent sessions ≥ 5,000,000
	Intrusion prevention systems	Maximum detection speed ≥ 20Gbps, Maximum concurrent sessions ≥ 5,000,000
	Secure gateways	Throughput ≥ 1Gbps, System delay ≤ 5ms

PLC: Programmable Logic Controller, HTTP: Hyper Text Transfer Protocol
Source: Information released by China: Catalogue of Critical Network Equipment and Network Security-specific Products (2017 No. 1)

2.2 Response to the Chinese CS Law

We formulated a compliance plan for the relevant products while inquiring with the Chinese standardization committees drafting standards for this law (SAC/TC28, TC260, TC124) as well as with candidate assessment and certification organizations. This plan includes addressing the requirements stipulated by the Chinese CS Law, projecting the timing for assessments and certifications, and arranging assessment equipment.

Also, measures were taken such as establishing a system for collaboration between a Product Security Incident Response Team (PSIRT)[(1)] (an organization responsible for improving the security level of products and services and responding to incidents company-wide), Chinese locations, and sales locations; and assigning and training specialized personnel in both China and Japan.

In March 2018, the “List of Organizations Conducting Security Assessments and Certifications for Critical Network Infrastructure Equipment and Network Security-specific Products (First Edition)” was published, and this clarified the relevant organizations. This list included organizations that we had already considered as candidates. Early establishment of relationships with these organizations facilitated relatively smooth assessments and certifications of the relevant products. This underscores the significant value of the preliminary research that started in 2017.

Also, between December 2022 and October 2023, GB standards (technical requirements and testing methods) for the relevant products were published, and we expressed opinions via local offices to help optimize the standards being formulated. Acquisition of this certification proves officially that the product has implemented appropriate security measures in compliance with relevant Chinese laws, regulations, and national standards. It has the advantage of allowing promotion of the product as government-certified to business partners and users.

Initially, in 2017, the grace period for obtaining product certification was until January 2019, but this was postponed to July 2023 or later. The current situation is such that, as a rule, products that have not acquired certification cannot be sold in China. Moreover, since such products are not listed on the Chinese government’s procurement list, they cannot be sold to state-owned enterprises, which are said to influence 20% of Chinese companies. Our relevant products in the FA field completed assessment and obtained certification by June 2023.

3. European CRA

The European CRA is a law that will take effect within the legal framework of the European region. Aside from exceptions, the scope is broad, “covering all products with digital elements.” Also, as EU directives are revised and approved in a form compliant with the CRA, meeting CRA requirements will become essential for obtaining “CE marking” on digital products.

Additionally, there are reporting obligations of incidents and vulnerabilities, and products cannot be sold in the EU market without fulfilling that obligation.

Furthermore, as a penalty for violations, strict regulations impose fines of up to €15 million or 2.5% of the company’s total global revenue, whichever is higher.

3.1 Investigative background of the European CRA and issues

As part of efforts relating to cybersecurity in Europe, the NIS Directive came into effect in August 2016, aiming to improve risk countermeasures for networks and information systems, strengthen incident response capabilities, and improve the level of safety. Also, the General Data Protection Regulation (GDPR) came into effect in May 2018. In June 2019, the EU Cybersecurity Act came into effect to strengthen the authority of the European Network and Information Security Agency (ENISA), and establish a cybersecurity certification system.

Up to this point, mandatory requirements regarding the cybersecurity of specific digital products had not been included. However, in September 2022, the European Commission released a draft of the European CRA, which listed critical digital products categorized into Class I (low risk) and Class II (high risk). Our relevant products in the FA field were included in these classes, and we began preliminary research (Table 2).

Table 2 Critical products with digital elements (excerpt from European CRA draft)[*1]

	Product name
Class I (low risk)	20. Microcontrollers, 21. ASIC and FPGA, 22. PLC, DCS, CNC, SCADA, Industrial Automation & Control Systems (IACS) (other than Class II products)
Class II (high risk)	7. Routers, modems, and switches for industrial use, 12. PLC, DCS, CNC, SCADA, Industrial Automation & Control Systems (IACS), 14. Robot sensing and actuator components and robot controllers

ASIC: Application Specific Integrated Circuit, FPGA: Field Programmable Gate Array,
DCS: Distributed Control System, CNC: Computerized Numerical Control,
SCADA: Supervisory Control And Data Acquisition, IACS: International Annealed Copper Standard
*1 Relevant products are expected to be subject to review when the European CRA is promulgated
Source: European public information: Critical products with digital elements (European CRA draft)

Currently, the trilogues (three-way dialogues) between the European Commission, Parliament, and Council have been completed, and preparations are underway for promulgation in fiscal 2024. In addition, while the aim at the draft stage was for “product application” to take effect by the end of 2025, adjustments have been made in the trilogues toward some delay. However, a geopolitical issue arose in February 2022 (the war in Ukraine) and many Ukrainian infrastructure facilities actually suffered cyberattacks so the need for early implementation of this bill remains unchanged.

Incident and vulnerability “reporting obligations” are expected to take effect earlier than “product application.”

3.2 Response to European CRA

In January 2023, a public comment period was held for the draft, and in cooperation with the Japan Business Council in Europe (JBCE)[(2)], which represents Japanese industry in Europe, Mitsubishi Electric also submitted opinions and made efforts to influence the process. We pointed out issues such as the difficulty of complying from overseas with the 24-hour reporting obligation to ENISA due to time differences, and the lack of clarity regarding the definition of the starting time for reporting.

At present, we are leveraging our experience with Chinese CS to build a system that includes our Head Office, while listing up our company’s digital products for the European market and considering how to

comply with the main requirements of the European CRA indicated below for relevant products.

(1) SBOM response

A Software Bill of Materials (SBOM) is a list of software components such as Open Source Software (OSS) included in a product, as well as their dependencies. Using an SBOM enables visualization of vulnerability risks latent in the supply chain.

(2) Compliance with reporting obligations and vulnerability mitigation

Centralized management of incident and vulnerability information is required, along with a reporting system to ENISA, and a product/service development organization that enables rapid response to vulnerabilities in products and services.

(3) Response for products and the development process

Standards such as IEC 62443-4-1, which prescribes a secure product development process for components and a security response process for the entire lifecycle, and IEC 62443-4-2, which specifies security technical requirements for industrial control systems, have been put forward as leading standard candidates.

Care is needed because there are many requirements other than these. Furthermore, even after promulgation of the European CRA, there have been many uncertainties, such as the harmonized standards to be complied with for specific conformity assessment methods and the like, and the impact on related laws and regulations (such as the AI regulation proposals, the Machinery Regulation, and Radio Equipment Directive). Therefore, efforts must be made to continue gathering information until the law comes fully into force.

4. Future Issues and Response

In Europe, in addition to the European CRA, steps such as AI regulation proposals, data laws, and digital product passports are being considered, and similarly, new or strengthened cyber-related laws, regulations, and standards are also being discussed in countries such as China and the US. Some of these, such as the Chinese CS Law, have already started to come into force. Taking into account the grace periods before penalties are applied, many of these will require compliance in stages by around 2030.

However, the examples of response described in section 2 and section 3 by no means went smoothly. In addition to the fact that these are new cyber-related laws, regulations, and standards, separate responses are required in each country and region. The departments in charge of the relevant products did not have enough capabilities and the resources to gather information and respond.

Therefore, the author’s department, which obtained the information, investigated overseas websites open to the public in order to correctly interpret the relevant laws, regulations, and standards, and gathered information on unclear points by utilizing research companies and consultants. We also requested cooperation with the investigation from overseas offices, retailers, and overseas industry groups. At the same time, because the relevant parties in-house were diverse, we persistently persuaded related departments through activities such as gathering them for various regular meetings. As a result, we clarified the promoting department and the people in charge who can provide ongoing consultation and response for the Chinese CS Law and European CRA.

A similar system is also necessary for other cyber-related laws, regulations, and standards. Particularly for AI and similar fields, there are challenges that cannot be addressed with the same system because the elements of digital technology differ.

To address this challenge, it is necessary, for example, to obtain information on cyber-related laws, regulations, and standards from overseas bases and sales locations where products are introduced to the market. Steps must also be taken in-house, i.e., establishing centralized management relating to laws, regulations, and standards, and securing resources with clearly defined roles, to ensure that information reaches endpoint designers without being interrupted in the course of information communication.

In addition, it is necessary to establish an information-sharing system with industry-related groups active overseas such as the European JBCE and JETRO, as well as with government agencies. Based on the information obtained, the impact on business must be investigated, including issues such as the need for changes to products already launched in overseas markets, and costs associated with continued market entry (such as addressing vulnerabilities when they are discovered), and, depending on the situation, decisions must be made such as stopping market entry (Fig. 2).

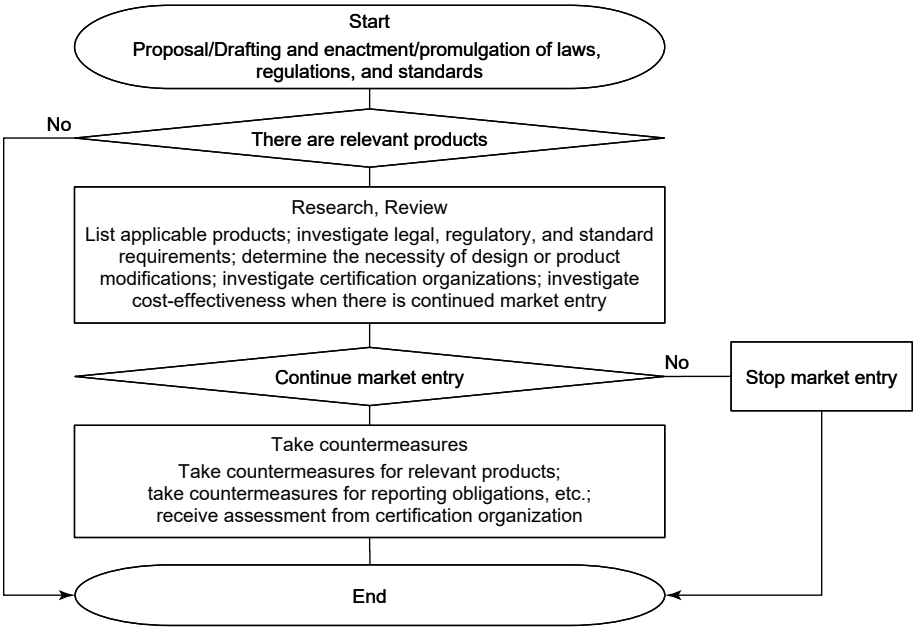


Fig. 2 Flow chart of compliance with laws, regulations, and standards

Overall, it is necessary to strengthen the existing physical-related legal, regulatory, and standards system to accommodate cyber-related laws, regulations, and standards and to develop and bolster human resources who are well-versed in cyber-related matters. This is a common challenge that needs to be solved by many companies.

5. Conclusion

As various transformations unfold on a global scale, recent geopolitical and economic issues have led to deglobalization, and the establishment and strengthening of cyber-related laws, regulations, standards, and requirements—such as the Chinese CS Law, the European CRA, and upcoming frameworks like AI regulation proposals, data laws, and digital product passports—are being considered.

For executives and managers of companies launching products in overseas markets, it is imperative to respond to such changes by proactively assigning appropriate personnel, strengthening human resource development, and establishing an organizational structure.

By promptly and seriously addressing cyber-related laws, regulations, and standards in various countries and regions, companies can adapt both as individual people and as organizations to diverse transformations of manufacturing, business models, and society, helping to raise the level of their corporate competitiveness. It is hoped this paper will help with that effort.

References

(1) Mitsubishi Electric PSIRT
https://www.MitsubishiElectric.co.jp/psirt/
(2) JBCE (Japan Business Council in Europe)
https://www.jbce.org/ja/