Charter of Trust

Harmonising Regulations – A Charter of Trust perspective

Publication date: September 2024

Introduction

In response to rising cyber threats, governments are enacting new cybersecurity laws and regulations, with some, like the United States (US), moving from voluntary public-private partnerships to more stringent regulatory approaches, while others, like the European Union (EU), are updating existing regulations (e.g. the Network and Information Security (NIS) Directive 2, or NIS 2) and creating new ones (e.g., Cyber Resilience Act, CRA). These efforts often set precedents for other nations, but the lack of international coordination in cybersecurity regulation remains a challenge. This fragmentation, coupled with shortages of cybersecurity talent, risks diverting resources from essential cyber defense to compliance, potentially increasing costs, complexity, and undermining resilience and innovation. Some solutions include reciprocity agreements, adopting international standards, and leveraging third-party assessments to streamline regulations and improve global alignment.

Discrepancies in definitions

Binding jurisprudence with technology. Integrating legal standards with technology presents a challenge, as technical and operational implementations depend on a precise understanding of legal requirements. The lack of uniformity and of a single consistent and authoritative definition for terms such as "product," make navigating and complying with these requirements complex.

Various definitions across jurisdictions. Discrepancies in definitions related to detection response activities may lead to **a) duplicative reporting** where manufacturers send a series of different reports corresponding to the same incident or b) **fragmented focus** where sectoral and national regulations may capture a different range of issues.

The CRA's likely definition of “vulnerability” based on cybersecurity weaknesses may not align with existing sectoral definitions. An example of this is in medical devices (MDR, IVDR), where the criteria for vulnerabilities depend on their impact on patient safety; in this context, vulnerabilities encompass not only those cybersecurity-related but also those due to malfunctions, safety hazards, or design flaws.

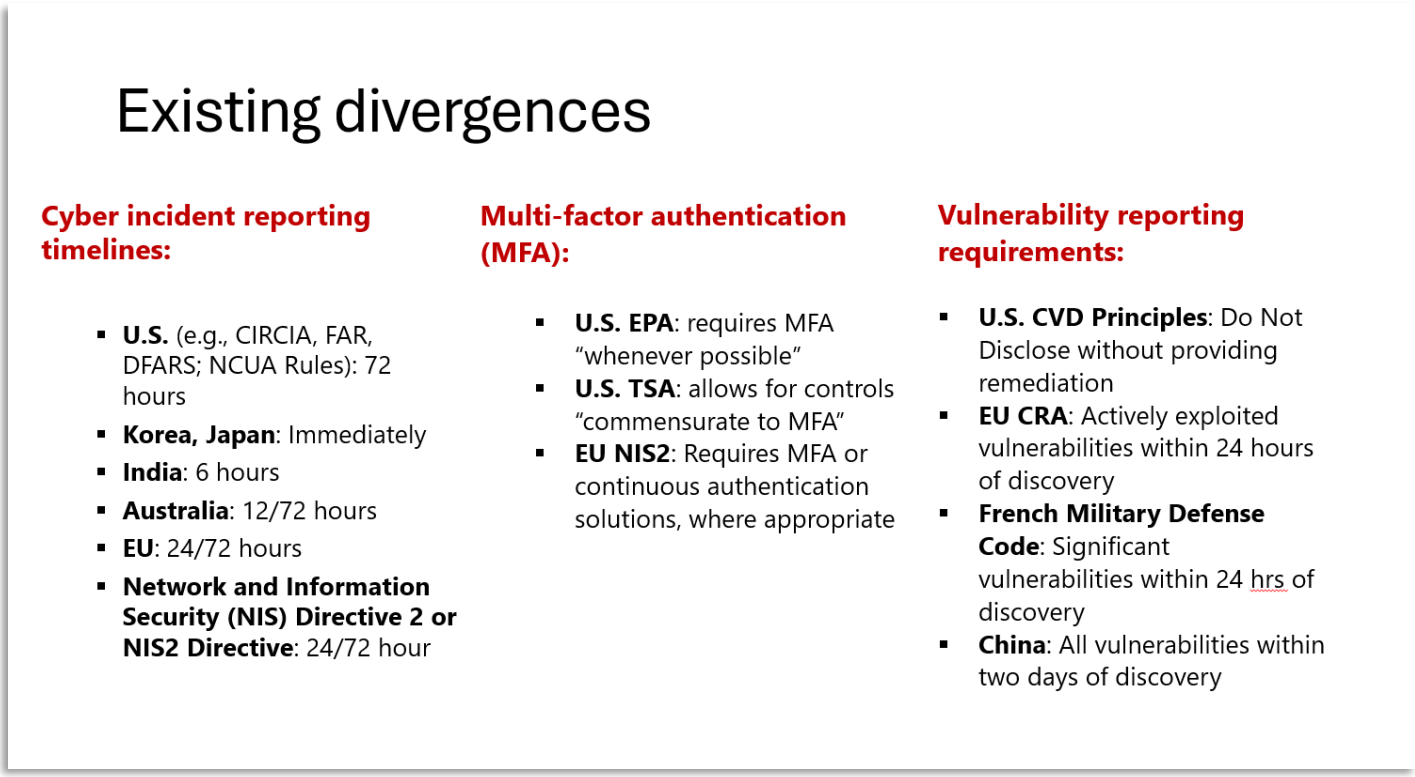
Discrepancies in obligations

Vague requirements. With regards to implementation, regulations can be sufficiently vague to allow for considerable flexibility. However, this vagueness does not always serve regulated entities well, as it leaves requirements open for interpretation. This creates vagueness on whether or not entities are meeting the compliance demands they are subject to.

Security requirements for products and solutions vary considerably. Products and solutions security requirements in the US and in the EU are not always equivalent. In some cases, requirements are more prescriptive and technical and can include mandatory encryption/ hardening, automated tools, and separate build environments for software development. In other cases, regulations are more risk-based, which set security objectives without going into technical details.

Incident reporting. There are numerous competing timelines for “incident reporting to authorities” (see table below). Moreover, the content and level of detail of the reporting differs between countries (i.e. between the EU and US). The reporting obligations landscape is also very fragmented in the US, which has around 50 cyber incident reporting requirements in effect or proposed across the Federal Government.

Security and practicality vis a vis patching The EU is leading in sustainability by requiring products to be supported for at least five years and obligating companies to provide patches for vulnerabilities (CRA). While these mandatory patches enhance user security, they can strain resources and potentially introduce new risks. Balancing security with practicality, and exploring alternative approaches, will be crucial in promoting a secure digital environment without hindering innovation.



Cost of fragmentation

Fragmentation in cybersecurity regulation inhibits adoption by creating a complex web of compliance requirements that are costly and challenging to navigate. This fragmentation increases operational pressures as entities must stay current, understand, implement, and build capabilities to meet varying local and regional standards. Manufacturers face difficulties in streamlining operations across markets, often leading to localised product variations and additional conformance schemes. The impact extends to product maintenance, including vulnerability reporting and patch management, which demands extra resources and infrastructure. High costs of compliance may be passed down the value chain, making manufacturers less competitive if they cannot leverage economies of scale.

In today's interconnected cyberspace, the need for regulatory harmonisation to avoid the proliferation of conflicting regulations is essential to offset challenges to cybersecurity and innovation. The lack of alignment could hinder effective defense against cyber threats, allowing malicious actors to exploit regulatory gaps across borders. By moving toward a more risk-based approach and embracing the need to organise regulatory cooperation, businesses and government agencies can streamline compliance efforts and effectively fortify global cybersecurity.