# Secure-by-design: Cybersecurity, IoT and the role of regulation

Security in technology is a double-edged sword for consumers and providers. It's supposed to be a driver for technological progress. But consumers' lack of confidence in security can make them slow to adopt new technologies. The secure-by-design (SBD) approach seeks to address this issue and to help build a technology ecosystem where consumers can feel confident entrusting their privacy to the industry. In fact SBD is now having an increased presence in regulation, and this will soon have implications within product markets worldwide.

**Authors:**

George Metaxas,
Legal and Regulatory Expert

Samuel Tew,
Senior Manager Consultant

**Analysts support:**

Elena Martín,
Associate Consultant

# Contents

# Abstract

**Technology connects much of society. It is present in just about every part of our lives. Today's consumers entrust a high volume of data to third parties through online and offline devices and services.**

Cybersecurity has therefore never been as important as it is today.

However, as we explain here, while security can be a driver of technological progress security concerns can make consumers hesitant to buy in to new technology.

The secure-by-design (SBD) approach seeks to address this paradox. It aims to help build a technology ecosystem where consumers can feel confident entrusting their private information to the technology industry.

Several countries are already enhancing SBD-related initiatives through policy schemes, guidelines and other 'soft law' instruments. However, little clear legislation or enforcement is in place at the moment.

This is about to change. The European Commission's recently proposed Cyber Resilience Act is the first EU-wide regulation with cross-sector cybersecurity obligations for manufacturers. For now, its jurisdiction is limited to the European market. But the Act will inevitably have repercussions across the world.

# 1. Introduction

Never before has the global importance of cybersecurity been as evident as it is today. From the real or virtual battlegrounds of geopolitics to the everyday use of computers and smartphones, communications, data and technology are regularly exposed to targeted and potentially crippling cyberattacks. The global annual cost of cybercrime was reportedly EUR 5.5 trillion in 2020, up from EUR 2.7 trillion in 2015.[1]

**Communications, data and technology are regularly exposed to targeted and potentially crippling cyberattacks**

The response to these threats has been a daily war, fought in the shadows by countries and businesses alike. However, with the exception of certain particularly critical areas, governments have generally stopped short of imposing clear legislative obligations on the ICT industry to support the fight against cyberattacks.

In Europe at least, this is about to change. The European Commission's recently proposed Cyber Resilience Act is the first EU-wide regulation with cross-sector cybersecurity obligations for manufacturers. Its market is European. However, its implications will be global. Like personal data protection, it will be negotiated, criticized and fine-tuned, but it will eventually be approved. It will then be emulated across the world.

The Act is not expected to be adopted before late 2024; most of its provisions will come into force only two years later. However, vulnerability and incident reporting by manufacturers to ENISA (the EU agency for cybersecurity) will become mandatory only a year after the Act's adoption. Importantly it will also apply for old products.

This is much less generous timing than it sounds. Manufacturers will have to align their design and development plans, and their reporting and updating procedures, well before the Act's obligations kick in.

Prominent among these obligations is a need for manufacturers of what are referred to as 'products with digital elements' to ensure these are secure by design and by default, in order to meet certain essential requirements listed in the Act's Annex I. Manufacturers must also assess any associated cybersecurity risks and keep these in mind during the planning, design, development, production, delivery and maintenance phases of the product.

1 https://publications.jrc.ec.europa.eu/repository/handle/JRC121051.

Meeting these standards as well as other obligations set out in the Act will require substantial preparation on the manufacturers' side.

In this article, we look at the factors that have led to the need for such measures, and the so-called 'security paradox' that can affect technology adoption. We then provide examples of various government 'secure-by-design' initiatives in this domain across the world. Finally we examine the relevant provisions of the European Commission's Cyber Resilience Act and their expected ramifications for the European and global digital technology industry.

# 2. Technology, cyberthreats and the 'security paradox'

Technology has become the primary means of connecting society; it is present in almost every facet of our lives. Digital transformation – the integration of digital technology into all areas of a business – has been accelerating, particularly during and because of the Covid-19 pandemic. In turn the creation of a technology-led landscape has encouraged consumers to entrust an increasingly high volume of data to third parties through online and offline devices and services.

Cybersecurity, and security in general, is therefore critically important. Recent events like the war in Ukraine have further demonstrated the importance of protecting digital systems and devices.

For manufacturers and developers, however, cybersecurity has traditionally been treated more as an afterthought. In reality, cybersecurity should be at the heart of the development of digital commercial offerings, ensuring consumer confidence but without constraining and limiting adoption of new technologies.

This brings us to the secure-by-design ('SBD') concept. Embedding security at the heart of services and products is the main pillar of the SBD concept. It involves encouraging security strategies or systems at the design phase of a service or product, thereby making the offering foundationally secure.

It also addresses the so-called '**security paradox**' whereby security may be improving but many consumers seem to have a completely different perception. A recent study in the UK showed that, due to security concerns, 28% of consumers would not buy any smart device in the following 12 months. And yet security is also perceived as a driver for technology progress, as companies are constantly seeking new systems and procedures to enhance privacy and security.

**Secure-by-design involves encouraging security strategies or systems at the design phase of a service or product**

SBD approaches seek to address this paradox and help build a technology ecosystem where consumers can feel confident about entrusting their privacy to the industry. SBD is guided by the principle that security and privacy should be a natural input to every service or product development – especially as these become more complex, manage more sensitive data and rely on several third-party integrations that blur the frontiers of data ownership and liability.

The SBD principle is underpinned by the following pillars:

| SBD pillar | Explanation |
|---|---|
| **Alignment and clear strategy** | Maintain a unified strategic vision of what security is meant to achieve. Supply chain stakeholders should align to assure all components are secure by default. Enforce clear accountability and responsibility |
| **Transparency and awareness** | Enterprises need to be transparent over any security and privacy measures they have integrated in their offerings |
| **Continuous monitoring** | Streamlining auditing through continuous and automated monitoring of the effectiveness of security mechanisms to evaluate progress or potential security breaches |
| **Resilience** | Developing continuity plans and security assessments to maintain updated policies and security measures and mitigate further collateral damage |

Figure 1: Main principles embedded in a secure-by-design approach

# 3. SBD in practice: IoT, 5G and new threats

SBD principles were initially conceived for the construction industry and related to the security of buildings and their immediate surroundings. Their scope now reaches quite different industries, not least because of the increased reach of IT and software, which today extends to many key sectors such as healthcare, transport, manufacturing and, of course, telecoms.

Cyberattacks are increasing in volume and sophistication. During 2021, their number rose by 15.1% compared to the previous year and more than 60% of companies were targeted by software supply chain attacks.

As organizations rely more heavily on third-party providers, their security exposure has increased. In fact 44% of organizations agree that relying on suppliers and partners increases their security risks. Commonly employed preventive tactics, such as vulnerability assessments, are not enough to guarantee a system's secure use.

SBD policies strengthen cybersecurity and ensure a more robust IT infrastructure, by monitoring and auditing data security from the initial phase of the development of a service. For instance, organizations with SBD-inspired cyberattack preventive strategies are expected to save up to 1.4M USD when reacting to a cyberattack. Further, enterprises with automated security systems reportedly spend an average of less than 2.5M USD after a data breach. Organizations without such systems can suffer average damages of more than 6M USD.

**SBD policies strengthen cybersecurity and ensure a more robust IT infrastructure, by monitoring and auditing data security from the initial phase of the development of a service**

An area in which SBD principles are now particularly critical is IoT systems. These involve several layers of stakeholders, making accountability and responsibility unclear, and leaving IoT systems open to security breaches.

Various shifts in consumer habits are accelerating IoT adoption. IoT systems are also offering cybercriminals new, less protected, entry points for accessing consumers' and organizations' private data. During 2022, the IoT market is expected to grow 18%, reaching 14.4 billion active connections; by 2025 there will be 27 billion connected IoT devices.

Many telecoms infrastructure or network components provide gateways for potential threats and cyberattacks to reach a great volume of users or devices. Take the GTP protocol. This is 3GPP-defined standard that allows GPRS data to be carried within 3G and 4G networks. Although this protocol is widely used, it contains inherent security flaws, one of which is that users' locations are not validated by the protocol for their legitimacy, opening the door to malicious or fraudulent traffic being sent using the protocol or even increasing the possibility of Denial-of-Service (DoS) attacks being coordinated.

**IoT systems are offering cybercriminals new, less protected, entry points for accessing consumers' and organizations' private data**

There is, however, an SBD angle here that can mitigate this threat. Previous network generations were much more vulnerable to attacks mainly due to a lack of knowledge of the potential threats faced by digital systems. This led to cybersecurity strategies and solutions (such as firewalls) being applied only on an ex-post basis. 5G networks have contributed to a security mindset shift as 5G is by default built on security standards, making its networks robust by design (see our recently published article: 5G security in super-connected operators.)

But other security threats have emerged as consumers' and workers' habits have changed. The most obvious example comes from recent Covid-19-related developments.

The pandemic has changed service providers' offerings and consumers' expectations. Interconnectivity is on the rise. More people are working from home and connecting from different countries or networks. Security thus needs to be extended to cover all use cases, including working-from-home rises of the sort seen during the Covid-19 pandemic.

The answer? Secure the whole supply chain (considering both hardware and software components), have the right security skills and support in place, and maintain and monitor security standards. This approach will lead to an efficient preventive cybersecurity strategy and a timely damage mitigation plan.

# 4. SBD and the role of regulation

In an increasingly technology-led society, governments and regulators have to promote digital transformation and adoption among providers and consumers while ensuring security and privacy are not compromised. Balancing these priorities can be challenging. However, a key lever for success is to target the supply side of the market, in particular through regulation. By supporting or even mandating an SBD scheme regulators can offer a path service providers can follow – one that allows them to adopt the correct security measures while generating accountability to all parties involved and creating awareness.

**Governments and regulators have to promote digital transformation and adoption among providers and consumers while ensuring security and privacy are not compromised**

There are two main areas that regulators and governments need to target when developing secure-by-design codes of practice:

1. **Policy and regulation:** Policymakers need to develop regulations and recommendations to make sure providers embed end-to-end security controls. Additionally, more efforts need to be tailored to handle cybersecurity-related attacks during specific events, such as the Covid-19 pandemic, to anticipate potential threats and to develop a rapid response minimizing impact and collateral damage.

2. **Incident reporting:** Maintaining a continuous monitoring of security attacks and reporting these to the corresponding regulatory authority can improve resilience efforts and enhance a collaborative approach between industry, regulators and even international organizations.

The latest SBD regulatory initiatives and guidelines are mainly focused on the IoT industry. This is not surprising given the increasing prevalence of connected devices in our homes and businesses. As mentioned previously, IoT has historically been a sector where security measures were mostly applied after issues were encountered.

**The latest SBD regulatory initiatives and guidelines are mainly focused on the IoT industry. This is not surprising giving the increasing prevalence of connected devices in our homes and businesses**

So what would be an appropriate cybersecurity SBD measure for IoT? One commonly offered example is a 'no universal default passwords' requirement. Many IoT devices are sold with default passwords and even default usernames (for instance 'admin, admin'). These are often not changed by the end user, thus creating a significant security risk. If all IoT devices have the same credentials malware can easily access them in a botnet.[2]

One of the most famous IoT hacks exploiting default passwords was the Mirai Botnet strike. Dyn, a DNS provider was attacked using a botnet of IoT devices. The Mirai malware infected one vulnerable IoT device and afterwards searched the Internet for other vulnerable devices by logging in with the default name and password. It thus kept infecting other devices and replicating through them. Huge sections of the Internet went down and tech giants such as Twitter and Netflix had their services interrupted.

2 i.e., a network of computers infected with malicious software and controlled without the owners' knowledge.

# 5. Examples of national SBD measures

Several countries are already enhancing – or planning to enhance – SBD-related initiatives through policy schemes, guidelines, recommendations, codes of practice and other 'soft law' instruments. However, little if any clear legislation or enforcement is in place at the moment.

**The UK** has already taken action in relation to SBD, although this action is so far limited to the IoT landscape and aimed at improving the cybersecurity of IoT-related devices. The idea is to promote a security mindset, starting from product development and extending throughout the entire life cycle by, for instance, regularly assessing cybersecurity risks.

In March 2018, the UK government published a secure-by-design report, aimed at making sure that security practices are built into products. The report identified two main security risks of IoT devices: **vulnerability of individual devices** affecting consumers' privacy and security, and the **risk of large scale cyberattacks**.

The report led to a code of practice with thirteen guidelines. These included implementing a vulnerability disclosure policy, keeping software updated and securely storing credentials and sensitive data. The guidelines mainly addressed device manufacturers, IoT service providers, and mobile application developers and retailers.

Publication of this report was followed by an informal consultation on its conclusions and proposed policy interventions. The conclusion was that, although the adoption of the thirteen principles had been satisfactory, there were still some outdated and risky practices that needed to be addressed. Hence policy interventions for proposed legislation to regulate the cybersecurity of IoT devices within the UK were made clear. These would include an obligation for manufacturers to comply with certain security requirements before making products available in the national market.

**In the UK, a Product Security and Telecommunications Infrastructure Bill will provide a legal framework for security obligations for 'internet-connectable' and 'network-connectable products'**

Most importantly, a Product Security and Telecommunications Infrastructure Bill (HL Bill 16), first presented in November 2021 and currently moving through its last stages of legislative adoption in the UK, will provide a legal framework for security obligations for 'internet-connectable' and 'network-connectable products'. Detailed security obligations under this (future) Act will be eventually specified by the Secretary of State, through regulations, but it can be expected that these will also include 'secure by design' requirements.

In **Saudi Arabia (KSA)**, the telecoms and ITC regulator (CST, formerly CITC) issued, in September 2019, a regulatory framework for IoT devices and associated services, with recommendations and (high-level) mandatory requirements. These revolve around IoT equipment, data management and general obligations. For instance, service providers must make end users aware of the importance of data security and offer recommendations to improve it.

In **Japan,** the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) published in October 2016 a framework to clarify the security requirements for IoT systems as well as sector-specific SBD requirements.

This framework highlights essential security requirements for IoT systems and has led to the development of guidelines or principles (each with specific measures against different types of security risks) based on key security strategies for IoT devices. These guiding principles are classified according to the development stage of the IoT product, such as analysis, design, implementation and maintenance.

**Most countries are developing SBD codes of practice or frameworks but with no legal obligations towards manufacturers**

Other countries have incorporated SBD into their national cybersecurity strategies, without yet taking any further action. For example, **Australia**'s government included the need to secure products and services (including IoT devices) as an objective in its 2020 strategy. In 2020, it developed a voluntary code of practice to secure IoT devices for consumers and design supply chain principles to promote transparency, autonomy and integrity in investment and security. This guide was developed in alignment with the 2018 UK code of practice.

Similarly, the Cyber Security Agency of **Singapore** (CSA) published the *Safer Cybersecure Masterplan* in 2020, with the aim of mobilising industry and consumers to create a cybersafe digital space – that is, one not limited to IoT devices. Singapore has also launched a Cybersecurity Labelling Scheme (CLS), which should allow consumers to identify which smart devices have better built-in cybersecurity features.

A summary of these countries' SBD-related actions is shown in the table below:

| Country | SBD actions |
|---|---|
| **UK** | ■ Secure-by-design report regarding UK IT market<br>■ Code of Practice in 2018 including guidelines for IT devices<br>■ Product Security & Telecom Infrastructure Bill in 2022 |
| **KSA** | ■ Regulatory framework for IT devices published in 2019 by CST |
| **Japan** | ■ Framework to clarify the security requirements for IT systems<br>■ IoT security guidelines published in 2016 including security principles to validate during the design phase of IoT devices |
| **Australia** | ■ National Cybersecurity Strategy 2020<br>■ Code of Practice to secure IT devices in 2020 |
| **Singapore** | ■ Safer Cybersecure Masterplan 2020 dedicated to secure the country's digital infrastructure (not limited to IT devices) through a secure-by-design mindset shift |

Figure 2: Selection of government policies utilising Secure-by-Design for IoT.

# 6. The EC's Cyber Resilience Act

## 6.1. Brief overview

The main objective of the European Commission's proposed Cyber Resilience Act, unveiled on 15 September 2022, is to lay down rules for the placing on the EU market of what are called 'products with digital elements' under conditions that ensure their cybersecurity. The Act aims to do this by imposing certain essential requirements for these products' design, development, production and vulnerability-handling processes during their whole life cycle.

**Products with digital elements** are defined as any software or hardware products and their remote data processing solutions. They also include hardware/software components placed on the market separately.

Products with digital elements are not limited to the more sophisticated IT industry products whose manufacturers are already familiar with the risk of cyberattacks and tools to avert them. They also include smartphones, computers and, especially, a large number of connected household devices.

This is important. While computers and phones may be at least partly protected today by design or through regular updates and commercial solutions available on the market such as anti-virus software, 'smart' household devices offer an open field for cyberattacks. According to the multinational consumers' rights organisation Euroconsumers, its 'Hackable Home' project has identified 54 vulnerabilities across 16 connected devices including doorbells, locks, baby monitors, robo-vacuum cleaners, Wi-Fi routers and alarm systems.

The Act does not apply to certain products already covered by existing EU regulations, namely **medical devices** for human use and their accessories, in **vitro diagnostic devices**, and **motor vehicles** and their systems and components. Products developed exclusively for **national security, military purposes** or the **processing of classified information** are also excluded from the Act's scope.

**While computers and phones may be at least partly protected by design today, 'smart' household devices offer an open field for cyberattacks**

**The Act does not apply to certain products already covered by existing EU regulations, such as medical devices for human use, in vitro diagnostic devices and motor vehicles**

Briefly, the Act sets out two sets of obligations, mainly for manufacturers, but also for importers and distributors:

- Obligations applying to all products with digital elements, regardless of their risk category. The relevant requirements also include various SBD obligations for manufacturers, which are discussed in section 6.2.

- Additional conformity procedures for more critical categories of products, representing about 10% of the total number of products with digital elements. These, more critical, products are divided into two Classes. Class II represents a higher risk than Class I and thus requires a third-party conformity assessment. Examples of Class I products include browsers, password managers, security software, VPN functions, network management systems, firewalls and physical network interfaces. Examples of Class II products include operating systems, industrial use firewalls, microprocessors, industrial automation & control systems, industrial IoT devices for use by 'essential entities' (i.e., various types of utilities, financial institutions, telcos, digital infrastructure providers, and public administration) and smart meters.

Technically, the Act is actually an EU regulation. This means that, once it enters into force (probably in late 2024), it will apply directly in all EU Member States, with no need for national implementation measures. Further, as a regulation (and unlike a directive), it will have 'horizontal effect'. This means that private parties, such as consumers, will have the right to invoke its provisions directly in national proceedings against other parties, such as in civil damages actions. This could be important given the several layers of stakeholders and business partners involved in IoT applications, all of whom could be seriously affected by the consequences of security breaches due to a manufacturer's or other party's failure to comply with the Act's obligations.

## 6.2. A closer look at the Act's SBD obligations

Secure 'by-design-and-by-default' is a generic requirement. It may cover more detailed obligations, and its enforcement is subject to case-by-case interpretation. In an earlier example of an EU approach to personal data protection, a reference to an SBD obligation was described in the 2016 General Data Protection Regulation in general terms only. The proposed Cyber Resilience Act is more specific on the individual requirements falling under the concept of SBD, and the high standards required.

**Manufacturers must undertake a cybersecurity risk assessment of the products concerned and take its outcome into account during the products' planning, design, development, production, delivery and maintenance phases**

The basic SBD obligation set out in the Act is for all manufacturers of products with digital elements to ensure, when placing them on the market, that these have been designed, developed and produced in accordance with a list of 'essential requirements' set out in Section 1 of the Act's Annex I, and are delivered without any known exploitable vulnerabilities.

To comply with this general obligation, manufacturers must undertake a **cybersecurity risk assessment of the products concerned** and take its outcome into account during the products' planning, design, development, production, delivery and maintenance phases.

The cybersecurity risk assessment must aim to ensure that the following essential requirements are met:

- Secure-by-default configuration, including a possible reset to the product's original state;
- Appropriate control mechanisms against unauthorized access (e.g., authentication, identity or access management systems);
- Protection of confidentiality of stored, transmitted or processed personal or other data;
- Protection of integrity of personal or other data, commands, programs and configuration;
- 'Minimisation of data', i.e., processing only adequate and relevant data – and no more data than necessary;
- Protection of availability of essential functions and minimisation of any negative impact on the availability of other devices' or networks' services;

- Limitation of any attack surfaces, such as external interfaces;
- Reducing the impact of any incidents through appropriate exploitation mitigation mechanisms and techniques;
- Provision of security-related information through recording or monitoring mechanisms;
- Ensuring that vulnerabilities can be addressed through updates.

This is a challenging checklist. Many manufacturers will wonder how to address it and whether there are any existing suitable standards and processes to help them achieve this in time. In principle, the Act describes three basic options.

**First**, insofar as products with digital elements and their processes are in conformity with the whole, or part, of harmonised standards that have been published in the EU Official Journal (or will be published in the future), they will also be presumed to be in conformity with the essential requirements covered by those harmonised standards (or their relevant parts).

**The Act's essential requirements will need to be supported and harmonized by other applicable or common EU standards in order to facilitate and guide manufacturers' compliance**

In its separate Impact Assessment accompanying the proposed Act, the Commission notes that while there is a variety of international standards concerning various aspects of product cybersecurity (such as consumer IoT, assurance of security throughout life cycle or vulnerability handling and access control), there are no harmonized European standards for products with digital elements across sectors.

The Commission has listed 24 'notable examples of relevant international standards [and] widely used industry best practices and guidelines' that touch upon cybersecurity of products with digital elements. Such examples include ETSI EN 303 645 (Cyber Security for Consumer IoT: Baseline Requirements); ETSI TR 103 621 (Guide to Cyber Security for Consumer Internet of Things); GSMA IoT Security Guidelines; and ISO/IEC 27400:2022 (Cybersecurity - IoT Security and Privacy Guidelines). The extent to which these standards will form a basis for harmonized European cybersecurity standards will have to be sorted out in the near future.

**As a second option**, where EU-harmonised cybersecurity standards for the Act's needs do not exist or are insufficient, and the required standardisation process is delayed or rejected by the relevant European standardisation bodies, the Commission will have the power to adopt 'common specifications' in respect of the Act's essential requirements. Compliance with these common specifications will also provide a presumption of compliance with the Act's corresponding essential requirements.

**As a third option**, a presumption of compliance with the Act's essential requirements can also be based on an EU statement of conformity or a certificate, issued under a European cybersecurity certification scheme, to be specified in the future by the Commission.

Other obligations for manufacturers under the Act include supplying a cybersecurity risk assessment in the technical documentation that must accompany the products in question. Manufacturers must also systematically document relevant cybersecurity aspects of these products, including any vulnerabilities they become aware of through third parties.

Although manufacturers are the main focus of the obligations described in the Act, there are also separate lists of obligations for importers and distributors of the relevant products in the EU.

**Although manufacturers are the main focus of the obligations described in the Act, there are also separate lists of obligations for importers and distributors of the relevant products in the EU**

The Act stipulates serious penalties, to be imposed by national authorities, for non-compliance with these and other requirements. They include fines of up to €15 million or 2.5 % of worldwide annual turnover (whichever is highest). These may well be accompanied by separate civil damages actions.

Perhaps most significantly, the Act will apply to the placing of products with digital elements on the EU market, regardless of where these products have been manufactured. This is bound to have a spillover effect across the world. Manufacturers of products affected by the Act may find it difficult to follow separate (stricter) SBD and other standards for products destined for the EU market than those they sell elsewhere. Importers and distributors too will be required to ensure that the products they import, distribute or sell are in compliance with the Act.

# 7. Conclusion

The European Commission's proposed Cyber Resilience Act is the first major regulatory initiative for specific and binding cybersecurity obligations on the manufacturers, distributors and importers of a very wide range of even partly digital products and systems. Most of these are now part of our everyday lives. Although it is jurisdictionally limited to the European market, the Act will inevitably have repercussions across the world.

If the proposed Act moves through the EU legislative process at the expected pace, there is little time left for manufacturers to align their design, development and sales processes to the Act's cybersecurity requirements and avoid serious penalties and damages claims. Official technical standards for compliance with the Act's requirements are bound to remain work-in-progress both before and after the Act's formal adoption.

This leaves manufacturers and other stakeholders in a difficult position, as the existing international technical standards and guidelines are not necessarily geared towards compliance with the Act.

On the EU Member State level, the Act will create a host of powers and duties for national supervisory authorities, which may or may not be identical to the present cybersecurity bodies. But even outside the EU, the Act is bound to have an impact on national cybersecurity regimes – as did the European data protection paradigm, which has had a geographic spillover effect, leading to a wave of similar laws and new regulators across the world.

There could be an indirect effect too. Cybersecurity is a global concern; the Act's provisions, and especially those on 'essential requirements', could provide a model for non-EU government bodies wishing to ensure the cybersecurity of (even partly) digital equipment and systems produced, distributed or imported in their jurisdictions.

Meeting the requirements of the Act will be a difficult undertaking for many groups. However, we can help. Axon's international team of cybersecurity experts stands ready to ensure that regulators and other clients are able to navigate successfully through this challenging process.

# About
# **Axon Consulting**

Axon is an international firm founded in 2006 that provides investment and advisory services to a broad client base in the technology and innovation space in more than 70 countries across the world.

Axon's cybersecurity practice is central to its business and an increasingly important service area for clients. Its work in this field includes strategy, policy/regulation, and research at business and governmental level. Axon works closely with national representatives to help them understand their cybersecurity needs and to define actionable recommendations aimed at improving their cybersecurity ecosystems.

**Tel:** +34 913 102 894
**Email:** marketing@axonpartnersgroup.com



**Madrid (HQ)**
Calle Sagasta 18,
3rd Floor,
28004, Madrid

**Brussels**
91, Avenue du Roi,
1190, Brussels

**Istanbul**
Buyukdere Cad.
No. 255 Nurol Plaza,
B0434450 Maslak,
Istanbul

**Bogota**
Calle 100 #13-95,
Torre Empresarial FD,
100 Piso 6,
Bogota

**Riyadh**
3141 Anas ibn,
Malik Road, Building B,
2nd Floor,
Al Malqa, Riyadh

**AxonPG**

**axon-partners-group**