DEKRA

Whitepaper

Strengthening Cybersecurity for Critical Infrastructure and IoT

[...] There are an estimated **2,220 cyberattacks per day** worldwide, adding up to over **800,000 attacks** per year.

Despite the undeniable rise in cyberattacks, many organisations still seem to think (or hope?) that it won't happen to them. As a result, they fail to take sufficient precautions against cybercrime. To address this situation in a move to increase the European Union's cyber-resilience, the European Commission is introducing various new pieces of cybersecurity legislation. But how do you know whether you've taken sufficient measures to shoulder your responsibility for cybersecurity – and will it stand up in court if necessary?

Due to the ever-expanding dependence on digital technologies in daily life and business, it is becoming increasingly important for organisations to take cybersecurity seriously. According to the **World Economic Forum (WEF)**, there are an estimated 2,220 cyberattacks per day worldwide, adding up to over 800,000 attacks per year. In 2023, these included major high-profile cyberattacks on the US State Department, the UK's Royal Mail, and the Indonesian Immigration Directorate General, with the latter leading to the theft of 34 million Indonesian citizens' passport records.

Cyberattacks can prove very costly. The European Commission estimated the annual cost of cybercrime to the global economy at €5.5 trillion ($5.9 trillion). Various data sources currently put the figure at around $8 trillion, but according to an article by the WEF this could surge to as much as $23.84 trillion by 2027. In addition to the losses directly resulting from the operational impact of a cyberattack, organisations that are held liable for an attack can also suffer extensive financial, legal, reputational and strategic consequences following a court case.

[...] Attacks on organisations in critical infrastructure sectors rose from less than **10 in 2013** to almost **400 in 2020**

Over the years, critical infrastructure has become more reliant on industrial control systems for monitoring processes and controlling networks of connected physical devices. Critical infrastructure includes sectors such as energy production & transmission, water & wastewater, transport, telecommunications, public services, healthcare, and food & agriculture.

However, **industry experts** are concerned that industrial control systems and other operational technologies receive less attention than IT systems in the context of cybersecurity, making critical infrastructure extra vulnerable to cyberthreats. Indeed, besides seeking to steal data and information, cybercriminals are increasingly targeting critical infrastructure. According to **Gartner,** attacks on organisations in critical infrastructure sectors rose from less than 10 in 2013 to almost 400 in 2020: a 3,900% increase.

This more clearly defines the **organisations covered** and their specific requirements, and also **expands the scope**

Against the backdrop of these rapidly growing risks and the potentially disastrous consequences for businesses, consumers and society as a whole, the European Commission is keen to strengthen the European Union's resilience to cybercrime. This is leading to a number of cybersecurity-related changes in the legislative landscape:

NIS2 DIRECTIVE

The Network and Information Systems (NIS) Directive was introduced in 2016 as the first European legislation enforcing cybersecurity measures by organisations identified as 'essential' service operators. In line with the theory that any digital network is only as strong as its 'weakest link', the directive's objective was to improve the functioning of the internal market by achieving a high common level of security of network and information systems in companies and organisations – i.e. at user level – within the EU.

Not long afterwards, however, it became clear that the implementation varied greatly between Member States. This led to a fragmented system where some companies and organisations were considered essential in some countries, but not in others. Moreover, deficiencies in the NIS Directive included insufficient cyber resilience of EU businesses, inconsistent resilience across sectors, lack of common understanding of threats, and lack of joint crisis response.

To rectify this, the European Commission launched the revised Network and Information Security Directive (**NIS2**), which was adopted in November 2022 and is due to enter into force in October 2024. This more clearly defines the organisations covered and their specific requirements, and also expands the scope.

Whereas NIS only covered sectors such as water supply, energy, digital infrastructure, banking, financial market infrastructure, health and transport, NIS2 now also includes public administration, digital providers, space, research, postal services, waste management, foods, manufacturing and chemical products. In addition, NIS2 also strengthens requirements for cybersecurity enforcement, including widened risk management, early mandatory incident reporting, and a newly defined designation of C-level cybersecurity responsibility.

ISO 27001

To comply with the NIS directive, you can use the **ISO 27001 standard**. It allows you to shape your information security management system in a structured way. DEKRA Audit is happy to certify you against ISO 27001.

These new cybersecurity requirements **apply to all products** with a radio connection, such as 4G, 5G, Bluetooth, Zigbee and Wi-Fi

Action to improve the cybersecurity of wireless devices **available on the European market**

Delegated Act of the Radio Equipment Directive (RED-DA)
The radio equipment directive 2014/53/EU (RED) establishes the regulatory framework for placing radio equipment on the market, setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum.

In 2021, the European Commission announced that it was taking action to improve the cybersecurity of wireless devices available on the European market. It adopted a **Delegated Act of the Radio Equipment Directive (RED-DA)**, laying down new legal requirements for cybersecurity safeguards, which manufacturers will have to take into account in the design and manufacture of their products.

These new cybersecurity requirements apply to all products with a radio connection, such as 4G, 5G, Bluetooth, Zigbee and Wi-Fi. Affected products include mobile phones, smartwatches, baby monitors, fitness trackers, wireless toys, smart TVs, connected streetlights, wireless sensors, charging stations, connected cars, drones, vending machines and more. Besides being aimed at ensuring better resilience of communication networks, RED-DA will also protect citizens' privacy and personal data, and prevent the risks of monetary fraud.

Apart from a very limited number of exceptions, all manufacturers, importers and distributors of products with a wireless radio connection on the European market must comply with the RED-DA from August 2025 onwards. Only medical devices (see next page) are exempt, plus – to a certain extent – civil aviation, motor vehicles and road toll systems.

Several **transitional provisions** are in place until 2025. These include some **key changes** from a cybersecurity perspective

Medical Devices Regulation (MDR)

For all manufacturers producing or selling medical devices in the EU, the existing Medical Device Directive (MDD) and the Active Implantable Medical Device Directive (AIMDD) are being replaced by the **Medical Device Regulation (MDR)**. The MDR originally entered into force in May 2017 and became applicable on 26 May 2021. Several transitional provisions are in place until 2025. These include some key changes from a cybersecurity perspective.

For custom-made implantable devices, the MDR significantly extends the scope to new sectors and entities, removes the distinction between OESs and DSPs, and addresses cybersecurity of the ICT supply chain. For all types of implantable devices, it introduces a list of seven key elements that all companies must address or implement, and envisages a two-stage approach to incident reporting.

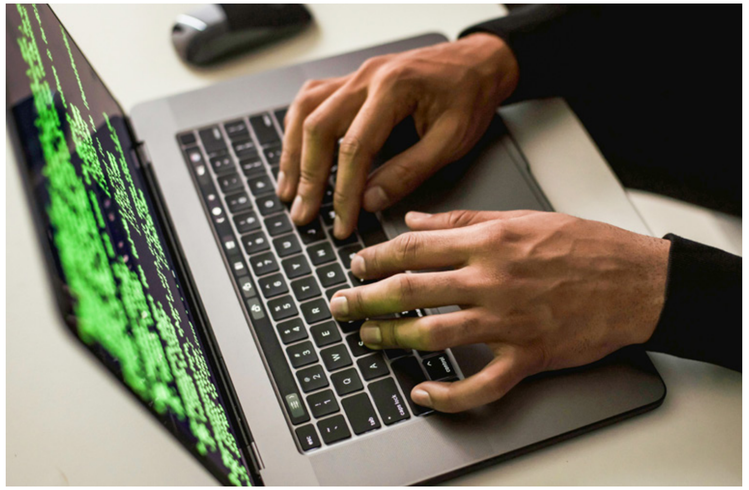
[...] manufacturers must ensure that **vulnerabilities are handled effectively** for the expected product lifetime or for a period **of five years**

Cyber Resilience Act (CRA)

In what can be seen as an extremely comprehensive and overarching piece of legislation bringing all of these aspects together, **the Cyber Resilience Act (CRA)** is currently being reviewed and updated by the European Commission. It provides a uniform set of mandatory, EU-wide cyber-security requirements for any products that have a digital element that enables connection to another device or a network. Because their connectivity makes them susceptible to cyberattacks, they will have to meet stricter security requirements.

The list includes private security cameras, connected doorbells, baby monitors, smart home assistants, smart watches, smart toys and Wi-Fi routers. When the CRA comes into force, manufacturers of these and other such systems and products will be required to take account of cybersecurity in the planning, design, development, production, delivery and maintenance phase. They must document all cyber-security risks, and they must provide clear and understandable usage instructions for products with digital elements. Manufacturers will also be required to report actively exploited vulnerabilities and incidents.

After the product is sold, manufacturers must ensure that vulnerabilities are handled effectively for the expected product lifetime or for a period of five years (whichever is shorter). This means that security updates must be installed automatically and separately from functional updates and must be made available for at least five years.



[...] Harmonised standards give you **peace of mind** that you are covered **across all Member States**

The Official Journal of the European Union is a good place to start for indications of which standards could be applied in the case of specific laws. In addition, a number of harmonised standards are particularly relevant in the context of cybersecurity. As an added bonus, harmonised standards give you peace of mind that you are covered across all Member States.
The most relevant standards are:

The design of IoT products

For manufacturers of consumer products that have Internet of Things (IoT) connectivity, for example, the **ETSI EN 303 645** is relevant. This global security standard covers the incorporation of cybersecurity into the design of IoT products.

The use of automation and control systems

For operational technology in automation and control systems, **IEC 62443** is an international series of standards that address the technical and process-related aspects of cybersecurity. The focus is on ensuring that the various stakeholders and roles – operators, providers of integration and maintenance services, and component/system manufacturers – follow a risk-based approach to prevent and manage security risks in the course of their activities. In other words, this series of standards relates to helping users to utilise end products in a cybersecure manner. IEC 62443 covers many of the aspects in the NIS2 and CRA.

Medical industry

IEC 81001-5-1 requires manufacturers of all kinds of software used in the health sector to take account of IT security in the software life cycle. IEC 81001-5-1 addresses many of the requirements of the MDR, and the legislation may even incorporate this standard eventually.

[...] some manufacturers may be tempted to issue **their own Declaration of Conformity** and then hope that they **don't get caught out**

Despite the increased focus on cybersecurity, the new and amended laws will still allow many manufacturers to state their compliance based on self-assessment. One notable exception is the MDR, which does not allow self-assessment at all.

Under the CRA, for example, only around 10% of products will fall into the Critical 'Class I' (e.g. password managers, network interfaces, consumer firewalls and microcontrollers) or Critical 'Class II' (operating systems, industrial firewalls and CPUs) category. Manufacturers of such products will be required to apply a standard and/or be assessed by a third party. The rest – accounting for approximately 90% of products (e.g. photo editing software, word processing, smart speakers, hard drives and computer games) – will fall into the 'default' category. This means that a Declaration of Conformity (DoC) is sufficient.

As a result, some manufacturers may be tempted to issue their own Declaration of Conformity and then hope that they don't get caught out. But given the ever-rising cybercrime statistics, do you really want to run the risk that your product is the weakest link that gives cybercriminals a way in... leaving you facing all the potential operational, financial, legal and strategic consequences?

An expert’s perspective gives you **objective new insights** into the your products and the **associated processes**

Third-party testing can be an attractive alternative to self-assessment. Working with a third party (‘Notified Body’) for testing and certification offers a number of benefits:

Credibility

In the case of a legal claim, the results from an independent test laboratory enable you to credibly demonstrate that you have fulfilled your legal obligations by taking all reasonable measures to minimise the risks.

Market positioning

Customers are increasingly seeking suppliers who support their own cybersecurity policies. And even if they don’t ask you for proof, you can set yourself apart by educating them on the risks and responsibilities, and subsequently demonstrating your proactive commitment to cybersecurity.

Future-proof your business

Cybersecurity requirements are here to stay. Certifying your products in line with today’s standards helps you to prepare for tomorrow. As a result, you can stay a step ahead of your competitors and benefit from first-mover advantage as the legislation continues to evolve in the future.

Independent view

An expert’s perspective gives you objective new insights into the your products and the associated processes. These insights can prove extremely beneficial in understanding your current level of cybersecurity and identifying gaps or continuous improvement opportunities.

The cybersecurity requirements in the EU will become **considerably tighter** over the next few years

The cybersecurity requirements in the EU will become considerably tighter over the next few years. Thanks to the NIS2, the RED-DA and the CRA, public and private sector users as well as consumers will have greater peace of mind when buying and using products with online connectivity. Forward-thinking manufacturers can start preparing for these developments by arranging third-party certification of their products in line with existing harmonised standards.

DEKRA is an EU Notified Body for the Radio Equipment Directive and is recognised for radio and telecommunications testing under the **IECEE's CB scheme.**

Besides testing and certification services, DEKRA also provides guidance on which legislation is most appropriate, advice on what the testing and certification process entails and how best to prepare for it, and support with understanding and evaluating the risks involved. Other opportunities include penetration testing by our cybersecurity experts, training, gap analysis and annual audits.

DEKRA Organisational & Process Safety **Contact**

DEKRA Organisational and Process Safety are a behavioral change and process safety consultancy company. Working in collaboration with our clients, our approach is to assess the process safety and influence the safety culture with the aim of making a difference.
In terms of behavioral change, we deliver the skills, methods, and motivation to change leadership attitudes, behaviors, and decision-making among employees. Supporting our clients in creating a culture of care and measurable sustainable improvement of safety outcomes is our goal.
The breadth and depth of expertise in process safety makes us globally recognised specialists and trusted advisors. We help our clients understand and evaluate their risks, and we work together to develop pragmatic solutions. Our value-adding and practical approach integrate specialist process safety management, engineering, and testing. We seek to educate and grow client competence in order to provide sustainable performance improvement. Partnering with our clients, we combine technical expertise with a passion for life preservation, harm reduction and asset protection.
We are a service unit of DEKRA SE, a global leader in safety since 1925 with over 48,000 employees in 60 countries and five continents. As a part of the world's leading expert organisation DEKRA, we are the global partner for a safe world. We have offices throughout North America, Europe, and Asia.

For more information visit
www.dekra-uk.co.uk

Would you like more information?

Contact