Enhancing EU Security Through the Cyber Resilience Act

In recent years, there has been a plethora of new European Union (EU) regulations covering technology and security. Among them is the Cyber Resilience Act (CRA), which will come fully into force in December 2027. How does this differ from all the other related Acts and Directives, and what do organisations need to be aware of? OpenSpace spoke to Cristian Michael Tracci from the European Cyber Security Organisation (ECSO) and Peter Kirkov, former National Cybersecurity Coordinator, Bulgarian Government, to find out.

Organisations selling technology-related goods and services in the EU marketplace are having to take account of a raft of recent and new Acts and Directives that place requirements on the way they operate and the security of their products. Among these are the Network and Information Security Directive 2 (NIS2), the EU AI Act, the Cyber Solidarity Act, the Critical Entities Resilience Directive and the Cyber Resilience Act (CRA). There are also vertical, or sector-specific, regulations such as the Digital Operational Resilience Act (DORA), which focuses on cybersecurity and ICT risk management in the financial sector.

Much attention has been focused on NIS2, which expands cybersecurity obligations for 'essential and important entities' (as defined in NIS2) and their supply chains. Of late, however, organisations have been broadening their attention to include the CRA in an effort to understand the requirements that this new regulation will place on them. Approved by the European Parliament and Council in October 2024, it will be fully applicable by December 2027, although some reporting obligations will begin in September 2026.

Why is the CRA needed?

Unlike NIS2, which applies to entities, the CRA applies to products: specifically, all products with digital elements, which are becoming more common in the consumer and business markets. These range from simple toys and components to networked robotic tools, autonomous vehicles and spacecraft. There can be security vulnerabilities in any software or hardware, meaning that any product with a digital element is a weak point that cyber criminals can exploit to carry out an attack, and this has become a concern for the EU.

Delia Ioana Spinu, Nexova Cybersecurity Legal Consultant, explains: "The Cyber Resilience Act addresses two fundamental problems. The first is the low level of cybersecurity of all products with digital elements, making them vulnerable to cyber threats and attacks. The second is that not only is there an

insufficient understanding of this by users, but in many cases they have very limited access to relevant information when they buy a product with a digital element. They simply don't know how safe it is – and how safe it continues to be over time.

"In some areas, manufacturers often don't provide regular security updates or timely updates, meaning that vulnerabilities that become known later on don't get fixed quickly or at all. Sometimes this is because in the absence of clear legal requirements, manufacturers are not currently held responsible for the cybersecurity of their products after sale. Additionally, investing in secure design and continuous updates is costly and manufacturers may opt to prioritise low consumer pricing and short-term profits."

Peter Kirkov, former National Cybersecurity Coordinator for the Bulgarian Government, explains why a low level of cybersecurity is a growing concern: "Ultimately, due to increasing digitalisation, this can have profound effects across the EU because so many things are now interconnected. In addition, you may not know your device is compromised because in some cases an attacker will want your device to continue functioning to use it to attack a third party."

With so many security-related regulations already in place or coming into force, the need for yet another one has been questioned in some quarters. But the CRA isn't simply repeating existing requirements in a different guise. Instead, because product security is different from organisational security, the CRA has been established as a complementary regulation to others that already exist. 'Ship and forget' is no longer going to be an option for any organisation producing products with a digital element in the EU.

What does the CRA cover?

According to the European Commission (EC): "The Cyber Resilience Act introduces mandatory

cybersecurity requirements for hardware and software products, throughout their whole lifecycle."[1] This covers all products with any digital element(s) and includes all related remote data processing components where "the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions".[2]

Manufacturers are obliged to ensure that[1]:

- Cybersecurity is taken into account in planning, design, development, production, delivery and maintenance phases
- All cybersecurity risks are documented
- Actively exploited vulnerabilities and incidents are reported
- Vulnerabilities are handled effectively for the duration of the support period
- Clear and understandable instructions are provided for the use of products with digital elements
- Security updates are made available to users for the time the product is expected to be in use.

A distinction is made between categories of products, which ultimately determines whether they can be

'self-assessed' by their manufacturer against specified standards or will need to be assessed by a third party. It's expected that around 10% of products will fall into the latter group, being subdivided into Important Products Class I and II, and Critical Products. The list of products that fall under Class I is long but includes many types of software including operating systems, plus hardware such as routers, switches and microprocessors. Class II products include, for example, firewalls and hypervisors, while Critical Products include hardware devices with security boxes, smart meter gateways and smartcards.

The current descriptions of categories are relatively broad, but this will be resolved in December 2025 when the EC will adopt an 'implementing act' that specifies the technical descriptions of the categories of products in each group.

Supply chains can be long and complicated, so it's essential that manufacturers and developers of software and hardware, including components, know their existing and target client sectors. Douglas Wiemer, Chief Technology Officer – Cyber, Starion and Nexova, notes: "How a component is going to be used may determine the level of assessment required. It's possible some manufacturers may choose not to sell into certain sectors or to specific organisations where the final product or environment is classified as Critical, to avoid the burden of additional assessment."

Software provided as part of a service is not covered by the CRA, as the NIS2 Directive (and other sectorial legislation) already requires that systems provided as a service or developed in-house meet equivalent technical requirements for cybersecurity. Open-source software is also exempt when distributed non-commercially by non-profit organisations, as are code contributions. But any open-source software used for commercial activities does fall under the CRA. Therefore any organisation using open-source software will be responsible for ensuring they are compliant. Smaller companies may find they need to seek external support to fully conform with the Act.

Some sectors are specifically excluded from the CRA's remit due to their specialised nature and existing sector-specific regulations. This includes products developed or modified for national security or defence purposes. The CRA does, however, cover the space sector (when not exclusively military).

Nexova's Delia Ioana Spinu says: "The main principles that are addressed in the CRA are cybersecurity by design and cybersecurity by default, and this applies as much in the space sector as elsewhere. For example, payload developers must identify all the threats in the design, including supply chain vulnerabilities and risks through physical access – even down to the level of ensuring passwords are sufficiently strong enough. Everything must be documented and up to date, and there need to be ways to enable security updates for the whole life cycle of the product or for at least 5 years."

Security considerations need to be embedded in every stage of a space programme or mission's life cycle, from design through development, deployment,

operation and decommissioning. In essence, this is no different from all other products covered by the CRA, but with so many companies likely to be involved in the supply chain, space is possibly one of the most complicated sectors in which to ensure full compliance with the new regulation – hence companies at all the stages in space supply chains need to start planning now, if this hasn't already been initiated.

Nevertheless, Peter Kirkov comments: "The space industry is very advanced technologically and as such they understand cybersecurity very well. They are almost certainly implementing security by design already and meeting minimum cybersecurity regulations because otherwise they would be putting their costly satellites at risk. So I don't believe it will be overly onerous for the space sector. They may need to introduce some more processes and paperwork because they will need to act on vulnerabilities if they are made aware of them by suppliers and report on any they incur.

"Despite the fact that satellites are very complex, their builders are, in effect, integrators of components and operating systems. However, it is the organisation that introduces a product to the EU market – be they manufacturer, distributor or importer – that has responsibility for CRA compliance. Therefore, if a company builds a satellite using modules from outside the EU, they will need to factor that compliance activity into their procedures."

Due in December 2025, the publication of detailed definitions of each type of product will be important for the space industry. In addition, Peter Kirkov notes that the cybersecurity aspects of the proposed EU Space Act[3], launched in June 2025, could override elements of the CRA for the space sector. As this Act was still in its public consultation period at the time of writing, and may only be implemented by 2030, the focus for now needs to be on the requirements set by the CRA.

Dealing with incomplete information

Although the CRA itself is now law, at the time of writing not every element related to the CRA was fully specified. Cristian Michael Tracci, Policy Analysis and

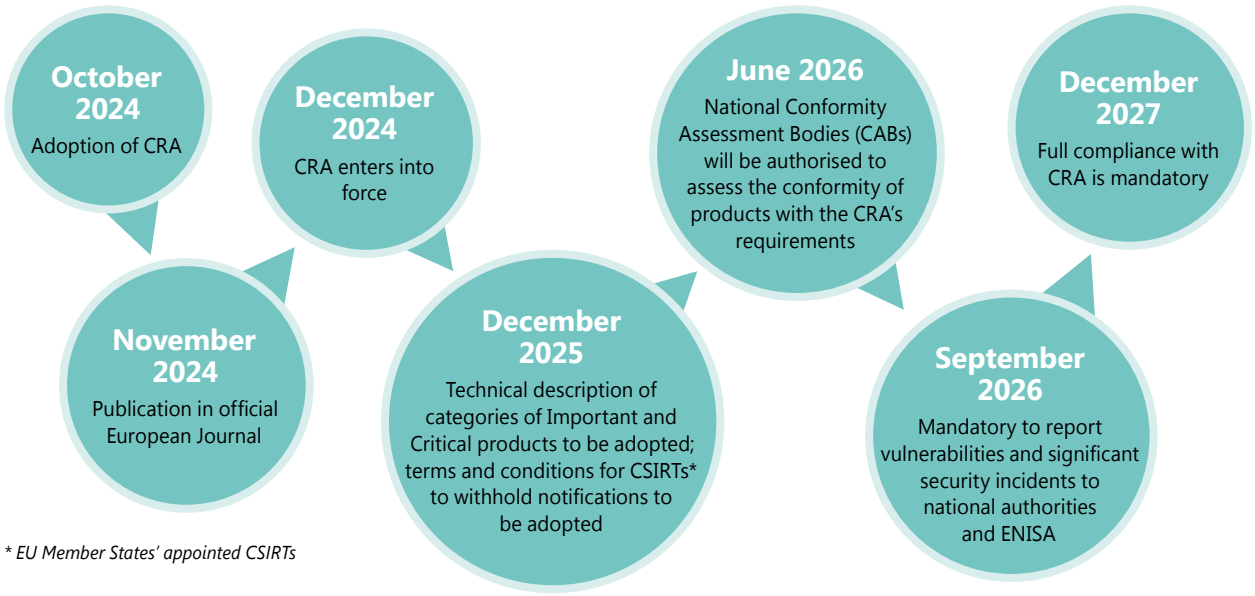
Outreach, Senior Manager, ECSO, explains: "There are still some aspects that have not yet been completely set out. For example, we're waiting for the standards to be developed and published [that organisations will need to meet to demonstrate compliance]. Overall, there will be 41 items within the standards, which is a huge task for the standardisation organisation to complete in a very short timeframe.

"And then it's unclear as yet whether the level of detail will be the same for any requirements where there is an overlap between two or more regulations – for example how user logins are secured – which might cause some complexity."

This interim period therefore presents challenges for manufacturers seeking to get prepared well in advance of the final deadline. Nexova's Douglas Wiemer adds: "It's possible that the EU Cybersecurity Certification Scheme[4] will provide a partial solution here. But while we wait for a full set of harmonised standards, there is currently no criteria for companies to measure themselves against in order to do any self-assessment."

Over the next 2 years, there will be a number of milestones for adoption of various elements related to the standard. It's important for manufacturers to be aware of these dates, but there are two key dates that they specifically need to prepare for. First, from 11 September 2026, it will be mandatory to report vulnerabilities and significant security incidents to national authorities and the European Union Agency for Cybersecurity (ENISA). From 11 December 2027, full compliance with the CRA is mandatory.

Even once the Act is mandatory, it is important to note that the regulation will only apply to products placed on the market before that day if they are 'substantially modified'. But what does 'substantially modified' mean? Not all security updates are regarded as a substantial modification. However, a modification may be considered substantial if an existing product (with digital elements) is changed – by physical or digital means – in a way that was not anticipated in the initial risk assessment, and that change either affects compliance with essential cybersecurity requirements or alters the product's intended purpose.



** EU Member States' appointed CSIRTs*

Post-sale requirements

One aspect that companies need to build into their business processes is that the requirements of the CRA don't stop once a product has been delivered. Instead, they will need to be compliant for a period after they are sold, during which time those companies will be expected to act upon any vulnerabilities that may be discovered.

Under the CRA, companies have to provide security updates for their digital products for a minimum of 5 years or the product's expected lifetime, whichever is shorter. Technical documentation must be continually updated during the support period as a minimum and, along with declarations of conformity, be available for 10 years after a product has been placed on the EU market.

Manufacturers must report any actively exploited vulnerabilities and severe security incidents to their appointed national Computer Security Incident Response Team (CSIRT) and ENISA within 24 hours. They may then need to provide further information within 72 hours and a final report within 14 days for vulnerabilities or within one month for severe incidents. They must also inform any impacted users – and, where appropriate, all users – in a timely manner of an actively exploited vulnerability or severe incident and, where necessary, provide details about risk mitigation and any corrective measures that they might deploy to mitigate the impact. (More details on this will be published in December 2025, including in what cases public notification can be delayed or omitted.) The aim is to ensure swift action to address vulnerabilities and mitigate the impact of security incidents, thereby improving the overall cybersecurity posture of products in the EU market.

Nexova's Douglas Wiemer points out: "Producers of commercial products will need to publish vulnerability advisories and make their clients aware of them, and that should flow through the supply chain very quickly. However, there are a number of inherent challenges and unknowns. For example, what happens when a vulnerability is identified in a previously evaluated and approved product that is being used by third parties along the supply chain? I believe the regulators are trying to mitigate the burden here, but it will be up to each company to decide what the perceived risk is based on their threats and assets, and therefore how this newly identified vulnerability will affect them. Overall, it comes down to responsible disclosure by the vendor and the risk management assessment of the buyer or user. The latter should look at the risk to their

infrastructure, how much risk tolerance they have and their understanding of the vendor's plans to address the vulnerability."

What do companies need to do now?

Although CRA-related standards don't yet exist, companies should be evaluating how the Act will affect each one of their products so that they can be ready to assess them, or have them assessed, when the standards are published.

The first thing companies need to do is to understand whether they are impacted by the Act or not. In essence, all products with a digital element, including ones that don't process data themselves but link to remote data processing, come within the scope of the Act. There are some exceptions and there are also prescriptive lists of categories of products that require more stringent conformity assessments.

The next step is to undertake a risk assessment to identify the actions needed to meet the requirements for compliance.

Nexova's Douglas Wiemer concurs that "there is no single risk management framework that every company should use" but suggests that companies could refer to a series of publications by ENISA related to risk management frameworks and standards.[5]

"It's all down to taking a risk-based approach that takes into account multiple aspects," says Nexova's Delia Ioana Spinu. "These include the criticality of the product within the sector it's going to be used in, the needs of that sector, the risks it may be exposed to, the likelihood of an incident and then the impacts, severity and consequences of any incident. Based on that assessment, manufacturers should tailor their approach – there is no universal methodology that can be applied in every case.

"Another way to consider it, especially if you are using components or software from other manufacturers, is to take the risk-based approach currently used by those implementing cybersecurity across their organisations. What do I need to protect? Why do I need to protect it? What's the threat? It's not solely about conforming with the obligations set by national or international laws – it's about taking appropriate measures to enhance your organisation's resilience, including avoiding any sanctions associated with failing to take appropriate measures related to the products you sell."

If products are found to be non-compliant, the relevant authorities could insist that they be made compliant, restrict their availability or order that they be withdrawn from the market or even recalled. There will also be provision for financial penalties for non-compliance reaching up to €15 million or 2.5% of a company's global annual turnover, whichever is higher. Other violations, such as those related to documentation or reporting, can incur fines of up to €10 million or 2% of global turnover, while providing

misleading information could lead to fines up to €5 million or 1% of global turnover.

Ultimately, the impact on each company may vary substantially, depending on where they are in any supply chain and how complicated their products are. If a component has already been certified or assessed to be OK, it should be possible to reuse the evidence put together by that component's supplier. However, companies will still need to do a risk assessment because they are integrating it, along with other components, in something new. Part of that assessment should look at whether it's better to remove a non-compliant product or if it will be less damaging to keep it and try to fix any related vulnerabilities.

Towards a more secure tomorrow

The CRA specifically focuses on products, including both hardware and software, which in many respects differentiates it from other security-related regulations. However, this does not mean that all preparatory activities can, or should, be distinct from ongoing work to meet the requirements of other EU Acts and Directives.

ECSO's Cristian Michael Tracci advises: "The EU aims that the CRA should complement other regulations such as NIS2. It's not the will of the regulator to make it overly complicated but there are likely to be some overlaps because they are tackling the same objective of improving security from different perspectives. Some regulations approach it from the aspect of an organisation's practices and procedures, while the CRA is about demonstrating that the products themselves are secure. Nevertheless, there are likely to be overlaps in terms of security-related practices and procedures to reach those goals."

For the space industry, the proposed EU Space Act will also impact security requirements in future, with resilience through tailored cybersecurity requirements being one of its three key pillars. But again, it is likely

the EC will want to avoid stifling the EU space sector by introducing another regulation that makes it overly complicated to do business.

The upshot is that while compliance with the CRA is likely to require separate, focused risk assessments and associated changes to products and processes, it is essential that all organisations shift towards seeing cybersecurity as a fundamental part of how they operate.

Ensuring cybersecurity is viewed by everyone as a core part of business, rather than an add-on or the responsibility of just one person or team, will make compliance – not just with the CRA but also with NIS2 and other security-related regulations – seem entirely logical rather than a burden.

Resources and sources

For more information on the EU CRA, including the EU CRA factsheet and Q&A, visit: digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Sources: See page 86

Classes of products in the scope of the CRA

Products will fall into different categories based on their risk level and criticality, with specific types classed as Important or Critical. Further information can be found in the Annexes of the Regulation and detailed definitions are due to be published in December 2025.

Important Class I

- Identity management systems
- Standalone and embedded browsers
- Password managers
- Antimalware software
- Products with virtual private network (VPN) functionality
- Network management systems
- Security and event management (SIEM) software
- Boot managers
- Public key infrastructure (PKI)
- Physical and virtual network interfaces
- Operating systems
- Routers and modems intended to connect to the internet
- Microprocessors and microcontrollers
- ASICs and FPGAs (application-specific integrated circuits and field programmable gate arrays)
- Smart home products and assistants
- Connected toys
- Wearables

Important Class II

- Hypervisors and containers
- Firewalls, intrusion detection/prevention systems (IDS and IPS)
- Tamper-resistant microprocessors and microcontrollers

Critical

- Hardware devices with security boxes
- Smart meter gateways
- Smartcards or similar