DIGITALEUROPE

24 MAY 2022

Building blocks for a scalable Cyber Resilience Act

Executive summary

Cyber resilience is central to Europe's social, economic and political future. This is reflected in the name of the European Commission's upcoming flagship proposal for a Cyber Resilience Act (CRA).[1] While the name is all-encompassing, the proposal should focus on solving the most pressing issues emerged so far – notably, around connected devices – as opposed to including too much too soon.

Our survey of experts last year has highlighted that as much as 70 per cent of baseline cybersecurity requirements are common across all connected products, and that horizontal legislation such as the CRA is the most appropriate way to address them.[2]

The proliferation of piecemeal cybersecurity requirements in different laws in recent years makes legal and technical compliance more difficult for companies, and as a consequence exposes our society to heightened cybersecurity risks. This is the fundamental problem that the CRA should aim to solve by regulating connected products horizontally, rather than adding another layer of requirements.

In order to enable a scalable CRA, the European Commission's proposal should:

- Put in place *lex generalis* baseline requirements for the cybersecurity of all connected products. The proposal should articulate its relationship with other relevant legislation and stipulate which law prevails.

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en.

[2] See DIGITALEUROPE, *Setting the standard: How to secure the Internet of Things*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/09/DIGITALEUROPE_Setting-the-standard_How-to-secure-the-Internet-of-Things.pdf.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- Focus primarily on digital tangible products currently governed by EU product regulation. It is these products that suffer from most legislative overlap and incoherence, and this is where most protection gaps can be remedied. Similarly, the CRA should stipulate requirements on embedded software, which is necessary for a product's intended function.
- By contrast, the CRA should not cover 'standalone software' nor 'ancillary services,' both of which function irrespective of a specific tangible product and are not suitable for the same legislative treatment.
- The proposal should allow for a key role for product manufacturers as well as for obligations of relevant economic operators, including third-party suppliers. This is especially relevant for software. Through obligations on manufacturers and relevant economic operators, the CRA can provide a coherent lifecycle framework centred around secure development and production processes, coordinated vulnerability report management, and transparency about security software updates or alternative mitigations.
- The CRA should set out general legal requirements that can be detailed at technical level through harmonised standards. The latter should be based on a number of relevant international cybersecurity standards, either already existing or under development, and would allow for self-assessment building on stringent market surveillance. Self-assessment by the manufacturer is vital to enable scalability of assurance across the myriad devices that will be in scope.
- At the same time, the CRA should enable links with the Cybersecurity Act,[3] in order to avoid duplication and leverage certification schemes. Notably, by recognising voluntary third-party certification as an alternative way to demonstrate compliance when companies have chosen the certification route, or where specific markets request complementary or higher requirements through certification.
- The CRA's requirements should apply after a sufficient transition period in order to allow for the development of the necessary harmonised standards, facilitate synchronisation with other pieces of regulation, and enable companies to adapt their products.

[3] Regulation (EU) 2019/881.

Table of contents

Solving the regulatory overlap

Cybersecurity is a key prerequisite for a successful digital economy and society. Due to the increased importance of cybersecurity, there has been a huge increase in legislative requirements concerning cybersecurity. This has resulted in a piecemeal approach to date, with an ever-growing number of existing or proposed legal acts aiming to regulate products or organisations. Examples of this include:

- A delegated act under the Radio Equipment Directive (RED) with requirements relating to the protection of personal data and network resources, and against fraud, for wireless products;[4]
- A proposed Regulation on machinery products, with requirements for protection against corruption;[5]
- The proposed AI Act, setting out cybersecurity requirements for high-risk AI systems;[6]
- The Medical Device Regulations,[7] setting out minimum requirements concerning IT security measures for all medical devices incorporating electronic programmable systems and software considered a medical device, as well as other vertical/sectoral legislation;
- A proposed General Product Safety Regulation extended to cybersecurity risks having an impact on safety;[8]
- Proposals related to security issues, such as operating system updates and roll-back of updates, emerging in ecodesign legislation such as the proposed Lot X Regulation;[9]
- Provisions related to software updates in the Digital Content and the Sale of Goods Directives;[10]

[4] Commission Delegated Regulation (EU) 2022/30.

[5] COM(2021) 202 final.

[6] COM(2021) 206 final.

[7] Regulations (EU) 2017/745 and 2017/746.

[8] COM(2021) 346 final.

[9] See DIGITALEUROPE, *Technical annex on operating system update requirements in proposed Lot X Regulation*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2022/05/DIGITALEUROPE-Technical-annex-on-software-updates-for-Lot-X-09.11.21.pdf.

[10] Directives (EU) 2019/770 and 2019/771.

- The Cybersecurity Act, establishing a cybersecurity certification framework for products and services; and
- Risk management and incident notification obligations for essential and important entities under the reformed EU framework for the security of network and information systems (NIS2),[11] as well as, among others, for the financial sector under the Regulation on digital operational resilience for the financial sector (DORA).[12]

In this context, any product with digital elements will likely be subject to more than one law stipulating cybersecurity obligations, directly or indirectly.[13] Tackling cybersecurity under various guises – and by different names – across multiple legal instruments will create legal uncertainty and put unnecessary burden on companies. What is worse, it will lead to incoherent outcomes that work against an increased level of cybersecurity for consumers, businesses and government users.

Users of connected technology need effective protection from cyber risks. Because basic cybersecurity risks and requirements are largely common across product categories, security regulation is most effective when it is consistent and horizontal across any internet-connected product.

The announced CRA is an opportunity to create such coherence by regulating the cybersecurity of internet-connected products horizontally. Should it instead add another layer of requirements, the CRA would exacerbate the problems it sets out to solve.

The CRA must provide market actors and surveillance authorities alike with the necessary legal certainty, providing a level playing field for all manufacturers regardless of their country of origin. To this end, it should become *lex generalis* concerning baseline requirements for the cybersecurity of connected products. It should explicitly articulate its relationship with other legislation incorporating similar requirements, and stipulate which legal act prevails.

This includes existing vertical/sectoral legislation such as automotive or medical devices as well as, crucially, the RED delegated act. The continued existence of an RED delegated act once the CRA is in place would fundamentally work against the CRA's coherence objectives, and we therefore urge that the RED

[11] COM(2020) 823 final.

[12] COM(2020) 595 final.

[13] We refer to the concept of 'good with digital elements' as outlined in Art. 2(5)(b) of the Sale of Goods Directive (Directive (EU) 2019/771). However, while this is helpful for a general approach, we believe that this concept needs to be further elaborated for applying specific requirements. This also applies to the term 'ancillary services' as introduced in the Commission's call for evidence of the CRA.

delegated act should be repealed by the CRA. Clarification with respect to conflicting requirements from other regimes that may undermine cybersecurity, such as ecodesign, should be contemplated as well.

Scope

Cybersecurity is by nature holistic – it is ultimately about systems consisting of different elements, tangible and intangible, processes and services. This poses a legislative challenge, because all these elements will be very difficult to cover in a one-size-fits-all approach.

Similar to the proposed Data Act,[14] the CRA's scope should focus primarily on tangible, movable products. It is these products that suffer from most legislative overlap and incoherence, and where most protection gaps can be remedied. By contrast, the CRA should not cover products that naturally belong to critical infrastructure, such as telecoms equipment, which are better dealt with separately.

Focus on connected products

The CRA's prime objective should be to provide one set of cybersecurity rules for all digital tangible 'connected products' (as defined below) currently governed by EU product regulation – from general-purpose computing to medical devices or security equipment for buildings. This approach will include all IoT devices relevant for a cybersecure society, and will remedy the legal uncertainty created by the current piecemeal legislative approach.

To cover such wide scope, the CRA must be generic enough to be applicable and specific enough to be effective. To this end, it should outline a set of essential baseline security requirements, to be applied selectively according to a risk management assessment of a device's intended use, taking into account the ecosystem or 'operational environment' in which the device will be placed. This is because threats and related risks can be extremely different between products used in a business environment, such as an IP network in a factory, and those used in a consumer environment, such as a tablet in a home network.

DIGITALEUROPE proposes that the CRA should govern 'connected products,' with the following definitions:

- Connected product: A finished product that is intended to communicate directly or indirectly over the internet.

[14] COM(2022) 68 final.

- Finished product: A product usable for its intended functions without being embedded or integrated into any other product. Components of a device, such as a processor or a sensor, should be outside the scope as security functionalities need to be assessed holistically.[15]

These definitions are compatible with the widely acknowledged ISO definitions,[16] and reflect the recent RED delegated act. Our definition of 'connected product' broadly coincides with that of 'hardware product,' intended as a digital tangible product, in the context of the Commission's call for evidence for the CRA. We believe that these definitions, combined, provide a better alternative to the definition of 'hardware product.'

Building on the product's intended use and a risk assessment, more specific requirements or more demanding conformity assessment procedures can be used to target applicable cybersecurity risks. Devices with more advanced computing capabilities (e.g. general purpose compute such as laptops, and IT devices) can and should enable more advanced protections than constrained IoT devices (e.g. a smart dog collar).

With a wide scope on products, it will be crucial for the CRA to differentiate between business-to-consumer (B2C) and business-to-business (B2B) use, and to account for different risk environments. Risks and mitigation options are fundamentally different, and the CRA should draw a clear distinction between the two. As specific requirements can depend on the domain or sector, these should be detailed by means of vertical standards.[17]

The proposed focus on connected products would allow for a key role of the device manufacturer, but also for obligations of relevant economic operators, which is especially relevant when software is concerned.

Software

In addition to connected products, as defined above, the CRA should cover software that is embedded into a product. We define 'embedded software' as 'software that is necessary for the intended function of a connected product.' This definition includes software physically stored in a product and closely connected to its hardware, e.g. firmware, driver software of a motor, and operating

[15] Assessing cybersecurity of products at the highest aggregation level prevents double regulation. For holistic aspects beyond the finished product, see the 'System level' section, p. 10 below.

[16] ISO/IEC 20924.

[17] For instance, a smart sensor that only communicates indirectly with the internet through a gateway may need to address different cybersecurity risks than the gateway. Also, as outlined above, devices with more advanced computing capabilities can and should enable more advanced protections than constrained IoT devices.

systems.[18] Additionally, it encompasses software in a wider sense, notably software that is not physically present in a product, such as patches that can be embedded at a later stage to support a product's intended use.

General-purpose software functioning irrespective of a specific tangible product ('standalone software') should be out of scope.[19] Examples would be for instance a weather app for a smartphone, text editor software for a laptop, or a video conference app in a conference room controller.

By the same token, the broader category of services ('ancillary service' in the call for evidence) should not be covered.[20] Services are fundamentally different from goods or software, and are performed in a manner and over a timeframe that are largely unrelated to any specific device, e.g. cloud, streaming or financial services. Consequently, legal requirements applicable to devices and their embedded software will not be relevant for services.

When embedded software is provided by a third party to the manufacturer of the connected product, the CRA should provide principles for a fair balance of responsibility between the manufacturer and the software provider. It should also provide a level playing field regardless of country of origin.

Covering the lifecycle

In a dynamic threat landscape, fixed-point-in-time test conditions on the product alone can only partly ensure security. To stay future proof, the CRA must stipulate baseline security objectives also beyond the product itself.

Importantly, in addition to essential requirements on products, the CRA can also stipulate obligations on manufacturers or other relevant economic operators. This approach is fully in line with product regulation under the New Legislative

[18] We believe our proposed definitions increase legal certainty compared to the definitions contained in the public consultation on the CRA, available at https://ec.europa.eu/eusurvey/runner/European_Cyber_Resilience_Act?surveylanguage=en.

[19] We note that at present, software separate from products is only envisaged in the medical device regulations (Regulation (EU) 2017/745 and Regulation (EU) 2017/746), but only to the extent that such software is 'specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device.' General-purpose software is explicitly excluded.

[20] While the Data Act also covers 'related services' in its scope, this is due to the different goal of that proposal, which aims to facilitate access to data. This may also involve the data generated in the use of a digital service offered with the product. Such digital service, however, will typically not have any cybersecurity impact, which is what the CRA should address. To the extent that there is a cybersecurity impact on the product, the inclusion of embedded and non-embedded software that supports the product's intended use will suffice.

Framework (NLF),[21] and addresses conformity needs before and after the moment of placing products on the market or putting them into service, whilst also reflecting established licences allowing continued code development to enhance security and functionality. Of course, care has to be taken to ensure consistency in the definitions of economic operators across relevant legislation.[22]

Through obligations on manufacturers and relevant economic operators, including third-party suppliers, the CRA should provide a coherent lifecycle framework building on three elements:

- Secure development and production processes in accordance with secure-by-design and by-default principles (to be detailed in harmonised standards);
- Coordinated vulnerability report management (to be detailed in harmonised standards); and
- Transparency about the minimum duration for the provision of security software updates or alternative mitigations (to be detailed in legal agreements).

Bolstering awareness and best practice relating to product development, vulnerability management, and transparency about security software updates can prevent major security risks.

Adherence to processes such as secure development lifecycle (SDL), building end-to-end security into app development (DevSecOps) or vulnerability report management is essential to improve security. Pursuant to the baseline security objectives stipulated by the CRA, manufacturers should be able to select the relevant risk-based processes, ideally based on harmonised standards or established industry-led frameworks. These baseline approaches to security will provide necessary foundational capabilities.

Software updates are an important element of ensuring security beyond placement on the market. A horizontal regulation, however, should not stipulate a specific duration for the provision of updates, as this will vary according to product and operational environment. Stronger transparency obligations to

[21] https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en. This is true, more generally, of EU product regulation contemplating the CE mark, with conformity assessment procedures defined in Decision No 768/2008/EC. The NLF is often misunderstood as ending after placement on the market. On the contrary, placement on the market is an important reference point but does not exclude subsequent obligations, for instance related to market observation of product failures.

[22] We note for instance that the concept of 'vendor' as introduced in the call for evidence is different from the NLF definitions, as it applies to distributors and manufacturers alike. It is also not coherent with the definition of 'seller' in consumer sales law. We propose aligning the CRA with the NLF concepts.

disclose the duration of available support (while maintaining flexibility to determine and adjust it) will create the right balance between customer needs and affordable solutions. The CRA should recognise that manufacturers' obligation should only be to provide software updates, as their adoption usually lies with the user.

Regardless of the development model (proprietary or open source), there is a need to ensure, in accordance with the relevant risk-based process, extensive curation, security screening and quality assurance testing prior to release, as well as subsequent tracking of developments on product components during the lifecycle. From this perspective, the CRA should recognise existing best practice in software vulnerability management and disclosure that is standard in the relevant industry, as well as collaboration within security and developer communities to ensure timely and effective patches.

System level

Device-based requirements and obligations on manufacturers alone may not cover all security aspects. As seen above, to cover a manufacturer's supply chain, the CRA should acknowledge that other economic operators are relevant and may bear responsibility.

Moreover, the network or system level in which the device is included is naturally of high relevance. Certain mitigation measures (or compensating controls) such as monitoring or segmentation of devices, are best resolved at the level of network or system configuration, integration or operation.

This being said, the CRA should solely focus on connected digital products. The network or system level can be considered by defining in the CRA a mechanism allowing delegation of some security features to a network counterpart or be factored in by a transparent, legally certain reference to other legislation that already addresses the system level, such as NIS2.

The connection could be construed by stipulating product-level requirements that allow for these mitigation measures or compensating controls. One example could be the interface with network-level security, making it possible for the device to be identified, monitored and managed. Details could be provided in harmonised standards, based on existing international standards.[23]

[23] See for instance the system-level aspects in IEC 62443-3-3.

Harmonised standards

The use of harmonised standards has a long and successful history in EU product legislation under the NLF. Its key strength is that it allows general legal requirements to be detailed at the technical level.

A very good example of this is the EMC Directive,[24] whose extremely broad scope is made possible by allowing detailed product-specific requirements to be managed at standardisation level. The same scalable approach to harmonised standards should be adopted by the CRA, given its ambition to ensure coherence across a wide range of products with digital elements.

Harmonised standards can leverage industry's technical expertise to support market needs and increase adoption, allowing effective incorporation of sector-specific needs on top of the horizontal requirements established by the CRA. Another key advantage of addressing technical details by reference to harmonised standards is that broad consensus and global acceptance can be ensured.

Harmonised standards for the CRA must not conflict with – and indeed, should be based on – internationally recognised cybersecurity standards, such as:

- The widely used ISO/IEC 27001 (information security management);
- Draft ISO/IEC 27402 (DIS) (IoT products), soon to be finalised;
- ETSI EN 303 645 (IoT consumer products);
- ETSI TS 103 732 (consumer mobile device) ;
- ETSI TS 103 848 (home gateway products);
- IEC 62443 (industrial automation and control systems and products);
- ISO/IEC 29147 (vulnerability disclosure);
- ISO/IEC 27034 (application security); and
- The GSMA IoT Security Guidelines for Endpoint Ecosystems.

These standards already cover a vast number of relevant requirements, and their early consideration in the CRA's essential requirements and obligations on economic operators would allow for a much faster development process for the necessary harmonised standards.

[24] Directive 2014/30/EU.

Harmonised standards allow for self-assessment by the manufacturer as well as for self-certification.

Conformity assessment

Self-assessment with harmonised standards

Safety legislation applicable to everyday products – such as the Low Voltage Directive (LVD)[25] – has proved self-assessment by manufacturers to be a demonstrable, efficient and risk-based approach to ensure safety for consumers.

Particularly given the broad spectrum of digital products that will come into scope, the same approach should be used with regard to cybersecurity under the CRA.

Self-assessment underlines the principle that manufacturers must guarantee and be responsible for the safety – and in this case, the cybersecurity – of their products. Companies who choose to rely on third parties should equally have the right to do so.

As with product requirements, the associated risk is also key in conformity assessment. While third-party assessment can be relevant for high-risk environments, we are convinced that well-performed self-assessment is the appropriate method for most connected products.

To be effective and secure, however, self-assessment must be accompanied by two important conditions:

- Clear technical requirements against which the assessment must be performed. Here, the experience of the LVD shows that these requirements can best be laid down in harmonised standards; and
- Effective post-market surveillance (see below).

Certification

Cybersecurity for ICT products can also be evidenced pursuant to voluntary certification schemes adopted under the Cybersecurity Act. For industrial IoT, certification schemes already exist under IEC 62443.

The crucial question is how obligations under the CRA relate to possible schemes under the Cybersecurity Act.

[25] Directive 2014/35/EU.

Where companies have chosen certification by third parties, it is vital for the CRA to include a flexible mechanism to avoid duplication and allow for a modular approach leveraging certification schemes.

Similarly, for markets requesting complementary or higher requirements, voluntary third-party certification should be accepted as an alternative way to demonstrate compliance.

Stringent market surveillance

A law without enforcement is just good advice. Conformity assessment – by both vendors and third parties – must be seen in conjunction with effective market surveillance.

For market surveillance to be effective when it comes to cybersecurity, the necessary competences need to be built up. This is especially the case because of the important role that processes play in cybersecurity, going beyond the traditional product-based expertise of market surveillance authorities and the global nature of such processes and products.

Successful enforcement should thus leverage the current framework for market surveillance and compliance of products covered by Regulation 2019/1020.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Zoey Stambolliu

Manager for Infrastructure and Security Policy

zoey.stambolliu@digitaleurope.org / +32 498 88 63 05

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Banco Santander, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, Danfoss, Dassault Systèmes, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK