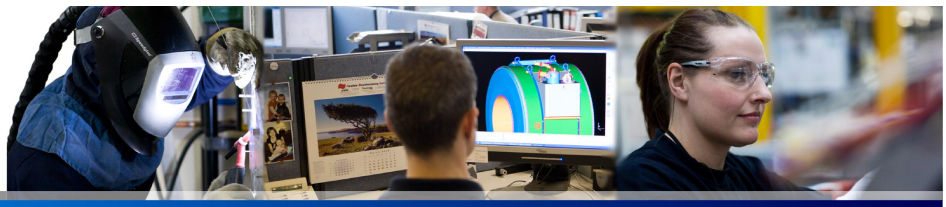

CYBER RESILIENCE ACT

Tuesday 28 February 2023

18h00–18h30 Cocktail Reception 18h30–22h00 Dinner Debate
Restaurant 12th Floor, Spaak Building
European Parliament

WELCOME & INTRODUCTION BY THE CHAIR

Vlad-Marius BOTOŞ MEP, (Renew Europe, Romania) Vice Chair Regional Development Committee, Committee on the Internal Market & Consumer Protection

It is a pleasure for me to host this event on cyber-security together with European Manufacturing Forum, an organization that is very active in establishing contacts between the European policy makers and the stakeholders. It has been organised jointly also with ZVEI.

We will be talking today about cyber-security, a subject that will be more and more important in the years to come since we are more connected, more digitalized and an increasing number of products are using new technologies.

I have to mention that I am Co-Rapporteur on the Product Liability Directive and this will include also the connected products, the cyber-security aspects.

EUROPEAN COMMISSION - OVERVIEW OF THE ACT

Lorena Boix Alonso, EUROPEAN COMMISSION, DG CONNECT, Director, Digital Society, Trust & Cyber-security
(Points noted from her presentation)

We have been really engaging a lot with industry and I must say that we are extremely thankful for that. It would have not been possible to have the proposal as it is without your input.

Because it is a new thing for you and also for us. It was the first time we were preparing this type of more prototype piece of legislation so we are really thanked you.

I think that I also do not need to convince this audience of the importance of Cyber-security.

There are a number of events that have made Cyber-security to be, I would say, finally, at the top of everybody's agenda.

We started with the pandemic which has increased the number of attacks, and the attacks on attacks. Then we had the work aggression, you have all types of series, whether the cyber-attacks have increased or not. And what is clear is that there is much more awareness. And we will have the economic situation that derived from these two events that has also an impact on cyber-security.

Today, as you know, we have a lot of ransomware attacks, we have a lot of activism. It is said that every eleven seconds, another organisation is hit by a ransomware attack. And we have had, in 2021, cyber-criminals who were able to leverage hacked devices allowing 9.75 million attacks worldwide.

So, we are facing a big challenge, as you know, with a lot of supply chain attacks. And these have an impact on society and also on the industry and in particular on SMEs.

These has created an impact on cyber-security policy as well.

I would have never imagined two years and a half ago when I was appointed that I would be so busy. At the time we had the the Network and Information Security Directive (NIS 2) on measures for a high common level of cyber-security across the Union to go. We were happily trying to implemented the Cyber-security Act.

And I do not know if you read yesterday's news but the Cyber Resilience Act is not going to be the last piece of legislation of this mandate. We announced the Cyber Resilience Act and the Cyber Skills Academy. So, we will keep you busy until I do not know when.

So, what are we doing? What is our main focus to protect society against cyber-attacks?

- We are trying to protect physical infrastructures,
- We have the Critical Infrastructure Recommendation of the Council.
- We are trying to reinforce the supply chain and
- We are also trying to strengthen our operational capacities in case of a large-scale cyber-attack if we have a big crisis.
- And this is why the Cyber Solidarity Mechanism has been announced yesterday

All of this is very nice, but there was a missing element in all of this, because if all the cyber-attack are possible it is because the devices have vulnerabilities. Except for phishing attacks, all of the types of cyber-attack come from the exploitation of vulnerabilities.

And most of the exploitation of the vulnerabilities come from software components and stand-alone software. We have a very important agency like the Cyber-security Agency that has identified the top 15 exploited vulnerabilities in 2021. Almost all of them are software.

I do not think that I need to explain to you what the Cyber Resilience Act is, but maybe what I can do is remind you a little bit the philosophy behind.

For us it is very important that it is a horizontal legislation so that we try also to help industry by avoiding plenty of sectorial type of legislation. The idea is that of course, for safety reasons, cyber-security becomes a part of the DNA of any hardware and software that is put in the market.

We would like, and I hope that is the case, that manufacturers see this piece of legislation not as a burden. Not only as something that is necessary but also maybe as an opportunity to boost use competitiveness. This is the first ever legislation and I think that the European Union can be an example and it will be a model worldwide.

Of course, an international point of reference not only as far as the legislation is concerned but also as far as standards are concerned. We all know how important this is for industry.

So, an EU standard based on the Resilience Act will facilitate its implementation but also it will be an asset for the EU cyber-security industry in the global market.

Of course, we have tried to be balanced. In one hand we have tried to rebalance the responsibilities that today are mainly on the users to rebalance and put a little bit more of responsibility on the manufacturers. That was necessary.

The same debate is taking place on the other side of the Atlantic with the rebalancing of responsibilities. But we have tried to do it in a way that is proportionate. So, I am sure now with the legislative proposal we are going to be proportionate.

You can decide what is the level of the requirements in your products.

The idea was also to be future proof and open to new technical solutions. But also, to constitute the basis of the standardisation work that then will translate all these requirements in something which is implementable.

We also think that it will be good also for SMEs. We know it is a challenge. It is a challenge for them as victims of cyber-attacks and it is a challenge, respecting the conditions and requirements. But in a way it is putting them at the same level as big companies.

So, in a nutshell what I want to say is that this is good for competitiveness as well.

Now, where are we in the legislative process?

We were the most important people. We were preparing the proposal but now the most important people are the people in this House, the Parliamentarians, and the Council.

We are here to help and to support the legislative negotiations.

But you also have a very important role to play.

We are very happy with the reactions we have to the consultations that we made after the publication of the proposal. We had more than 130 responses and submissions, that are being analysed very carefully by my team. And that I am sure they will be very helpful also to support the work of the co-legislators.

I think now you know better than me what are the key points, the key issues that are for debate.

One of them of course, is the scope of the proposal and also the clarity of the scope:

- Are we sufficiently clear on who is in who is out etc?
- Also, a lot of debate of course on the reporting obligations
- What should be reported, and to whom?
- Is it good to report certain things or not?
- All the debate on reporting on vulnerabilities is there. And for MEPs it is very important and we agreed
- Also, the clarity of the criteria, informing the critical product
- About the practical work on the conformity procedure
- SMEs - it is not surprising that there is a lot of debate about how SMEs will cope with that and how we can support both in the legislative proposal but also outside of the legislative proposal with support, financial support and other.
- And last but not least, extremely important the standardisation. It is going to be key. It is very important and we need to make sure that our standardisation is ready for the challenge and that we take the right approach. Of course, on the standardisation process as we know it is something that takes time and we are not waiting. We have started already some work in the mapping.

So, we are working very closely with the support of the European Research Centre and the European Union Agency for Cyber-security (ENISA). So that we can map what is already there, including international standards and we can do a proper gap analysis.

So, this is going to be very important and we really wanted to start now. So that when the legislative proposal enters into force, we have done already a lot of work.

Now, we really hope that the legislative negotiations will be quick, because we need this piece of legislation. What we are getting now for the moment is a lot of support.

I have not heard anybody from anywhere putting into question the concept of the proposal, the objectives and the fact that there is a need for this proposal. And that for me it is a big success taking into account the innovative character of this proposal.

IMPLICATIONS FOR EUROPEAN MANUFACTURERS

Marcel Hug, ZVEI, German Electro & Digital Industry Manager Cyber-security & Strategy

Call For a Realistic Implementation Approach.

The Cyber Resilience Act [CRA] is the right approach, but it needs the right "transition strategy" to work.

In the light of the proliferation of a fragmented regulatory landscape regarding cyber-security, the ZVEI is a strong long-time proponent for a horizontal cyber-security regulation for products within the proven New Legislative Framework (NLF). Therefore, we welcome in principle the coherent proposal of the CRA, as it follows the logic of the NLF and only adds some needed limited requirements in the life cycle, especially the establishment of a vulnerability management process, in a considerate manner.

Positions of the German Electro and Digital Industry:

- Make the CRA the central reference point for product cyber-security requirements and align the interplay with other regulations, including those of the new machinery regulation (esp. reg. Annex III, section 1.1.9), the General Product Safety Regulation and the AI-Act. Also include the repeal of the delegated act under article 3 (3) d,e,f of the Radio Equipment Directive (RED) in the text of the CRA to avoid double regulation.
- Ensure a realistic transitional period and transition strategy, potentially through a staggered approach, for a successful implementation through the cascade (comp. fig), including the development of hEN, their fast assessment and listing.
- Clarify the definitions & scope of the Regulation: focus on products, which are really able to exchange data (bidirectionally); add an exemption regarding spare parts to allow for the continuous use of long living goods. Add missing definitions and streamline and clarify the content of the Regulation to ensure unambiguity for the development of the harmonized standards (hEN) as well as for the economic actors concerned.
- Choose a more differentiated approach to critical products with digital elements by amending the too broad classification in Annex III and differentiate between components and systems. Delete art. 6 (5) and encompass "highly critical products" in the third-party conformity assessment procedures acc. to art. 24 (3).
- Optimize the connection of the obligations to the manufacturer and essential requirements for an effective and efficient implementation. Especially amend essential cyber-security requirement 1 (2) in Annex I to reference the vulnerability handling requirements and not to address hypothetical vulnerabilities of products during transit, which will be fixed by the process requirements, e.g., through initial security updates
- Conformity assessment – strengthen the consistent NLF-Approach of the CRA**;** other means of showing conformity, like common specifications and CSA-Schemes, should undergo similar obligations and quality safeguards as hEN. Allow for the prudent (re)-use of established international standards like IEC 62443 in the development of the hEN.

- Mitigate possible additional challenges through the CRA in already strained supply chains, by taking into account the incomplete character of most components, especially in regard to their conformity assessment and testing and through the introduction of a lower limit for components, which pose only minimal risk.
- Align the reporting obligations for incidents and vulnerabilities with the NIS-2-Directive and limit those requirements to significant incidents having a significant impact and actively exploited vulnerabilities. Refer to already established international reference points and scoring systems like the MITRE reference-method for "common vulnerabilities and exposures" (CVE) and the CISA "known exploited vulnerabilities catalog" (KEV).

Electro and Digital Industry Association

The CRA is the right approach, but it needs the right "transition strategy" to work

The Current Situation.

The German electrical and digital industry welcomes in principle the coherent and consistent proposal of the Cyber Resilience Act with the intention to simplify the complex regulatory landscape and to counter the further proliferation of piecemeal cyber-security requirements.

The most important task at hand is now to ensure a practicable horizontal regulation that allows the industry to get into the practical implementation. There is little time for the experts in the companies as well as for other stakeholders like notified bodies and the European Standardization Organizations (ESO). The harmonized standards (hEN) must be developed by the ESO in time. Cyber-security expertise and staff in companies must be expanded, processes must be amended or established. Products have to be redesigned or in some cases designed from scratch and these tasks are spread over the whole supply chain. Often with one actor waiting and depending on the tasks and work the actor before him in the chain has to do.

The CRA is a coherent proposal, because it follows the logic of the NLF and therefore differentiates itself positively from the CSA, which only contains some NLF-elements and wording and therefore is no fitting way to place products onto the market. Only some needed limited requirements in the life cycle, especially the establishment of a vulnerability management process were added in a considerate manner. Otherwise, the CRA follows the common framework laid down in decision no. 768/2008/EC.

This way the CRA allows for the use of already known procedures and uses the strengths of the NLF:

- Technological neutral requirements
- Risk based requirements according to a risk assessment in consideration of the intended use and intended operational environment of a product
- Use of proven NLF conformity assessment procedures; especially the internal control procedure based on module A; which allow for a stringent assessment of a large number of products without creating bottlenecks

Beatrice COVASSI MEP, (S&D, Italy) Industry, Research & Energy Committee, Shadow Rapporteur, Cyber Resilience Act

As ITRE Shadow Rapporteur for the Group of Socialists and Democrats on the Cyber Resilience Act, I am preparing a set of amendments to this more than welcome European Commission proposal. I believe that an open and transparent consultation with all actors involved or interested in this legislation is the best way forward to reach ambitious and effective rules that will allow us to put the EU as a frontrunner on such a strategic issue.

In this regard, I am also glad to announce that I will be hosting a Hearing that will be held in the European Parliament next week, on 8 March, in order to listen to the wide spectrum of considerations coming from all relevant actors interested and impacted by this new legislation.

In this regard, I accepted this invitation as a precious occasion to listen to the considerations of producers and manufacturers of products with digital components, as you will be key in ensuring a stronger cyber-security of these products.

The number of connected devices on the market is growing, with a projection to reach 34.7 billion connections globally by 2028. Today, only in my country, Italy, we estimate more than 20 million connected devices.

From connected fridges, coffee machines and light bulbs to security cameras and smart locks, the number of connected products is constantly rising. This does not only increase the risk for vulnerabilities of households and networks, but also increases the potential impact of cyber-attacks. While cyber threats used to be mainly targeted at phones, networks or computers, their potential reach expanded to other connected products such as power grids, cars, railways, toys or watches just to name a few examples.

This new Regulation needs to define a regulatory scenario where companies and authorities are put in the right position to satisfy the consumers request for safety and security of products and to limit potential losses for economic activities linked to cyber-attacks.

As said, the number of digital services and connected devices is skyrocketing and they are increasingly interconnected and present in consumers' lives. Cyber-attacks on connected devices can put consumers at risk and endanger their privacy and security. It is therefore fundamental that the EU develops a strong horizontal legal framework to ensure that companies set up strong cyber-security measures to protect consumers in this connected environment.

This will not only benefit consumers but also strengthen the internal market, where a stronger reliability of products can have clear impacts on perspectives of economic growth and set a standard for international markets.

Joint action at EU level is important to increase the level of trust among users and the attractiveness of EU products with digital elements. But in addition, by strengthening cyber resilience of products, we can also limit potential economic losses deriving from cyber-crime, where in the EU the average cost of a data breach for individual businesses was €3.5 million in 2018 and estimates point at a global annual cost of €5.5 trillion by 2021.

Evidently, all this has an enormous relevance both in terms of quality of life of our citizens, security and of economic impact. In particular, at a time, where cyber-crimes are also related with geopolitical tensions and where, in many Members States, we faced hacking episodes related to the war in Ukraine.

The Cyber Resilience Act can and will offer long-term solutions to help manufacturers, users and authorities strengthen their business. According to the EC figures, 57 % of SMEs say they would go out of business in the event of a cyber-security attack, and the impact on the cyber-security of their products. For the Act to provide long-term solutions, however, we must consider measures that make compliance clear and actionable, while avoiding measures that might generate new uncertainty.

We just heard a presentation on implications for the manufacturing sector and more speakers will follow to describe impacts on specific sectors. I can assure you that all remarks will be taken in due consideration and I will do my best to contribute to a position of the European Parliament able to keep together ambition and feasibility.

GAPS & NON-CONFORMITIES WITH THE UPCOMING REGULATION

Tomislav SOKOL MEP, (EPP, Croatia) Internal Market & Consumer Protection Committee

It is very important to have strong discussions with the industry.

On behalf from my political group, I can say, as you know, that we believe in this partnership with the policy makers and the industry. The EPP is a strong believer in the industry and as such we are always keen to hear the position of the industry. In that regard, the fruitful collaboration with various stakeholders is crucial for legislative procedure.

It is important that we have this kind of discussions in all the stages of the legislative process, so that we know how the industry stands and that we definitely do whatever we can to provide good legislatives solutions.

Speaking of Cyber Resilience of course, this is a very important topic for all of us, especially in today's world of hybrid's threats, but also with the increase of digital trade, of which we saw the explosion during the pandemic.

So, it is very important that we have very strict control, protocols and standards on how digital trade is being carry out and that we have good and clear rules on how we can protect citizens from any kind of cyber threats.

I just wanted to point out the survey which the European Commission carried out in 2020. It showed that more than three quarters of the population is deeply concerned about the possibilities of cybercrime and all the consequences it might have.

Of course, since I am a member of the IMCO Committee, from my point of view it is especially important that products which are being sold on the market fulfil all the security requirements and that the consumers in the end are protected.

In this sense I think that the proposal that we have, the Commission initiative, is a step in the right direction. I think it will definitely be a step forward in the regulated field which is not regulated in the right manner currently on the European level.

We have different rules on national levels - in some Members States more than the others. But this fragmentation is something we do not need. We need a level playing field, we need common rules which will be applicable to all Member States. Also, from the point of the Single Market, if we want to have a real Single Market, we need to have common European rules on this.

Since digital trade, and the digitalisation in general has become such a big part of our market, of our trade, this definitely needs to be regulated. On the proposal itself, I think that it is a step in the right direction.

There is room for improvement but I think the overall principles, the ideas, the needs to have standards protocols on how to act with cyber threats, how to act and prevent the vulnerabilities that we detected, are all things that are very important, things that we definitely need to regulate.

One area where I see additional room for improvement is the area of accountability and especially in terms of legal accountability. Meaning that I think we have to clearly regulate remedies and means of redress for consumers in cases where they suffer damage because of the violation of rules that we make on the European level.

So, if somebody does not respect the future Cyber Resilience Act, we have to make clear how the consumers who suffer damages are entitled to reimbursement, and under which conditions.

I think that it is very important to address the right to legal remedies - this is important for lawyer like me. I think we have to make it clear that we have it in the current proposal but I think that definitely during the negotiations this is something that can be done.

I will not go in too much detail at this stage, we will see how it will play out in all of the relevant Committees.

As I said, as a member of the IMCO Committee I will for my part make the proposal better than it is, whatever the role that the Committee will have in this current process.

Of course, I would like to call on you if you have any suggestions and proposals on how you think this proposal could be amended, could be improved. Please do not hesitate to send them to me, to my office and we can organise a meeting in order to see what steps should be undertaken and what parts of this proposal can be incorporated in our amendments.

So definitely as I said, I have a long track record of collaboration with the industry.

I am open for all concrete suggestions and proposals and I am looking forward for discussion that will give us concrete ideas and enable us to improve the proposal that we have today at our disposal.

Johannes Nitschke, SIEMENS, Senior Director EU Government Affairs

We support the CRA: Siemens welcomes a horizontal EU-wide cyber-security regulation. We have been promoting the importance of cyber-security for many years and initiated the "Charter of Trust" to foster cyber-security.

There is a difference between B2C and B2B: We ask to consider the specifics of products intended to be used by professionals only in industrial and critical infrastructure domains as opposed to products which are used by consumers in a B2C environment.

Safeguard spare parts supply: the CRA should address the aspect of spare parts which often cannot be replaced or updated easily. Therefore, for spare parts a realistic transitional period of 10 years is necessary to allow the repair of existing machines and plants in the field.

Adequate transition period of 36 months: Many products in the B2B environment are small batch series products. It will require significant investment and time to make them "CRA ready". Therefore, the transition period between the entry into force of the CRA and its applicability should be 36 months.

Ensure fair compensation for cyber-security: Cyber-security threats are a moving target and require significant investments to be tackled. Therefore, software and hardware vendors in the B2B environment must have the right to charge an appropriate fee for cyber-security services including updates and patches which they will be required to provide under the CRA.

Keep vulnerabilities secret where beneficial**:** Siemens welcomes the inclusion of requirements addressing development and design processes as well as the vulnerability handling process to support the cyber-security of products. Siemens recommends to report only significant exploited vulnerabilities to ENISA.

Siemens is opposed to mandatory reporting of unpatched and not yet exploited vulnerabilities, as this opens up new attack scenarios if this information is disclosed to the public.

Equally address harmonised standards (hENs), common specifications, and certification schemes: CSA schemes and common specifications need to be subject to the same test procedure and assessment with regard to the coverage of essential requirements of the CRA as hENs. hENs should be available and listed at minimum 12 months before the application of the CRA.

Vincenzo Belletti, CECIMO, Director of EU Public Affairs

The machine tool industry perceives cyber-security as a technical and a business risk, therefore needing full attention to preserve industry competitiveness.

Machine tools are long-lasting capital goods that are often operated for decades. As the majority of Operational Technology, they have complex technical systems connected with other machines, IT and cloud systems. This complexity makes it challenging to secure the entire system with a single intervention during the use phase of the machine. Therefore, more and more manufacturers are integrating high levels of security standard during the phase of design.

Because of the complexity of operational technologies, CECIMO strongly advocates that cyber-security policy actions should make a clear distinction between Information Technology and Operational Technology (OT) security. This is primarily because of the significant differences between the IT-Systems for "carpeted areas" and the ones used in the production environment. In particular, there are at many differences that mark the differences between machine tools (and other production equipment) and classic Office-IT equipment:

- Lifetime of an IT system is three to five years; the one of an OT system like machine tools is twenty years.
- The management of the patches can be done often even daily in an IT system. For the OT system this can happen rarely and must be released by system integrator/component manufacturer.
- Vulnerability scanning - in IT, an active scan can be done without causing major impacts while an active scan in OT can disrupt the operational production. This also shows that in OT, availability of the machine is essential and there is no margin for delays.

The publication of the Cyber Resilience Act can offer a long-term solution to help manufacturers, users and authorities.

We support the horizontal approach to cyber-security for connected devices and appreciate that the proposal aims at applying the NLF principles which will ease compliance for our sector. Nevertheless, we think there is still room for improvement.

For instance:

- Regarding the scope, we believe that it should be reduced and kept consistent with other regulations such as Data Act or RED Delegated Acts. In addition, it is important to clarify the inclusion of components in the proposal's scope when it comes to a product that entered in the market before the date of application of the CRA.
- Clarify the roles and responsibilities in the supply chain when it comes to transmitting updates and patches to end-users.
- Distinguish, in a more explicit manner, between B2C and B2B relationships when it comes to placing cyber-safe products on the market.
- Analyse existing standards and ongoing development in the different technical committees and see what can be used and how much work needs to be carried out in terms of standards development (either general framework or at products level).
- Extend the transition period, adapting the period according to different risk classes (eg. 36 months for class I and 48 months for classes 2 and 3).
- Create a European regulatory sandbox to support compliance, particularly for SMEs and start-ups, and to contribute to regulatory learning for a future revision of the CRA.

There is no doubt that the legislation will generate benefits and enormous pressure on our industries.

Therefore, we encourage all policymakers not to rush this legislative process and ensure that legislation provides the necessary protection and incentives for industry, workers and consumers.

I am looking forward to continuing the discussion with the co-legislators in the coming months.

Maria GRAPINI MEP, (S&D Romania) Vice Chair Internal Market & Consumer Protection Committee

I will speak from the perspective of IMCO Committee since I am the Vice-Chair of this Committee. First of all, I would like to thank the European Forum for Manufacturing for the invitation to this event. Taking into account the fact that we live in an era of digitization, I consider that the subject of this debate is important and welcome.

With the rise of smart and connected products, a cyber-security incident on a single product can affect the entire supply chain, potentially disrupting social and economic activities in the internal market.

Through this legislative act, it is important to ensure better consumer protection by increasing the responsibility of manufacturers, requiring them to provide security support and software updates to address identified vulnerabilities, and providing them with information about the cyber-security of the products they buy and use.

The proposed act imposes cyber-security obligations on different economic operators, depending on their role and responsibilities in the supply chain. Manufacturers must ensure that digital products comply with essential cyber-security requirements and conformity assessment procedures before placing them on the market. In addition, they must record technical documentation and comply with notification obligations for cyber-security breaches. Importers must only place on the market digital products that comply with essential cyber-security requirements and carry the CE mark. Distributors must check that digital products carry the CE mark. They also have a duty to ensure that manufacturers and importers have complied with their obligations under the law.

The act wants to provide a unique set of cyber-security rules for EU companies, reduce the number of cyber-security incidents and increase transparency and consumer trust in products with digital elements and guarantee better protection of data and their privacy.

My concern is related to the burden of this act on industry, especially on SMEs. I also believe that the application is very important in order not to create dysfunctions and unfair competition in the internal market.

I expect to continue to have an interesting debate to see what is the position of the stakeholders and how we, as legislators can legislate so that this act to be in favour of both the industry, and the consumer.

Paolo Falcioni, APPLiA – Home Appliance Europe, Director General

Around 10% of products are classed as 'critical' or 'most critical' in the EU's proposed Cyber Resilience Act, including the vast majority of home appliances. The list of critical products with digital elements is extremely wide, to feature nearly every connected application. Yet, the cyber-security of components does not determine the cyber-security of products. For a house not to fall, it is not enough for all bricks to be certified. Instead, for all bricks to be brought together in a (cyber) secure manner, it is the final product that we should be looking at.

A clear distinction must be made between high and low-risk cyber-security appliances. The exchange of data when using a washing machine will clearly be low-risk, if compared to the exchange of data when using a mobile banking app, for instance. If that same washing machine is used in a home environment, then it is considered subject to a low cyber-security risk. However, if the machine is used in a power plant instead, then it becomes high-risk because of the sensitivity of the environment in which it is installed. In the unlikely event of this latter case, then all washing machines become high-risk, according to the proposal. Which clearly does not rightfully reflect the nature of the product. Appliances come with different cyber-security risks, which standards must reflect.

According to the proposal, manufacturers have twenty-four hours to notify the vulnerability of a product, even in the absence of a corrective measure. Which means opening the door to possible cyber-attacks, de-facto exposing a vulnerability without having a solution for it. The opposite of what cyber-security should look like.

If the Cyber Resilience Act was a ship, it would stay afloat, but it would not be ready for rough seas. The proposal is a great opportunity to further bolster the cyber-security of products. Yet, it must be weatherproof.

Manuel Ifland, SIEMENS ENERGY, Principal Industrial Cyber-Security Consultant

I am pleased to be here today to represent Siemens Energy's position on the EU Cyber Resilience Act. Our portfolio drives the energy transition, we offer products, solutions, and services across the entire energy value chain. We are present in more than ninety countries worldwide and our customers are in the critical infrastructure sector.

At Siemens Energy, we look at the CRA proposal from our role as manufacturer of critical infrastructure systems, such as Industrial Automation and Control Systems (IACS) and SCADA Systems (Supervisory control and data acquisition). In this role, we believe that the European Commission's CRA Proposal will help to make products of all stakeholders in the supply chain more secure by design and resilient against cyber-security threats.

We especially appreciate the integration of cyber-security into the product design process, throughout a product's lifetime, based on risks. Siemens Energy have been doing that for many years by using the international IEC 62443 standard series as a reference.

As critical infrastructure systems manufacturer, we believe, the CRA needs further clarification and refinement in some areas. For example, industrial automation and control systems are listed

in Annex III as Class II products used by essential entities as per NIS2. IACS usually contain a non-negligible amount of components, which are products with digital elements themselves.

The CRA requires products to be delivered without any known exploitable vulnerabilities. However, especially in case of systems, there are far more cost and effort-efficient ways of mitigating vulnerabilities, for example, by introducing a firewall. It is important to point out that, in the critical infrastructure world, there are situations where patches cannot be applied without risking an impact on the safety properties of a system, for example, performance or reaction times of real-time applications.

In general, we urge for the CRA to adopt an even more risk-based approach and to empower manufacturers to make well-informed decisions, based on risks. This includes, but is not limited to, decisions like when to patch, what to patch, what information to publish, and how long to support products. Please have a look at the Siemens Energy position paper where you will find more details and examples.

Alberto Di Felice, DIGITALEUROPE, Director for Infrastructure, Privacy and Security Policy

Cyber-security Everywhere: Deciphering the Cyber Resilience Act

Cyber-security has become indispensable to our economy and society, and can no longer be an add-on to Europe's regulatory landscape for products. DIGITALEUROPE strongly welcomes and supports the objectives of the proposed Cyber Resilience Act (CRA), which will for the first time introduce mandatory cyber-security requirements for 'products with digital elements.'

DIGITALEUROPE has consistently advocated in favour of horizontal cyber-security requirements for connected devices. This is not only because of the heightened importance of securing the growing number of devices on the market, which are projected to reach 34.7 billion connections globally by 2028, but also the increased risk of an unclear regulatory framework.

Recent years have seen a proliferation of piecemeal cyber-security requirements under different EU laws. This complex regulatory scenario is making compliance more difficult for companies, as well as authorities, which in turn will work against a more cyber secure posture in the EU.

The CRA can offer a long-term solution to help manufacturers, users and authorities strengthen cyber-security across the board. For this to happen, however, we must consider measures that make compliance clear and actionable rather than generate new uncertainty.

An effective CRA must:

- Factor in the specificities of standalone software, such as the impact of software updates on old concepts such as 'substantial modification,' including through the development of guidelines with input from a newly created Stakeholder Expert Group, which should advise the Commission on the CRA's implementation and future review;
- Exclude hardware, software and services used for remote data processing, transmission and storage, to avoid excessive overlap with the new Directive on measures for a high common level of cyber-security across the Union (NIS2);

- Introduce the concept of 'partly completed product with digital elements,' allowing for more accurate conformity assessment of software or hardware that must be incorporated into finished products;
- Maximise self-assessment through the development and use of harmonised standards, leveraging the many cyber-security standards which are already in place, in Europe and globally, to support companies' compliance. An implementation period of forty eight months should be provided so that the necessary harmonised standards can be delivered, and a bottleneck of third-party assessments avoided;
- When required, provide for scalable third-party assessments across other legislation, such as the AI Act, and prioritise mutual recognition agreements to facilitate market access in third countries, particularly with the US as part of the ongoing EU-US Cyber Dialogue;
- Automatically recognise voluntary cyber-security certification schemes approved under the Cyber-security Act as a means for manufacturers to prove compliance, and stipulate a direct presumption of conformity vis-à-vis the AI Act's cyber-security requirements;
- Align incident reporting obligations and timelines with NIS2, requiring an 'early warning' within 24 hours, followed by an incident notification within 72 hours. For vulnerabilities, ENISA should establish a European catalogue of known exploited vulnerabilities, which should be reported by manufacturers;
- Directly repeal the Radio Equipment Directive (RED) delegated act on cyber-security, which the CRA makes redundant, and provide for a transition period where compliance with either will be possible; and
- Create a European regulatory sandbox to support compliance, particularly for SMEs and start-ups.

Lutz Jänicke, PHOENIX CONTACT GmbH & Co. KG, Corporate Product & Solution Security Officer

Introduction

Phoenix Contact welcomes the proposal of the EU Cyber Resilience Act (CRA), which formulates cyber-security requirements for products and their manufacturers. As a manufacturer of products with digital elements, this affects our product offerings. On the other hand, it helps us as an operator of such products in our own OT (operational technology) and IT environments.

As a manufacturer of products with digital elements aimed at the industrial automation market, we comply with the product regulations under the New Legislative Framework (NLF) very well. The EU CRA also follows NLF principles, which helps the integration into long-established structures and processes.

General Considerations on Products with Digital Elements

Digitalization introduces new technical options and, unfortunately, creates a lot of complexity. Innovation is based on technology being developed by other parties – no organization can develop complete technology stacks on its own. Instead, organizations rely on integrating hardware or software components. It therefore makes perfect sense to also consider such components and ask for due diligence when integrating them.

On the other hand, even with increasing security efforts, such components are not free of vulnerabilities. When coordinated disclosure is used, from finders of vulnerabilities to organizations along the supply chain, handling these vulnerabilities takes time. In the case of non-trivial products with digital elements, a manufacturer may therefore at some time have knowledge about vulnerabilities in a product while working on security updates and coordinating these efforts with other parties under embargo and wait until an agreed date to release fixes.

Considerations Regarding Industrial Automation

Phoenix Contact provides products to the industrial automation market. In industrial automation, many installations and machines are custom-designed, using components such as programmable logic controllers, sensors, actors, etc. Such components are designed to fulfil specific purposes. Therefore, automation is no mass market where millions of instances of a specific product might be sold. Instead, there are large portfolios with limited numbers of products of each type sold.

Every change to an existing installation bears the risk of failure or problems that may be hard to understand and solve. Customers therefore expect product change notifications in order to be informed about upcoming changes to products several months in advance. In a significant number of cases there are agreements to supply a customer with a specific older version of the product that has been approved in the customer's internal processes. For the same reasons, customers like to purchase old products as replacement parts for existing installations. Installing later versions or even new products might lead to very high effort in re-engineering the installation and testing it again.

Recommendations On Further Improvements

Phoenix Contact supports the positions of ZVEI, VDMA, and Orgalim and recommends the following improvements to the EU Cyber Resilience Act.

- Delivery of products and known vulnerabilities

  In complex products, it may be that vulnerabilities are known and being worked upon. The necessity to stop placing products on the market in the meantime may significantly hurt both manufacturers and customers. Manufacturers should still be allowed to deliver products while addressing the vulnerabilities, which already is an essential requirement (Annex I.2). The fulfilment of the other essential requirements in Annex I.1 should be sufficient to increase the cyber-security of products with digital elements significantly.

- Providing cyber-security support

  Providing cyber-security support becomes more costly with every year as the technology evolves and the focus moves to later products. Engineers will have to re-engineer older products once new vulnerabilities are found.

  The duty to supply updates to products should therefore allow supplying updates that also include new features at the decision of the manufacturer. The time should not extend the currently listed five years. If longer support periods are needed in certain markets, suppliers and customers always have the option to negotiate commercial terms.

- Spare/Replacement Parts

  The CRA requires products to be placed on the market to fulfil the state of the art at that particular time. In industrial automation, a direct replacement of a defective product is often requested, even if the product is already quite old. This way, the operator does not risk

problems due to changes in the product. The security of the existing installation is not affected by installing a replacement part. The CRA should add the possibility to provide replacement parts that may not be state-of-the-art when being placed on the market and to not start a new security support period.

- Digital Documentation

  The documentation necessary to operate a product with digital elements securely can be exhaustive. In one example of a programmable logic controller, the English documentation alone is around 200 pages. The CRA should allow cyber-security documentation to be provided in a digital format and either packaged with the products with digital elements or made available via download.

- Determination Of Critical Products

  The current proposal of the CRA places all products in the industrial automation market into the category of critical products. While the use of harmonized standards is best practice in industrial automation, the number of products requiring third-party involvement should be reduced significantly, since it increases the time before a product can be made available on the market. In addition, there are not enough security experts available for third parties to provide the service needed.

- Transition period

  The planned transition period of 24 months for products to comply with the essential requirements is too short. In industrial automation, the development of products typically takes a significant amount of time (18-36 months), considering additional properties such as electromagnetic compatibility, mechanical properties, and temperature ranges. Having to redevelop and test many products within the given transition period is hardly possible, especially as harmonized standards are not available yet. It also must be considered that all other innovations would stop in the meantime. In addition, there are not enough security experts available. We therefore recommend extending the transition period. In the upcoming Machinery Regulation, which aims at the industrial market, a much longer transition period is planned.

Nils Scherrer, VORWERK SE, Manager Regulatory Affairs

Vorwerk welcomes the Commission proposal for a horizontal regulation creating a central reference point for cyber-security requirements for connected products placed on the EU market. The Cyber Resilience Act (CRA) is in our view a very important step towards enabling a harmonised level of cyber-security for products in the EU based on the principles of the New Legislative Framework and using a risk-based approach that takes the intended use and intended operational environment of digital products into account.

In order to avoid any fragmentation of cyber-security rules and in order to strengthen this horizontal approach, Vorwerk suggests:

- to further clarify the interplay of the CRA with existing legislation. From the perspective of Vorwerk and household appliances this particularly concerns the Delegated Act on Article 3

(3) of the Radio Equipment Directive (RED) and the recently adopted Network and Information Security Directive 2 (NISD-2).

- Include a repeal of the delegated act under Article 3(3) d,e,f of the RED in the legal text

  It is crucial that there is a legally secure statement in the legal text on the interplay of CRA and the security-related requirements of the Radio Equipment Directive. In the current text there is only a short reference in the Recital stating that "the Commission would repeal or amend the Delegated Act".

  The relationship between both pieces of legislation should be clarified in the legal text (e.g. in a new Article 7a similar to Machinery Regulation and AI Act) and should avoid any confusion for manufacturers of radio equipment. This is justified as the Commission correctly states in its explanatory memorandum that the "essential requirements in the CRA cover all the elements of the essential requirements referred to in Article 3 (3) point (d), (e) and (f)" of the RED. The crucial standardisation work that has been invested so far will not be lost and should be taken into account to influence the work on harmonised standards for the CRA.

- Clarify definitions and ensure alignment with existing provisions:

  - Since important legislations such as the NISD-2 is already in place aimed at entities to ensure a high common level of cyber-security on organisational level, it is important that definitions and requirements across cyber-security legislation remain consistent.

    Important definitions such as "cyber-security risk" and "vulnerability" can be understood very broadly and must be clearly defined in order to guarantee a uniform and harmonised understanding of European cyber-security legislation – eg. while the CRA refers to "cyber-security risks", the NISD-2 only defines the broader term "risk". Also, it would be helpful to explain the difference between "incident", "vulnerability" and "actively exploited vulnerability" with regards to reporting obligations. In fact, the term "incident" is currently not defined and needs to be added in reference to the wording in NISD-2.

  - In our view this interplay of CRA and NISD-2 is also relevant in the context of reporting obligations in Article 11.

    The obligations of reporting either to national CSIRTs or to ENISA need to be further aligned with the existing obligations for entities in the NIS-2-Directive to limit the burden for companies to comply.

    Vorwerk suggests an extension of the time limit for the reporting of incidents in Article 11 to 72 hours for incident notifications in general.

    An alternative solution would be to do the "risk-based approach" of the proposed regulation justice, by reflecting the actual security risk of vulnerabilities and actual severity of incidents in the respective timespans for reporting. The lower the severity of incidents and possible harms, the higher the timespan.

    Manufacturers already have very limited personnel resources qualified for the vulnerability management. In order to deal with strict reporting obligations, there needs to be clear guidance what is the scope of relevant information to be reported – limited to significant exploited vulnerabilities.

    We are also concerned by potential additional costs if national authorities in the member states require further or different information (e.g. in the context of NIS-2

implementation) which would lead to a "hotchpotch" of information provision that cannot be handled even by medium-sized companies.

Mette Peetz-Schou, DANSK INDUSTRI DI, Leading Senior Adviser

Dansk Industri supports the ambition to improve the cyber-security of products in the EU. We have worked to secure a horizontal approach to clean up the patchwork of initiatives that has been taken during this legislative tenure in the Radio Equipment Directive, the Machinery Regulation, the General Products Safety Regulation, and the AI Act. Therefore, we are happy to see that it is indeed what the Commission has in mind. We are also happy to see a proposal based on the New Legislative Framework (NLF), a regime our member companies deeply rely on when it comes to ensuring compliance with EU law, and which will ease compliance when the rules come into application.

That being said, it will be a mayor challenge for businesses to handle stand-alone software as a product in the regulation, and it will call for a longer transition period than the expected 24 months to be able to do so, despite our common concern of the existing cyberthreat at hand. 48 months seem more reasonable.

I highlight four (aspects of the regulation that our members are concerned about that may not be highlighted by others:

- Criteria for products and products that need to undergo higher level of conformity assessment, especially those that need to undergo third party assessment

  The proposal lists criteria that can be applied to determine which products that need to undergo what level of conformity assessment and includes an annex that specify which products that belong to two categories of critical products. The application of a product in an industrial setting is seen as sensitive requiring higher level of conformity. That needs to be changed. DI believes what matters is whether the product is applied in a critical function which can be either in an industrial setting or a consumer setting.

  Furthermore, the criteria need to be assessed based on the products' intended use. The Annex consists of comprehensive lists of products requiring higher level of conformity assessment; however, the definitions of those products are not foreseen before one year after the regulation comes into force. That won't work. Businesses need clarity to prepare. Furthermore, there is a need to scrutinize the lists, for instance industrial robots should not be required to undergo third party conformity assessment if a harmonised standard exists.

- The ability to process data as a basis for developing new business opportunities

  The proposal lists in line with NLF (in Annex 1) essential requirements products must fulfil. One is to minimize or limit the processing of data, personal or other, to what is adequate and relevant to the intended use of the product. Although we agree the amount of data being processed is relevant to cyber-security, we need to strike the right balance that allow businesses to collect data to develop new services that are not in line with the intended use when the product was first placed on the market. That would also be in line with the intentions of the Data Act.

- One product one regulation and alignment of requirements with the NIS2 for entities

  The proposal includes Articles to explain how the regulation relates to other legislations that contain requirements related to cyber-security. DI fully supports these. To ease compliance only one set of rules should apply for one product. However, there is a need to make this point clearer in the legal text. This could be done simply by adding an article that states that products that are in compliance with the Cyber Resilience Act also is considered to be in compliance with the Radio Equipment Directive, the Machinery Regulation, the General Products Safety Regulation, and the AI Act. That would also ease challenges related to many different application dates for manufacturers that are able to comply with the requirements of the Cyber Resilience before its extended applicability date but after the other legislations are applicable.

  As the production of many products now falls under NIS2 for instance the production of machinery or electronic and electrical products, it is important to align the reporting obligations of the Cyber Resilience Act with the NIS2 and limiting the reporting obligations to significant incidents.

- Reasonable fines and guidance

  As a product regulation it is logical the Cyber Resilience Act is to be covered under the rules of the Market Surveillance Regulation. Therefore, it is also surprising to have special rules on penalties with fines up to 5, 10 or 15 million Euros. The fines need to be aligned with fines related to non-compliance of other product regulations which is determined at national level and reported to the Commission as effective, proportionate, and dissuasive. Furthermore, we need to focus on guidance. The Cyber Resilience Regulation is a complex piece of legislation including many new aspects, for software and with requirements in the entire life cycle to mention a few. That calls for guidance as a carrot, sticks and huge fines.

Alexander Eisenberg, BSH HOME APPLIANCES SA (Bosch Group), Head of Office EU Technical Market Access

Introduction

The CRA is the legislation we, as BSH, asked for since a long time. It has the potential to be the one legal reference when it comes to Product Cyber-security. Its key elements are well set. To potentially become a game changer some aspects should be smoothed out. This intervention focusses on some important aspects from a European hardware manufacturers point of view such as the Bosch Group with a broad portfolio from industrial B2B solutions, through mobility components to end-consumer B2C products such as connected home appliances. Further aspects can be found in association positions, such as DIGITALEUROPE, which we also fully support.

- The CRA is good product regulation: we asked for it – we need it!

  Europe needs legal certainty and a level playing field for product cyber-security. The CRA is the solution and it is a good approach. It is good because

- Based on the New Legislative Framework (NLF), it provides the same rules across Member States and beyond by compelling importers and thus allows for free movement of goods based on the same security standards in EU.
- It protects the Single Market with fair and clear market entry conditions for all economic operators
- It offers a risk-based approach considering the intended use thus balancing the societal need for security and a functioning economy alike.
- It relies on well-known Conformity Assessment methods, so-called "Modules" including the internal control procedure (self-assessment)
- Enforcement is realized through well-known procedures for market surveillance
- It draws on one of the biggest assets of the NLF: it builds on the competence of EU Standardization through harmonized standards to provide the technical details.

- Software is a product, a service is not a product

  CRA faces the reality: software is considered a product, and this enables a fair balance of responsibility between software providers and hardware providers. Why is that needed? Because currently the responsibility for all cyber-security related issues lies on the last one daring to put his logo on the tangible product.

  Examples:

  - A hardware manufacturer (eg. of a laptop or a cell phone) is responsible for conformity of and incidents originating from the operating system, even if that is from a third party.
  - It is currently possible to exclude cyber-security responsibility for firmware for components by artificially splitting the contract for it in two: one for the component - one for the necessary firmware
  - App providers for instance in the context of a smart home are only bound by individual contractual provisions for cyber-security, but not by objective legal obligations for their apps.

  Once software is unambiguously a product when sold in a commercial activity this will strike a better balance and would certainly reduce effort and increase fairness within B2B contracts.

  However, it is important to focus on software and keep services out of scope.

- Everybody says "Standards are key" but efforts are needed to make it work!

  NLF works through the listing of harmonized standards in the official Journal of the EU; this listing will be easier if:

  - the Commission's "Standardization Request" is non-prescriptive without adding requirements beyond the legislation
  - risk-based procedures and methodology were accepted in standards in order to meet the challenges that:

    - cyber-security is not quantifiably measurable
    - the state-of-the-art changes quickly
    - in the beginning horizontal standards cannot be specific

  - the Commission would be lenient – at least in a first phase – to accept existing standards without modifications and possibly even without formalities such as specific annexes, and
  - it was acknowledged that detailed, specific standards need time.

- Timeline: we need the CRA quickly but also enough time for application

  BSH alongside with Bosch has a long track record of asking for a horizontal product regulation in order to provide legal certainty and one - and only one - legal reference point for a manufacturer of a connected product. So, the earlier the CRA provides such certainty the better.

  However: the time between entry into force and application needs to be prolonged significantly.

  The main reason is missing experts: While many economic operators are providing high security products, yet nobody is ready for the necessary compliance work – which means testing and validation, especially when notified bodies are necessary for conformity assessment. At the same time, notified bodies and market surveillance authorities are competing with industry for the same product security experts (keep in mind that product security is different to the relatively well described enterprise / IT security).

  The second reason is that mutually agreed product security standards must be in place in a single market with fair conditions to all, and these need time as product security standards are new to many sectors.

- Reporting once in one format for the same incident

  If a company undergoes a significant incident its primordial objective is to mitigate the impact. Reporting is done already to the company's board of management, to its concerned customers, to concerned suppliers, potentially to data privacy authorities. The more you report the less you have time to act.

  So, the request is: One Incident, One Report to authorities only!

  This should be in line with NIS2 reporting, but ideally where applicable the one report should also cover other mandatory reporting such as personal data breach reporting under GDPR, financial incidents under DORA or incidents in vehicles under UNECE Regulation 155.

Conclusion

The CRA can effectively increase cyber-security for digital products placed at EU market and hence improves cyber-security protection for EU product users, EU business, and EU society in general.

CONCLUDING REMARKS

Antony Fell, EUROPEAN FORUM FOR MANUFACTURING, Secretary General

In concluding this EFM event on the Cyber Resilience Act, I would like to thank each of the European Manufacturers for their useful presentations, the MEPs for their interventions and the European Commission for its policy statement.

And especially I would like to thank Vlad Botoș MEP for chairing and moderating of this EFM Forum

I formally close this European Form for Manufacturing meeting on the Cyber Resilience Act.

* *