# Cyber Resilience Act – Podcast transcript

German audio · English transcript · 26:05

English translation of the German discussion, edited for readability and time-stamped. The editorial notes clarify several simplified statements in the recording.

## Editorial notes on the discussion

Editorial notes as of 15 November 2026.

Support and updates. The support period is generally at least five years. Where a product is expected to be used for a shorter period, support may match that period. Automatic security updates are required where applicable.

Software bill of materials. The SBOM must cover at least top-level dependencies. The duty to document components does not give every purchaser a general right to receive the complete SBOM.

Reporting. Article 14 has applied since 11 September 2026. Once aware of an actively exploited vulnerability or severe security incident, manufacturers must generally give early warning within 24 hours and notify within 72 hours. Final report deadlines differ between the two cases.

Product liability. (EU) 2024/2853 is a directive. A missing update may be relevant in establishing a defect. The claim also requires compensable damage and a causal link. Damage to property and data used exclusively for professional purposes falls outside this directive.

CE marking. Article 30(4) of the CRA requires the notified body’s identification number to follow the CE marking when that body takes part in the full quality assurance procedure under Module H.

(EU) 2024/2847 · (EU) 2024/2853 · CRA reporting obligations

## The connected baby monitor and scope

**00:00** Imagine buying a brand-new car, right? Yes, okay. A nice new car. Exactly. You drive off the dealer’s lot, accelerate on the motorway to about 130 kilometres an hour, and suddenly realise the manufacturer forgot the brakes. That would be less than ideal, yes. Absolutely. You phone customer service in a panic and they calmly say, “Oh, sorry. You’ll need to download the brake pads yourself from the internet and work out how to fit them. Good luck with that.” That sounds absurd. Right. Anyone would sue straight away. Exactly.

**00:34** Yet in the digital world you can buy smart door locks, baby monitors and Wi-Fi routers every day where precisely that happens. Unfortunately, yes. You’re buying an unfinished product. Exactly. An unfinished, insecure product, and you as the buyer bear all the risk. At least until now. The EU is hitting the emergency stop button, and with a

force that’s hard to imagine. It really is going to shake the whole global tech industry. Well put.

**01:06** Welcome to today’s deep dive. It’s good to have you back as the third person in the room with us. Thanks for listening. Today we’re looking at something that, at first glance, sounds like dry Brussels bureaucracy. But it isn’t? No, not at all. It’s a regulatory earthquake. We’re talking about the new EU Regulation 2024/2847, better known as the EU Cyber Resilience Act, or CRA for short. Exactly. Today our source is exclusively the original EU legal text. But don’t panic. We’ll translate it into everyday language for you. Let’s unpack it.

**01:47** Let’s get into it. To make this tangible, I thought we’d invent a product and work through the law using that example. Let’s call it the Smart Baby 3000. The Smart Baby 3000. I like it. What does it do? It’s a state-of-the-art baby monitor connected to Wi-Fi, with an HD camera, a cloud app for your phone, the works. How does the CRA change life for this particular device? To understand that, we first need to look at the new scope of application.

**02:19** The CRA applies to all, and I’m quoting here, “products with digital elements”. That sounds extremely broad. It is. The text defines them as products whose purpose includes a direct or indirect logical or physical data connection to a device or network. So our Smart Baby 3000 definitely falls within scope. Absolutely. It combines hardware and software and depends on being connected. The exceptions are essentially areas that already have extremely strict sector-specific legislation. Things like medical devices or aircraft? Exactly. Cars, aviation, medical devices: they already have some tough rules.

**02:57** Okay, but hang on. The baby monitor itself sits in my child’s room. What about the app and the cloud? Good question. The video signal often travels through a server overseas. Does the EU regulate just the plastic case and the chip, or does that cloud service come under the rules too?

**03:17** That’s an important distinction. In principle, the CRA regulates products rather than stand-alone services. But, and it’s a big but, remote data processing such as cloud processing falls under the CRA if the product couldn’t carry out its function without it. I see. If your Smart Baby 3000 can’t display a picture on your phone without an interface on the manufacturer’s server, that cloud component is legally part of the regulated product. Wow. So the manufacturer can’t simply say, “Our device is secure. Unfortunately the server over there got hacked.” Exactly. That no longer gets them off the hook. They’re responsible for the whole thing.

## Secure defaults and supply-chain responsibilities

**03:54** That makes sense. What exactly does the EU require? Can the manufacturer just put it on the market and issue a patch later, say, after hackers start shouting creepy things into the nursery? Not any more. Those days are over. At the heart of the regulation is the principle of security by design and by default. Security straight out of the box. Exactly. Security used to be an afterthought, like sticking a plaster on an open wound. The idea being, “We’ll patch it later.” Right. The law now requires manufacturers to place products on the market free of known exploitable vulnerabilities. That obligation starts at the drawing board. Wow.

**04:33** That includes data minimisation. The baby monitor can’t secretly collect metadata for advertising when it doesn’t need those data to work. That’s reassuring for a baby monitor, I must say. Isn’t it? And most importantly, protection against unauthorised access must be the default. So all those notorious default passwords, “Admin123” or just “0000”, that used to be hard-coded into millions of devices, become illegal. Absolutely. Each device must have individual credentials or make you choose a genuinely secure password the first time you switch it on. At last.

**05:13** What I find fascinating is the economics behind this. The EU is intervening to correct a classic market failure. How do you mean? Information asymmetry. Exactly. As an ordinary user, you can’t judge how secure a complex smart-home device is. No, I really can’t. It looks good and it works. Right. You can’t see whether the code behind the scenes has more holes than Swiss cheese. The manufacturer knows, of course. But up to now there was no financial incentive to put money into security you can’t see. Because the design of the case sells better than code quality. Exactly. The CRA is radically shifting that economic burden to the manufacturer.

**05:54** Okay, the manufacturer who builds the thing has to invest. But let’s be honest: a baby monitor like that is usually made somewhere in Asia. Usually, yes. Then a small importer brings it to Europe and it ends up on the shelves of a big electronics shop here. What if the manufacturer in Asia says, “I don’t care about EU rules”? Are the European retailers off the hook? No, not at all. The EU has learnt from earlier regulations. It’s bringing in the whole supply chain now. Including the electronics shop around the corner.

**06:27** Yes, EU importers and distributors share responsibility. If you’re a big retailer buying container loads of cheap smart-home gadgets from overseas, you can sell them only if they carry CE marking and you can demonstrate their IT security. So the retailer has to check that? Exactly. If a distributor even has reason to believe the Smart Baby 3000 poses a risk, they can’t put it on the shelf. They have to block it and inform the authorities immediately.

## Open source and commercial use

**06:55** I have to jump in here. That sounds great in theory, but doesn't it run straight up against the reality of software development? In what way? Nearly every modern commercial product uses open-source components. The manufacturer of my Smart Baby 3000 isn't writing the operating system from scratch. True. They take a free version of Linux, add an open-source camera library from GitHub, and the thing's ready to go. If that freely available code written by volunteers turns out to be insecure, who's liable?

**07:26** I see where you're going. It sounds as if this law could shut down the whole independent developer community. Suppose I write a cool smart-home plug-in in my basement at the weekend and put a little Patreon link on my website so people can buy me a coffee. Can someone suddenly sue me for millions if my code gets hacked? Honestly, if that's the case, I'll take my code offline today. Okay, take a deep breath. You can leave your code online. Phew, that's a relief. But the point you're raising was the open-source community's biggest fear when the first drafts came out. Understandably. Absolutely.

**08:03** If we look closely at the text, particularly recitals 17 to 19, we can see how neatly the legislators addressed this. The CRA draws a distinction between the development stage and the commercial supply stage. What does that actually mean? Free and open-source software, FOSS, is subject to these strict obligations only when it's made available in the course of a commercial activity. And my Patreon coffee button? That isn't a commercial activity. Donations made without a profit-making intention are expressly treated as an exception in the legislation. Good.

**08:38** It really becomes commercial when you actively monetise the software or, for instance, charge for technical support. Or, and here's the important point for businesses, when a large company takes that free hobby code and incorporates it for profit into a commercial router or baby monitor. Then, and only then, do you as the manufacturer of that end product become fully liable for the security of those open-source building blocks. That's clever. So the maker of the Smart Baby 3000 can no longer say, "It wasn't our fault, the bug was in the free camera library." Exactly. They earn money on the whole package. So they must also guarantee that the free parts they put in it are secure. That protects innovation by small developers while holding the big tech companies accountable. Pretty smart.

**09:31** What about the really big open-source foundations? You mean the Apache Foundation, for example? Exactly. They develop software that seems to run half the internet, but they're often non-profits. The law introduces a new role for them: open-source software stewards. That sounds formal. It is. These are legal entities that provide systematic, sustained support for open source without selling finished products like conventional manufacturers. Why give them their own role?

**10:09** The EU understands that if you hit an organisation like the Apache Foundation with millions in fines, the internet could fall apart tomorrow. So these stewards have lighter obligations. A bit of protection for the little guys? Something like that. They need a documented cybersecurity policy and must handle vulnerabilities professionally. Of

course. But, for example, they aren’t allowed to affix CE marking, and the text specifically shields them from harsh fines. The idea isn’t to bankrupt them. That makes sense. So we’ve covered design and the development phase.

## Updates, support and the software bill of materials

**10:44** Let’s jump ahead to after the purchase. Sure, the period of use. I’ve had my Smart Baby 3000 for three years. Suddenly a security researcher discovers a serious hole in that very camera library. The classic scenario. Manufacturers used to say, “That’s an old model. Buy the new Smart Baby 4000.” How does the CRA deal with updates? This is where things get painful for many manufacturers. The CRA requires a guaranteed support period.

**11:17** Support period? Yes, the period during which security updates must be provided. It has to reflect the product’s expected time in use and is generally at least five years. Five years? That’s half a lifetime in the tech world. There are exceptions when the product’s useful life is inherently much shorter. A temporary app for an event, for instance. But for a physical device we’re generally talking about at least five years.

**11:48** Do those updates have to arrive automatically, or do users have to keep digging through obscure menus and clicking “Check for updates”? That’s the next big step. The law requires products to be designed so that security updates download and install automatically by default. Yes! There’s a simple opt-out if you really don’t want that. But automatic is the default. There’s another interesting requirement: feature updates are to be separated from security updates. Thank you, EU. So I won’t be forced to install a completely redesigned, memory-hungry app interface just to close one tiny security hole. Exactly. The security side is decoupled. That’s very user-friendly.

**12:36** Now comes the Herculean task for manufacturers. Which is? How does the maker of the Smart Baby 3000 even know, three years later, that this specific, vulnerable three-year-old open-source library is buried deep in its code? This is where that acronym everyone in IT is sweating over comes in, right? SBOM? Exactly, SBOM. It stands for “software bill of materials”, a list of the ingredients of your software. The CRA requires manufacturers to compile and maintain a machine-readable list of all the components, libraries and dependencies used in their product.

**13:16** Put it in everyday terms: it’s like the ingredients list on a food packet, isn’t it? Exactly. If you’re allergic to peanuts, you turn the packet over and check for peanuts. If a vulnerability is found in a particular piece of code, the manufacturer checks its SBOM ingredients list and immediately sees, “Oh no, that vulnerable code is in our baby monitor. We need to patch it straight away.” Great analogy. Now imagine the list has hundreds of thousands of entries, and some ingredients are themselves made up of dozens of ingredients from suppliers you don’t know personally. That sounds like a nightmare.

**13:55** It is. But look at the bigger picture and you’ll understand why the SBOM is revolutionary. Remember Log4j? Oh goodness, yes. It was a tiny Java logging library that was built into practically everything. When a vulnerability was found, there was worldwide panic. It took major companies weeks just to work out which of their own

systems were running Log4j. An enormous butterfly effect. Right. With an SBOM you can scan your bills of materials automatically and know in a fraction of a second which products are affected. Building that retrospectively for old code is a huge logistical challenge, but going forward it’s essential.

## Product risk, conformity and CE marking

**14:35** Wow. We’ve got secure design, five years of automatic updates and a complete ingredients list. Who checks all this? Does the EU just trust manufacturers to get it right? Will anything change on my baby monitor’s packaging? The visible mark on the packaging will still be the CE marking, but its meaning is changing dramatically. In what way? On many smart devices the CE marking often stood mainly for electrical safety, for instance that the power supply wouldn’t catch fire, or for radio standards. From now on it must also stand for IT security under the CRA. Who checks that?

**15:17** That depends on the risk class. For standard low-risk products, the manufacturer can still use an internal control procedure to assess and document conformity. But the Smart Baby 3000 has a camera looking straight into my child’s room. That can’t be standard risk, can it? Quite right. Such products fall into the category of important products with digital elements. These are subdivided into Class I and Class II. What’s Class I? It includes things like smart-home devices with security functions, baby monitors, connected toys and password managers. If a manufacturer doesn’t work strictly to harmonised EU standards here, an independent assessment body has to be involved.

**15:59** How can I tell as a buyer? You’ll see the assessment body’s four-digit identification number next to the CE marking. I see. What about Class II? Those are more sensitive items such as firewalls, container runtime systems and tamper-resistant microprocessors. An external third-party assessment is always compulsory there. No exceptions. That’s quite something. But the law also mentions a category of critical products. What’s in that if firewalls are already Class II?

**16:31** These are the central nervous systems of our infrastructure. An example? Think of smart meter gateways that control our power networks, or hardware security modules that manage cryptographic keys for large banks. The EU goes all the way here. By means of delegated acts, the Commission can make obtaining a European cybersecurity certificate compulsory for these products. Before they can even be sold? Exactly. At least at the substantial or high assurance level. They can’t be put on the market before that. That will really change the market. As a customer in the shop I’ll look beyond the camera’s megapixels to the certification and the length of update support on the box. Exactly.

## Reporting and information sharing

**17:14** There’s another point that really made me stumble when I read it. Go ahead. What happens in a crisis? Even with SBOMs and independent assessments, there are going to be hacks. Hackers are creative. Of course. There’s no such thing as a hundred per cent security. Quite. I read something in the text about a reporting deadline. Twenty-four hours. Yes, the 24-hour rule. Picture it: an actively exploited vulnerability turns up at my company. My servers are on fire, so to speak. The IT department is in a complete panic. We’re desperately trying to take systems offline.

**17:53** And that’s when the EU expects me to sit at my desk and fill out forms within 24 hours? That’s precisely the part that left many executives gasping. Understandably. But let’s take a closer look at the process. If there’s an actively exploited vulnerability or a severe security incident, you have to issue what’s called an early warning. Without undue delay and within 24 hours at the latest. To whom? It goes to a single central reporting platform run by ENISA, the EU’s cybersecurity agency. The platform then distributes the report to the relevant national computer security incident response team, the CSIRT for your country.

**18:36** That sounds mad. Think it through. I report a major, completely unpatched vulnerability to an EU database. What if the database gets hacked, or a member of staff talks? I’ve just supplied a detailed set of instructions for getting into my system, and I don’t even have a patch ready. Surely that makes things much worse. I see your point. That’s a very legitimate concern.

**19:03** The EU has thought about that too. The idea isn’t to broadcast vulnerabilities to the whole world immediately. There are strict rules for sharing information. Such as? For cybersecurity reasons, sharing the report can be delayed or the information can even be completely anonymised. So they keep it confidential? Exactly. The relevant CSIRT can decide, “Sharing this with other states now could cause a catastrophe. We’ll hold it back until the manufacturer has released the patch.” I see. And then, as the manufacturer, you have to submit a detailed final report at the latest 14 days after the fix becomes available. Until then the information is often tightly restricted.

**19:45** So there’s a kind of quarantine for the information. But why all the urgency? Why put me under that pressure in the first 24 hours if they’re going to keep it confidential anyway? Because of the European single market and what’s called the blast radius. Blast radius? The extent of the damage. Exactly. The blast radius of a hack. A server on fire at a manufacturer in France could be just a local problem for them today. Tomorrow morning, it could be a systemic security problem for connected hospitals in Germany and power networks in Italy.

**20:20** That makes sense. The 24-hour early warning tells national defence centres that a wave is heading their way. They can warn critical infrastructure operators, block specific network traffic and secure networks before the attack spreads widely. Okay, I have to admit that makes perfect sense. It’s like an early-warning system for tsunamis. Precisely. But what happens if a company simply ignores those 24 hours, or cheats more generally by failing to design its product securely? What are the sanctions? Presumably more than an angry letter from Brussels?

## Market surveillance and the timetable

**20:55** A lot more. Market surveillance authorities are getting real teeth. They can order products to be recalled across Europe, with enormous reputational damage and costs for the company. And fines? Yes. They can impose steep fines, in the tens of millions or based on a percentage of worldwide annual turnover, whichever is higher. That hurts.

**21:23** But, and this is important for proportionality, there are exceptions so that start-ups and tiny businesses aren't wiped out by a purely procedural mistake. Thankfully. Yes, microenterprises and small enterprises aren't fined just because they miss that extremely tight 24-hour deadline, provided they otherwise cooperate with the authorities. A bit of leniency for the little guys. Fair enough. How much time does the industry have to change its old habits? When does this sheriff get to work in the digital Wild West?

**21:58** The timetable is tight, but it's staggered. The CRA generally applies from 11 December 2027. That's when the new CE marking and the design obligations fully take effect. But watch out: the duty to report vulnerabilities and incidents, that 24-hour rule we've just been discussing, starts more than a year earlier, on 11 September 2026. From that point the clock is ticking in a crisis.

**22:28** Wow. Let's briefly sum up, because that was a lot to take in. The Wild West of insecure IoT devices and software full of holes is finally getting a strict rulebook. From a basic smart-home camera to a password manager and right down to microprocessors, security from the factory is becoming a legal requirement. Right. Five years of guaranteed updates will be the norm. Manufacturers will need an SBOM to know exactly which digital ingredients their products contain. If you use open source commercially, you're liable for it. And if you're hacked, you have to report it in a highly secure system within 24 hours. Nicely put.

**23:09** It really is an enormous step. Anyone hoping to sell in the lucrative EU market will have to adapt, whether the company is based in Munich, Silicon Valley or Shenzhen. That's the most important tip I have for you if you're listening. Next time you buy software for your home or roll out a new IT solution at work, ask the vendor about the SBOM. Ask specifically when the guaranteed support period ends. Good advice. Once the CRA applies, you have a legal right to those answers. You won't have to buy the digital equivalent of a pig in a poke. Absolutely. You're buying a product for which the manufacturer really has to account.

## Product liability and closing thoughts

**23:54** We've spent so much time on fines and infringements today, but something else struck me when I reread the text. What was it? I nearly missed it the first time. And it might be the biggest thing of all. Look at recital 31 and you'll find a small, easily overlooked cross-reference. I think I know where you're going. It says the Cyber Resilience Act works hand in hand with the new EU Product Liability Directive. Regulation 2024/2853. Oh yes, the Product Liability Directive.

**24:30** That’s the legal wrecking ball that takes things to another level. Think about it. The directive introduces the principle of no-fault liability for software. That’s huge. In practical terms, suppose a manufacturer doesn’t send you a timely security update, which under the CRA is their legal duty, and you suffer damage as a result. Your company network is brought down through that very vulnerability, or your account details are stolen from the baby monitor. You could sue the manufacturer directly for damages.

**25:05** Right. Regardless of whether the manufacturer directly caused the hack. The missing update alone is enough to establish liability. We’re no longer talking just about fines paid to the state. We’re talking about users bringing civil claims worth millions. Something’s just dawned on me. Will the fear of massive damages claims finally make the tech industry give up that old Silicon Valley motto, “Move fast and break things”?

**25:31** That’s a brilliant conclusion, because that’s precisely what follows from all this. “Move fast and break things” works only as long as you don’t have to pay for what breaks. And that’s changing for good. A new era for software, I’d say. Think about that this evening when you install the next update on your phone. Cybersecurity used to be more a matter of faith. With the Cyber Resilience Act we finally see an attempt to make security visible, measurable and, above all, enforceable in court. That’s our deep dive for today. Stay curious.