Quo vadis CRA? Chancen und Herausforderungen aus der Sicht eines Produktherstellers

Marko Wolf [1)], Alexander Eisenberg[2)], Michael Jochem[1)] et al.
[1)]Robert Bosch GmbH, [2)]BSH Home Appliances S.A.

OMNISEC Forum 13-A | Europäische Cybersicherheitsstandards für Consumer IoT
Berlin, May 23rd, 2023

BOSCH

1

Delayed gratification

BOSCH

Delayed gratification
The diner

Marko Wolf (C/CYG-GP) | 2023-05-23

Delayed gratification
The marshmallow test

Walter Mischel
American psychologist, Stanford University

Photo: FLY:D auf Unsplash

Human preference for **smaller but instant rewards** (*instant gratification*) **over larger but delayed rewards** (*delayed gratifications*) or even over long-term pains (*procrastination*).

Delayed gratification
Beyond the marshmallow test

Some related real-life “Applications”

Cybersecurity!

Delayed gratification
“*A **quick win eats security** for breakfast*”

Product manufacturers usually:

- Need predictable risks and predictable costs (which ‘moving target’ security cannot provide)
- Prefer features w/ positive customer experience (while ‘good security’ should not need any UX/CX)
- **Prefer instant savings** on costs, complexity, time, resources etc. (“1st marshmallow”)

Product users usually:

- Cannot really assess security risks nor protection level of a product (since both is hard/impossible to quantify)
- Care little about cybersecurity (“2nd marshmallow”)
- **Do not want to pay** much for (extra) cybersecurity

Resulting amongst others into**:**

- ⓘ **Low product cybersecurity** that yields to:
  - ⓘ Long-term pain for product users (e.g., hack)
  - ⓘ Long-term pain for manufacturer (e.g., recall)
  - ⓘ Long-term pain for others business & society
- ⓘ **Unfair competitive advantages** at the expenses of others (e.g., consumers, environment, society)

Like safety, environmental, or labor protection, **cybersecurity protection will not work without some regulation**. A cybersecurity law is needed to:

- ➢ Ensure **minimum protection** for product users, business, supply chains, infrastructure
- ➢ Enable **fair competition** at EU market (again)

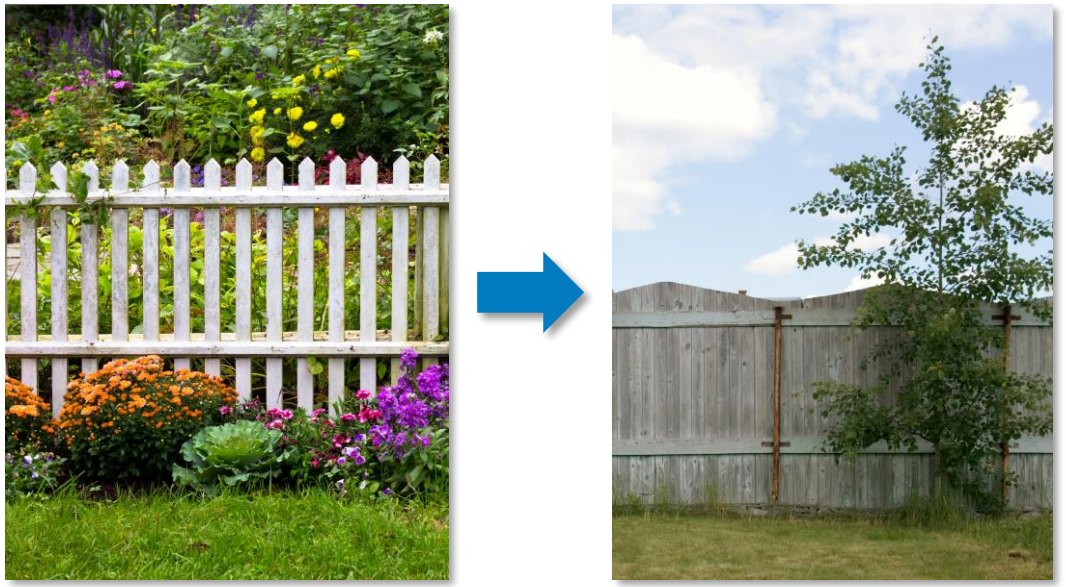
Marko Wolf (C/CYG-GP) | 2023-05-23

2

Cyber Resilience Act in a Nutshell

European Cyber Resilience Act (CRA)
Product Cybersecurity becomes Law!

- Ensure that **digital connected hardware and software** products placed on the EU market have **fewer cybersecurity vulnerabilities.**
- **Better protection** for **consumers**, **business users**, **supply chains**, and **IT infrastructures**.



- Requires **secure-by-design** and **secure-by-default** approach plus regular **security testing**
- Select and implement essential product security requirements **based on product risk analysis**
- Based on **well-established New Legislative Framework** for product-related legislation (CE)
- **Improve transparency** on security properties and security vulnerabilities of products.

- **Manufacturers remain responsible for cybersecurity** up to 5 years after product sales.
- **Strong market surveillance** and penalties up to **15 m€** or **2,5% worldwide annual turnover**.

European Cyber Resilience Act (CRA)
CRA vs. ETSI EN 303 645

Phase	Item	European Cyber Resilience Act (Draft, 09/2022)	ETSI EN 303 645: Cyber security provisions for consumer IoT (V2.1.1)
Design	Access control	Yes, by “appropriate control mechanisms” (I.1.b)	Yes, incl. HW-protected memory access control (5.5-4, 5.5-5, 5.6-8)
	Secure update facility	Yes, automatic where possible incl. user info (I.1.k)	All SW components; automatic on startup and periodically; user info/options, if not updatable (5.3)
	Secure storage	No direct requirement	Yes, with unique per device parameters (5.4)
	Secure comm.	Yes, but w/o further details on conf	crypto, if possible (5.5)
	Secure boot	No direct requirement	(5.7)
	Security logging	Yes, incl. local monitoring where p	
	Min. attack surfaces	Secure-by-default (I.1.a); Yes, in g	ault (e.g., passwords,
	Privacy protection	Factory-reset (I.1.a); Confidentialit minimization (I.1.e)	er for any “external); Data protection (6)
	Resilience	Availability of “essential functions” w/o further details (I.1.i)	ver outages esp. regarding ation (5.13)
	Impact on others	Minimize their own negative impac	
Produce	SBOM	Yes, incl. machine-readable and fo	
	Secure dev. process	Risk-based approach over complet	risk assessment)
	Secure prod. process	No direct requirement	
	Documentation	Risk assessment (10.3); Vulnerabi for 10 years; User instructions (10.	curity limitations (5.3);
	Conformity assessment	From self-assessment up to EUCC	ex B)
Operate	Deployment	Delivered w/o any vulnerabilities (I.	
	Disclosure policy	Yes, once a security update has be	.2-1)
	Monitoring incl. 3P	Up to 5 years (10.6)	s” detection (5.10)
	Regular testing/reviews	Yes (I.2.3)	Not direct requirement
	Vulnerability Reporting	Active exploits within 24h to ENISA (11.1); “Without delay” to users (10.4) and 3P components (10.7); Reporting includes all legacy products (55.3)	To affected stakeholder or national authorities (5.2-3)
	Vulnerability Sharing	Passive “facilitate the sharing” incl. 3P (I.2.6)	Optional for authorities and industry bodies (5.2-3)
	Security patches	Within “a timely manner” (I.2.7) and “free of charge” (I.2.8); Up to 5 years	Within 90 days for SW (5.2-2); during defined support period; no info on costs

- **Scope of CRA** is **larger** than EN 303 654
- Over **70%** of both **requirements overlap**
- **CRA** remains **more general** (as law text)
- **CRA** includes more **explicit requirements** on processes especially **on vulnerability management process** during operation
- Both **do not address cybersecurity risks during production** (e.g., vs. credential theft/cloning)

Included | Partial | Missing

Marko Wolf (C/CYG-GP) | 2023-05-23

BOSCH

3

Cyber Resilience Act from a Manufacturer’s Perspective

BOSCH

Cyber Resilience Act from a Manufacturer's Perspective
Selected **Chances** with CRA at Bosch

- **Harmonized, horizontal product cybersecurity legislative act** based on well-established **NLF principles** that **avoids fragmentation** of product cybersecurity requirements (cf. MD, AIA, RED, eIDAS, DORA).
- **Risk-based approach** based on intended / foreseeable use to realize **economic cybersecurity**.
- **Mainly based on self-assessment** with (**tbd**) product-specific standards.
- Clear set of 13 essential **product security requirements** and 8 essential **vulnerability handling requirements** to be applied **acc. associated risk**.
- Quality- and compliance-oriented companies **should already have/use most** of the necessary processes, methods, and organizational structures.
- **Effectively increase cybersecurity for digital products placed at EU market** and hence improves cybersecurity protection for EU product users **incl. business users, EU business**, and EU society in general.

BOSCH

Cyber Resilience Act from a Manufacturer's Perspective
Selected **Challenges** with CRA at Bosch

- **Creates additional efforts, complexity, and costs** since (better) security unfortunately does not come for free.
- Interplay with the security requirements from **Radio Equipment Directive** (DA 2022/30).
- Application to **(automotive) components, incomplete products, spare parts, accessories**.
- Exclusion of non-commercial **open-source software** (activities).
- **Static** ("random") **product criticality classification list** for assessment depth that will always be incomplete, outdated, too wide/narrow etc.
- **Reporting obligations** (any,24h) going beyond similar regulations like NIS2
- Short **transition phase** (24m) for industry, **hEN**, and notified bodies.
- Interplay of **NLF with software and agile SW development** like DevOps.
- ENISA becomes **central point of attack** for 0-day hackers and espionage.

BOSCH

Summary

BOSCH

Cyber Resilience Act from a Manufacturer's Perspective
Summary

- We **support CRA** because its benefits clearly outweigh the necessary efforts.
- Some **improvements are still needed** to make it more practicable & effective.
- **ETSI EN 303 645** could serve as **starting base** for CRA standardization, while more domain/process standardization is required.
- **Alignment with other cybersecurity regulations** from other domains (e.g., automotive) and other regions (e.g., USA, Japan) remains essential for efficient and effective product cybersecurity worldwide.
- **Better wait for second marshmallow** 😉

Photo by FLY:D auf Unsplash

BOSCH