CYBERSTAND.eu

Impacting the CRA

Defining standards for the future

14:15 - 15:30

Breakout session 3:
Risk management and assessment

Minerva Room

Chair: *Lucia Lanfri, CEN-CENELEC*
Panelists:
Ben Kokx, Philips

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Co-funded by the European Union

slido

Join at

slido.com

#2475 503

CYBERSTAND.eu

Essential requirements of the Cyber Resilience Act

Risk management and Risk Assessment

www.cyberstand.eu

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Meet your speaker

Ben Kokx

Director Standardization Product Security, Philips, Eindhoven, Netherlands:

- 24 years with Philips, started as software designer, 23 years in product security
- Currently responsible for Product Security related Standards & Regulations
- Previous roles: Responsible for the Philips Global Product Security Policy and Process Framework, Product Security and Privacy Officer for interventional x-ray products

Leading roles:

- Chair of the MedTech Europe Cybersecurity focus group
- Chair of the COCIR Security and Interoperability working group
- Convenor of CEN/CENELEC JTC13 - WG6, WG8 and WG9, developing harmonized standards for the RED Delegated Regulation and the Cyber Resilience Act

Expert roles:

- ISO TC215, IEC TC62, IEC TC65, IEC ACSEC, ISO/IEC JTC1 SC27 WG1 & WG4, ETSI TC-CYBER, and several other international and regional TC's
- Member of various expert groups of the European Commission including CRA
- Member of the AdvaMed, MITA, Online Trust Coalition, Digital Europe, APPLiA and many other public-private, industry and standards organizations….

Risk assessment, Risk management, Risk classification and Risk levels…

- **Risk assessment** is the process of identifying and analyzing potential hazards. You look at what could go wrong, how likely it is to happen, and what the impact might be. It's about understanding the risks.
- **Risk management** goes a step further. It involves taking action to minimize or control those risks. You create and implement strategies to reduce the impact of those identified hazards. It's about handling the risks during the total product life cycle. Risk assessment is part of risk management.
- **Risk classification** is about categorizing risks. You group them based on their nature or source, like financial, operational, or strategic risks. It helps prioritize and address them more effectively.
- **Risk levels** indicate the severity and likelihood of risks. Typically, a 3 scale low to high or a 5 scale very low to critical.

We need to indicate which “risk assessment” we are talking about

- A manufacturer needs to conduct a **regulatory compliance risk assessment** to identify the possible risks with a product based on the intended use, used technologies, etc., this is based on the generic capabilities.
- Example for an electric heater with WiFi for personalized settings:
  - The product uses mains power LVD is in scope because of the electric risks
  - The product is a heater In scope of the GPSR because of risks for burning and fire
  - The product has a WiFi radio transmitter/receiver In scope of the RED
  - The product has a (WiFi) internet connection In scope of the RED/DA CRA
  - The product processes personal data RED 3.3.(e) applies & probably the GDPR
  - Etc..

We need to indicate which “risk assessment” we are talking about

- A manufacturer needs to conduct a **product security risk assessment** as part of the risk management activities to identify the possible risks with the implementation and used technologies, etc., to improve the design:
- Example for an electric heater with WiFi for personalized settings:
  - The product receives commands from the internet Risks of spoofing and unauthorized access (S & E from STRIDE)
  - The product accepts software updates Risks of tampering (T in STRIDE)
  - The product use personal data Risk of information disclosure (D in STRIDE)
  - The product uses insecure communication Many STRIDE related risks
  - Etc..

Hazard, hazardous situation, harm

- A shark is a hazard
- It is a property of the ocean that a shark can be present
- The shark can cause harm, but its presence alone does not mean that harm will occur
- A shark by itself does nothing

- Swimming with a shark is a hazardous situation!
- A situation where you are exposed to a hazard, and where harm could occur
- One step away from harm, but it hasn't happened yet

- Possible/actual harm
- Injury to skin, muscles, tendons
- Broken bones
- Blood loss
- Damage to property (your surfboard)

Risk control

- Inherently safe design (control the hazard)

- Protective measures (control hazardous situation)

- Information for safety (control behavior to avoid harm)

Dealing with risk

Total Product Life Cycle

total product life cycle (TPLC)

development, support and end of support stages in the life of a product.

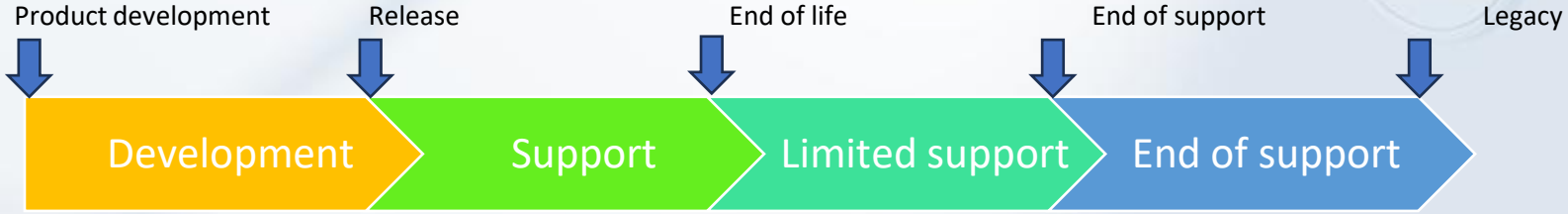
Note to entry: A limited support stage might be optionally planned between support and end of support

end of life (EoL)

point in time in the life cycle of a product starting when the manufacturer no longer supports the product beyond its useful life as defined by the manufacturer and the product has gone through a formal EOL process including notification to users.

end of support (EoS)

point in time in the life cycle of a product starting when the manufacturer terminates all service support activities and service support does not extend beyond this point.



The basics

- **Product with digital elements** means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;
- CRA Essential Requirement Part I (1): Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.
- As such we need to determine the risks to the product with digital elements.

Risk

- **Risk** is a combination of the consequences (magnitude of impact) that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event (ISO 27005:2018)
- Any event comprising the availability, authenticity, integrity or confidentiality of stored, transmitted, or processed data, or of the related services offered by, or accessible via, network and information systems is called an **incident.**
- Incidents can be caused by attacks or accidents. The potential cause of unwanted incidents which may cause harm to a system, individual or organization is called a **threat**. (ISO 27032:2012)

Risk

- Such threats can manifest from a weakness of an asset or control that can be exploited. (ISO 27000:2018) This is called a **vulnerability.**
- An **asset** here is anything that has value to an individual, an organization or a government (ISO 27032:2012).
- As such. To determine the appropriate level of cybersecurity based on the risks we need to know:
  - what the assets are;
  - to what risks these are exposed;
  - to what extend these need to be protected.

What risks?

Free from unacceptable risk resulting in:

- Injury or death
- Privacy violations (eavesdropping, identity theft, surveillance)
- Data loss and theft (ransomware, phishing attacks)
- Being denied access to critical infrastructures, e.g.,
  - electricity and gas,
  - phone and internet,
  - transportation (roads, planes and trains),
  - financial systems,
  - medical care
- Breaking into your home
- Breaking into your bank account (financial loss)
- Products not functioning as intended
- Cyberwarfare attacks

Context

- To determine the risk we first need to understand our product with digital elements, we need to establish the context of the product.
- The product context is comprised of:
  - The products intended and reasonable foreseeable use;
  - The products functions;
  - The products system architecture;
  - The products intended and reasonable foreseeable environment;
  - The products intended and reasonable foreseeable user;
  - The products intended support period.

Context

- The products intended and reasonable foreseeable use of the product forms a basis needed to determine the risk acceptance criteria. A smart card used for access nuclear powerplants has a different risk profile than one used to open a piggy bank toy or the company gym.
- The products functions are needed to determine potential attack surfaces and can also play a role in the impact of potential risk.
- The products system architecture grants insight in the interplay between the products elements and as such display how threats can pro.

Context

- The products intended and reasonable foreseeable environment grants the manufacturer insight in potential attack vectors as well as intrinsic defenses expected at these environments. Like products in a secure network or products publicly accessible.
- The products intended and reasonable foreseeable user grants insight into the ability of the user to ensure their own protection and as such the risks they can be safely exposed to due to their own ability to mitigate the risks.
- The products intended support period grants insight needed for the selection of components based on legally required support periods.

Risk acceptance criteria

- Using the product context the risk acceptance criteria can be established. These criteria will differ depending on the products intended use, reasonably foreseeable use, operational environment and user. And are established on behalf of the user.
- Defining risk acceptance criteria is difficult and sector/ use case specific. It's important to ensure that whatever is used to establish the risk acceptance criteria the criteria:
  - Account for the nature and type of risks inherent to the products functions, including health and safety of the user;
  - Are transparent about how the risks are defined and measured;
  - Are consistent in their application.

Further risk acceptance criteria considerations

- See article's 7 and 8 of the CRA for further specific guidance
- Is the product B2C or B2B/B2G?
- Is the product part of the critical infrastructure?
- Is the product processing personal data? and of special categories?
  - If yes, how many data subjects
- If an exploitable vulnerability is discovered and exploited:
  - How many users are impacted (a few, 100's, 1000's or millions)?
  - How disruptive is it to the end user or society?
  - Can it lead to an impact on safety?
- Does it contain critical AI?
- How significant are the financial / legal consequences for the manufacturer?
- How significant are the financial / legal consequences for the user?
- etc…

Typical product security risk assessment steps

1. Scoping / Identify and classify assets
2. Identify risks via Threat modeling / Security test results / Requirements review, etc.
3. Estimate likelihood and/or exploitability
4. Estimate impact
5. Calculate initial risk
6. Identify mitigations / controls
7. Calculate residual risk
8. Manage residual risk (could include impact on business risk)
9. Assess linkage to safety hazards

Asset identification

- With the product context in mind, we can now identify the product with digital element's assets.
- This can include things such as:
  - Data stored, processed or transmitted by the product;
  - Functions of the product used by or accessible through the product.
- Depending on the nature of the data this could be financial, or privacy sensitive data. The nature of the assets can influence your risk acceptance criteria. This is something you already know from your context as this would be part of intended use.

Threat identification

- Threat modeling:
  - Threat modeling is a systematic approach for analyzing the security of an item in a structural way such that vulnerabilities can be identified, enumerated, and prioritized, all from a hypothetical at-tacker's point of view.
  - Threat modeling can be applied to a wide range of things, including software, devices, systems, networks, distributed systems and business processes.
  - Threat modeling typically employs a systematic approach to identify attack vectors and assets most desired by different threat actors. This leads to a decomposition of the item (software, device, system, and so on) to look at each possible attack vector and asset individually and determine to which kind of attacks they are vulnerable. From this, a list of vulnerabilities can be created and ordered in terms of risk, potential to impact safety, effectiveness, or any other criteria deemed appropriate (like privacy).
  - Various threat modeling techniques exist (STRIDE, VAST, OCTAVE, PASTA, DREAD, TRIKE, etc.)
- Various other sources like the results of security testing, req. reviews, etc.

The four Threat Modeling Questions That Must Be Answered

What are we working on?

- Provides common understanding
- Provides scoping
- Create data flow diagrams
- Create swim lane and state diagrams

What can go wrong?

- Identify threats
- Look at assets, boundaries
- Attack vectors

What are we going to do about it?

- Eliminate, Mitigate,
- Accept or Transfer

Did we do a good job?

- Reflection of whether all threats were found, and all treated
- What went well?
- What went poorly?
- Document activities & track progress

Risk determination

- Each of these threats will, depending on the model, have a likelihood and magnitude of impact. This is also where vulnerabilities play a role. An asset that cannot be exploited is not a risk as the likelihood of the occurrence would be zero.
- The best methodologies to determine the risk will again be sector or product category specific. As such the most important factor here is consistency in the applied methodology and documentation of the risks.

Risk evaluation

- Now that the risks are determined we can compare them to the previously established risk acceptance criteria.
- From this comparison we can learn if the risk is acceptable or if risk mitigation is required.
- If the risk is treated there might still remain residual risk. If this residual risk is acceptable it is transferred to the user. This means that typically there is always some amount of risk that ends up with the user.
- This is why communication (within reason) about risks is critical so the user can either accept it or mitigate it further.

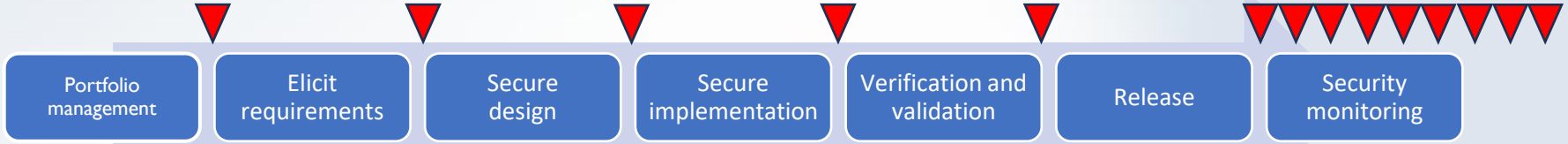
Risk treatment

- After the assessment of the risks we now know if the risks are acceptable or not. For those that are not acceptable we require to take additional action.
- We can attempt to avoid the risk by cutting the function/feature that causes the unacceptable risk.
- We can apply cybersecurity controls to reduce the risks, like implementing authentication mechanisms or whatever is applicable to mitigate the specific risk.

But you are not done yet

- Risk is ever evolving. The threat landscape can change and new vulnerabilities can be discovered.
- Risk assessments are not a one and done activity. Its a constant process. New vulnerabilities are found. You select controls, that impacts your product, meaning your assets might change. Which requires you to repeat many of these steps.
- The specifics of how often to review these steps might differ per product but as long as its connected there will always be the risk that you have to do this all again.
- As such its important to make sure you have this process ready and have a product designed in such a way it can adjust to the changing threat landscape.

When to execute a risk assessment



- At every phase of the development process to:
  - Verify your initial user specification has cyber security risks
  - Verify your requirements address the perceived risks
  - Verify the design uses secure components and addresses defense in depth
  - Verify requirements are satisfied and vulnerabilities are mitigated
  - Continuously assess after release till end-of-life if new vulnerabilities have emerged, and incidents and changes in the threat landscape are evaluated
- Risk management is the entire process, including reverting back in the process to address any risks identified which requires mitigation

Cybersecurity risks obligations for the manufacturer

- 13.2 For the purpose of complying with paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users.
- 13.3 The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.
- 13.7 The manufacturers shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products.

Annex I, Part I - Essential (Product) requirements

Cybersecurity requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

a) be made available on the market without known exploitable vulnerabilities;

b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorized access;

e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (minimisation of data);

h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

j) be designed, developed and produced to limit attack surfaces, including external interfaces;

k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Risk assessment inputs and acceptance criteria

- Risk assessment is done at an engineering level where various inputs such as but not limited to product design documentation, threat modeling, pen testing, vulnerability management, requirements evaluation, code analysis, supply chain risks and brainstorming with a multi disciplinary team will identify vulnerabilities which are risk assessed and controlled to an acceptable level.
- This acceptable level depends on the intended use, the intended operational environment of use, regulatory obligations, the state-of-the-art and various other considerations such as the attack potential the manufacturer intends to be resilient against / is expected as a minimum by the state-of-the-art.

THE CRA HORIZONTAL STANDARDS DO NOT ENFORCE ANY METHODOLOGY!

Example methodology: OWASP Risk Rating

OWASP Risk Rating Methodology

https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

- Step 1: Identifying a Risk
- Step 2: Factors for Estimating Likelihood
- Step 3: Factors for Estimating Impact
- Step 4: Determining Severity of the Risk
- Step 5: Deciding What to Fix
- Step 6: Customizing Your Risk Rating Model

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

THE CRA HORIZONTAL STANDARDS DO NOT ENFORCE ANY METHODOLOGY!

Example methodology: OWASP Risk Rating

OWASP Risk Rating Methodology

https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

- Step 1: Identifying a Risk
- Step 2: Factors for Estimating Likelihood
- Step 3: Factors for Estimating Impact
- Step 4: Determining Severity of the Risk
- Step 5: Deciding What to Fix
- Step 6: Customizing Your Risk Rating Model

Threat Agent Factors

The first set of factors are related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by this group of threat agents. Use the worst-case threat agent.

- **Skill Level** - How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)
- **Motive** - How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)
- **Opportunity** - What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
- **Size** - How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

THE CRA HORIZONTAL STANDARDS DO NOT ENFORCE ANY METHODOLOGY!

Example methodology: OWASP Risk Rating

OWASP Risk Rating Methodology

https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

- Step 1: Identifying a Risk
- Step 2: Factors for Estimating Likelihood
- Step 3: Factors for Estimating Impact
- Step 4: Determining Severity of the Risk
- Step 5: Deciding What to Fix
- Step 6: Customizing Your Risk Rating Model

Vulnerability Factors

The next set of factors are related to the vulnerability involved. The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.

- **Ease of Discovery** - How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)
- **Ease of Exploit** - How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)
- **Awareness** - How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)
- **Intrusion Detection** - How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

THE CRA HORIZONTAL STANDARDS DO NOT ENFORCE ANY METHODOLOGY!

Example methodology: OWASP Risk Rating

OWASP Risk Rating Methodology

https://owasp.org/www-community/O

- Step 1: Identifying a Risk
- Step 2: Factors for Estimating Likelihood
- Step 3: Factors for Estimating Impact
- Step 4: Determining Severity of the Risk
- Step 5: Deciding What to Fix
- Step 6: Customizing Your Risk Rating Model

Technical Impact Factors

Technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability. The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.

- **Loss of Confidentiality** - How much data could be disclosed and how sensitive is it? Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)
- **Loss of Integrity** - How much data could be corrupted and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)
- **Loss of Availability** - How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)
- **Loss of Accountability** - Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9)

THE CRA HORIZONTAL STANDARDS DO NOT ENFORCE ANY METHODOLOGY!

Example methodology: OWASP Risk Rating

OWASP Risk Rating Methodology

https://owasp.org/www-community/OV

- Step 1: Identifying a Risk
- Step 2: Factors for Estimating Likelihood
- Step 3: Factors for Estimating Impact
- Step 4: Determining Severity of the Risk
- Step 5: Deciding What to Fix
- Step 6: Customizing Your Risk Rating Model

Business Impact Factors

The business impact stems from the technical impact, but requires a deep understanding of what is important to the company running the application. In general, you should be aiming to support your risks with business impact, particularly if your audience is executive level. The business risk is what justifies investment in fixing security problems. The factors below are common areas for many businesses, but this area is even more unique to a company than the factors related to threat agent, vulnerability, and technical impact.

- **Financial damage** - How much financial damage will result from an exploit? Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
- **Reputation damage** - Would an exploit result in reputation damage that would harm the business? Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)
- **Non-compliance** - How much exposure does non-compliance introduce? Minor violation (2), clear violation (5), high profile violation (7)
- **Privacy violation** - How much personally identifiable information could be disclosed? One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)

Sander's kitchen knife

- An example of risk can be found in an everyday household item, the humble kitchen knife.
- Its intended use is to cut vegetables, meats, etc. It might even be used to cut paper, plastic packages or rope.
- This is possible due to the inherent property of the knife: it is sharp.
- Its sharpness however conveys risks:
  - You could cut yourself;
  - It could slip out of your hand and land on your foot.

Sander's kitchen knife

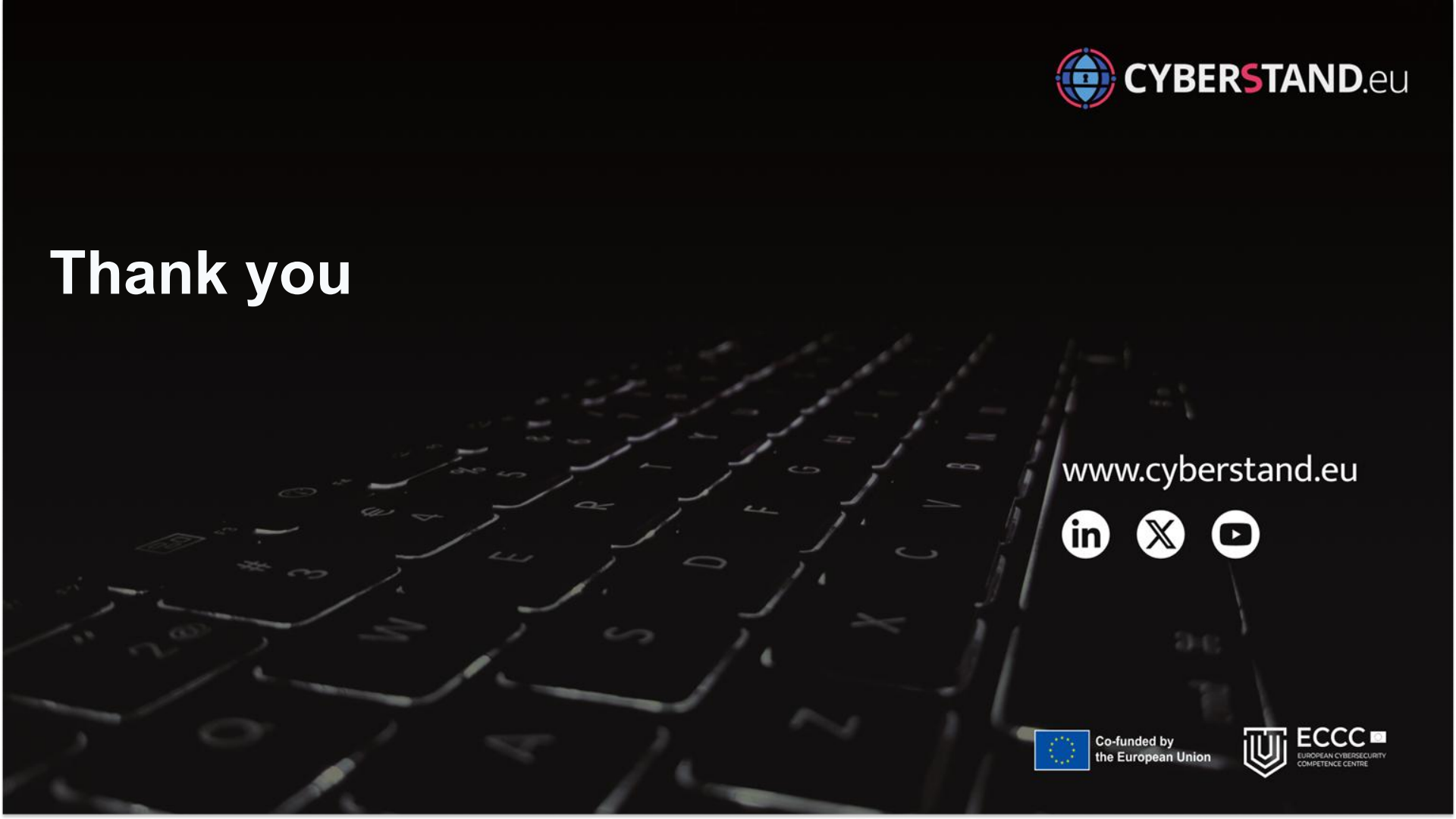
- Some of these risks can be mitigated:
  - We can blunt the knife on one side;
  - We can give the knife a round tip;
  - We can give it a better handle with more grip and a safeguard.
- However, we cannot fully mitigate the risk of cutting as this is inherent to the knife due to its intended function. It needs to be sharp.
- As such some risk is transferred to the user. This is communicated, and safe usage or mitigation measures on the side of the user of the product are expected.

Cybersecurity requirements for products with digital elements — General principles for cyber resilience

- The General principles for cyber resilience standard defines the overall expectations for risk management including all the activities to develop and maintain the security of products with digital elements

CYBERSTAND.eu

Thank you



www.cyberstand.eu

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE