Are You Prepared For the Cyber Resilience Act?

Kir Nuthi, Senior Policy Analyst, Center for Data Innovation, @kirtinuthi
Questions We’ll Answer

1. What Does the Cyber Resilience Act Cover?
2. What Is Security-By-Design?
3. What Are the Act’s Essential Requirements?
4. Who Oversees and Enforces the Cyber Resilience Act?
5. What Are the Key Compliance Challenges Facing Businesses?
Why the Cyber Resilience Act?

The Issue of Cybercrime:
In 2020, global cybercrime cost €5.5 trillion, and global cybercrime will likely cost $10.5 trillion by 2025.

The EU’s Proposed Solution:
A broad horizontal regulatory framework of tangible and intangible products with digital elements—including connected devices and non-embedded software—to enforce cybersecurity standards on the entire digital supply chain.
Objectives of the Cyber Resilience Act

**Ensure Life-Cycle Cybersecurity**
To ensure manufacturers improve the cybersecurity of covered products throughout the whole life cycle

**Prevent Legislative Fragmentation**
To create a single coherent framework for cybersecurity compliance in the EU

**Increase Transparency**
To increase the transparency of cybersecurity practices and properties of products and their manufacturers

**Protect Customers**
Provide consumers and businesses with secure products ready for use
Scope

“Any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately”
Covered Product Classification

**Class I**
Faces critical cybersecurity vulnerabilities but have a lower cyber security risk than Class II products

**Class II**
Higher-risk products with digital elements with regard to critical cybersecurity vulnerabilities

**Unclassified or Default**
Covers 90% of connected devices and applies to products without critical cybersecurity vulnerabilities
Exempt from the Cyber Resilience Act

Devices Already With Sectoral Legislation

Some Free Open-Source Software
If developed or supplied outside the course of commercial activity, i.e. not charging for a product or technical support service, not providing a software platform where the manufacturer monetizes other services, or not using personal data for reasons that don’t improve security, compatibility, or interoperability
Security-By-Design in the Cyber Resilience Act

**Security-By-Design**
Requires companies to address information security and other cybersecurity vulnerabilities during the initial design and development of products.

**Essential Cybersecurity Requirements**
Security requirements and properties covered products **must** have, including secure-by-default configurations and avoiding known exploitable vulnerabilities.

**Vulnerability Handling Requirements**
Requirements put in place to ensure products comply with the regulation and ensure the cybersecurity of covered product in every part of their life cycle.
Enforcement of the Cyber Resilience Act

European Union Agency for Cybersecurity (ENISA)
Must be notified within 24 hours after becoming aware of “any actively exploited vulnerability” or “any incident having impact on the security” of a product

National Market Surveillance Authorities
Ensure the implementation of the Cyber Resilience Act, cooperate with authorities designated under NIS2 and the 2019 cyber security certification regulation, cooperate with ENISA, conduct sweeps, and impose administrative fines

Penalties
Vary depending on the type of noncompliance, the highest penalty costing either €15 million or 2.5 percent of their global annual turnover for the previous fiscal year
Key Compliance Challenges

**Definitions**
Definitions need to be clearer and consider how different products work, their varying vulnerabilities and functionalities, and development processes.

**Added Compliance Burdens**
Extra costs may burden development and innovation as businesses have warned or ultimately fall to consumers.

**Overlap of Reporting Obligations**
Need consistency and clarity in the overlap between NIS2 and Cyber Resilience Act reporting obligations and their interactions with national authorities and ENISA.
Key Compliance Challenges Continued

**Drawing Lines Between Stages of Software Development**
Some interpretations fail to distinguish between originators or providers and developers of software

**Broad Interpretation of Commercial Activity for Open Source Software**
The proposal lacks a clear definition of commercial activity and could disrupt the activity of open source distributors on GitHub and of open source organizations that provide consultations
Next Legislative Steps

**Implementation After 12 Months**
Manufacturers and developers obligated to report exploited cybersecurity vulnerabilities and breaches

**Implementation After 24 Months**
Member states and affected businesses must adapt to new requirements proposed

**After Implementation and Entry Into Force**
EU can re-review regulation, create sectoral regulation for specific vulnerabilities, and within twelve months of entry into force adopt delegated acts specifying product category definitions


Thank you!

Kir Nuthi, knuthi@datainnovation.org, @kirtinuthi

Icons used in the presentation are by Icons8