Bug bounty and the EU Cyber Resilience Act – everything you need to know

BY INTIGRITI · MARCH 14, 2023 · LAST UPDATED ON MARCH 6, 2025

The EU Cyber Resilience Act aims to protect Europe from increasingly sophisticated cyber-threats.

The first quarter of 2023 has seen significant cybersecurity legislation coming out of the European Union (EU).

In early February, we reported on the adoption of the NIS2 Directive – a major EU cybersecurity initiative – and today we'll focus on another sweeping piece of legislation, the EU Cyber Resilience Act, which is set to shake up how manufacturers, importers and distributors of hardware and software within the EU market do business.

What is the purpose of the EU Cyber Resilience Act?

The EU has set a high bar in implementing what it calls the Digital Decade by 2030 – a set of common objectives and targets for Europe's digital transformation. In essence, this initiative is helping cause the rapid expansion in information technology in Europe.

Such expansion, of course, needs to be complemented with an equally proactive approach to cybersecurity. However, at the current time, much of the hardware and software made available by businesses operating in the EU is not bound by any legislation that requires specified levels of security.

The Cyber Resilience Act aims to address this gap by meeting several objectives, and should provide an important step forward in protecting Europe from increasingly sophisticated cyber-threats.

The act was initially proposed by the European Commission (EC) to protect European citizens and businesses, and to promote best practices in connected hardware and software cybersecurity, as well as contributing to the development of a more coherent and coordinated approach to cybersecurity at the EU level.

What are the key components of the Cyber Resilience Act?

Such wide-ranging objectives will potentially require a great deal of red tape, but some requirements of the act are, at least, clear at a glance.

Firstly, two **general objectives** were established to guarantee proper functioning of the EU internal market in digital goods and services:

1. Create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that

manufacturers take security seriously throughout a product's life cycle; and

2. Create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

Secondly, four further and more specific objectives were also indicated:

1. Ensure that manufacturers improve the security of products with digital elements from the design and development phase and throughout the whole life cycle;

2. Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;

3. Enhance the transparency of security properties of products with digital elements, and

4. Enable businesses and consumers to use products with digital elements securely.

In short, the act seeks to make products and services safer; make consumers more aware of cybersecurity; require that manufacturers ensure the cybersecurity of their products before *and* after sale; and ensure better product cybersecurity throughout the EU into the future.

What will the EU Cyber Resilience Act require of businesses in Europe?

Businesses operating in the EU will be legally bound to meet common cybersecurity requirements that will apply throughout the expected lifecycle of devices and software they make available.

Specifically, this means that any business supplying devices to the EU market will be bound to exercise a duty of care for a minimum of five years. Devices not complying will be prohibited from accessing the EU market.

The act also goes into some detail on how all devices and software will be assessed to establish their risk level and conformity within the execution of the new law.

The legislation will therefore, hopefully, create a higher level of accountability for device manufacturers and software developers, and this should, in turn, create a more secure cyber environment in the EU.

YOU MIGHT ALSO LIKE How policymakers are expanding the adoption of bug bounty programs

How will the act help businesses to become more cyber resilient and protect themselves from attacks?

The requirements of the act will undoubtedly require changes in how many device and software manufacturers operate in the EU. However, businesses are expected ultimately to benefit from the act because compliance with its standards will help them to meet ever-evolving cyber threats.

Additionally, improved levels of cyber resilience are expected to give European firms a global competitive advantage as industry standards for cybersecurity become stricter across the planet. Proactively creating

a safer digital economy in Europe now will be instrumental in the success of companies operating in both the region and beyond, in the long-term.

Finally, NIS2 is already establishing heavy penalties for businesses and individuals that do not meet its standards. As compliance increasingly becomes the norm, adopting a strong security posture will make more and more business and legal sense for all organizations.

What are the downsides of the EU Cyber Resilience Act?

The proposal of the EU Cyber Resilience Act has not been without critics. Many business owners predict it will be costly to implement the necessary security measures, and lament the bureaucracy it will engender.

Further, some producers of open source software that is distributed *as-is* are **concerned about the implications for the free and open software movement**. Will producers and distributors of software that has no commercial value *per se* be subject to the same stringent requirements as commercial producers?

What are the consequences of non-compliance with the act?

Failure to comply with the EU Cyber Resilience Act will result in penalties, and the removal of access to the EU market for vendors' devices and software.

> **"Stiff financial penalties will also be imposed, with potential fines for non-compliance ranging from either €5 – €15 million or 1 – 2.5% of global annual turnover, whichever is greater. There will, of course, also be increased risk of reputational damage from legal action that could hurt future business opportunities. "**

How can businesses make sure they are compliant with the act?

Obviously, businesses should prepare for the EU Cyber Resilience Act by proactively putting in place security practices that ensure they will not fall foul of the new requirements. Getting up to speed then staying up to date on the requirements of the law will be the first step, and it will be challenging to begin with given that the act requires compliance in all of the following areas:

Cyber Risk Management, Vulnerability Management, a Conformity Assessment Regime, an Appointed Representative, and Record Keeping.

How bug bounty programs can help businesses comply with the EU Cyber Resilience Act

Among the preemptive steps that minimize cyber risk, the proposal for the new legislation specifically includes Vulnerability Disclosure Policies (VDP) and bug bounty programs among its list of recommendations.

This is becoming increasingly the norm. Harry Grobbelaar, Chief Customer Officer at Intigriti, has been observing this trend for some time, noting that more and more recommendations are shifting from the use of pentesting to crowdsourced initiatives:

> **"Around the world, legislation is being signed that serves to not only validate but also promote bug bounty and crowdsourced security services. Interestingly, the Cyber Resilience Act is even more explicit in its terminology about the utility of bug bounty programs as part of a layered security approach – citing that, due to the fact that exploitable vulnerabilities can be sold at high prices on the black market, manufacturers are encouraged to ensure reporters of vulnerabilities receive recognition and compensation for their efforts."**

Crowdsourced bug bounty programs are thus seeing rapid adoption as an important tool for helping businesses comply with legislation, and it is likely they will perform the same role as the EU Cyber Resilience Act comes fully into effect.

Bug bounty programs like those hosted by Intigriti provide a very cost-effective way to identify and report security vulnerabilities in software, and they dramatically increase the speed at which businesses can patch security issues to keep their solutions secure.

Why this flood of major legislation?

The cyber domain is experiencing unprecedented growth, transformation and, as a consequence, security threats. This latter is something the EU is well aware of:

> **"Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021."**

The legislation is therefore intended to safeguard users and improve the quality of connected hardware and software within the EU. And, clearly, this will save a lot of money and lessen criminal disruption. Let's see how.

Closing thoughts

The EU Cyber Resilience Act will be a positive step forward for the cybersecurity of consumers and businesses in Europe, though it may create a few initial headaches for businesses as they get their heads around the changes required for production and business practices.

However, businesses will almost certainly see long term benefits as EU culture shifts towards providing higher levels of cyber resilience. This should mean that in future they are losing less money to cyber criminals and, hopefully, to EU prosecutors too!

READ MORE Intigriti named in the Financial Times' top 500 fastest-growing European companies list

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com