

IOT & OT CYBERSECURITY REPORT 2026

Final Push Toward CRA Compliance:
Industry Is on the Right Track, but
Implementation Must Accelerate

ONEKEY

CYBERSECURITY REPORT

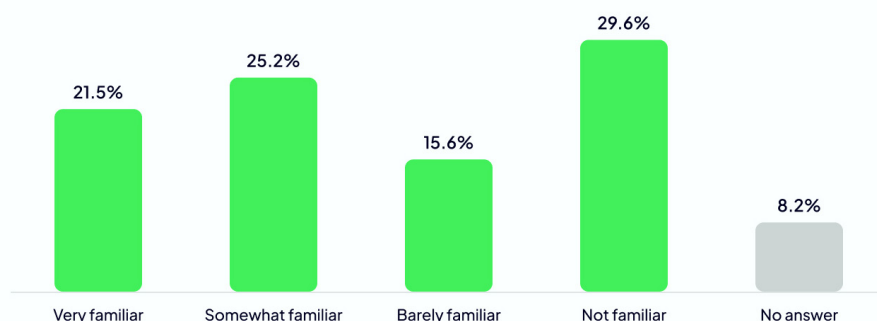
EXECUTIVE SUMMARY

IoT & OT Cybersecurity Report 2026

Reading time: Approximate reading time: 15 min.

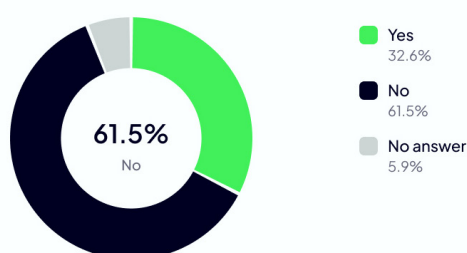
German industry is making progress in implementing the Cyber Resilience Act (CRA). However, with key deadlines approaching, the pace needs to accelerate and significant gaps remain. This is one of the key findings of ONEKEY's "IoT & OT Cybersecurity Report 2026", which surveyed 200 German industrial companies on their strategies and progress in implementing the new EU cybersecurity regulation. 46% of companies are familiar with the CRA, including 21% who say they are very familiar with it. At the same time, 60% admit that they are unaware of the regulation's subsequent phases and deadlines.

How familiar is your organization with the requirements of the EU Cyber Resilience Act (CRA)?



Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

Do you know when the remaining CRA phases take full effect?



Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

„German industry now has the Cyber Resilience Act on its radar. The key now is to turn awareness into consistent implementation. Those who fail to make use of the time remaining until the end of 2027 risk significant delays in development and market launch later on.“

— Jan Wendenburg, CEO of ONEKEY

The gaps become particularly apparent when it comes to practical implementation. While many companies have taken initial steps, considerable work remains in key areas such as risk management, documentation, security updates and technical evidence. Among the biggest challenges are the requirement to report security incidents within 24 hours, effective September 11, 2026, as well as vulnerability management, software bills of materials (SBOMs) and Security by Design / Security by Default.

The supply chain presents another challenge. Manufacturers must not only secure their own developments but also manage risks introduced through third-party software, firmware and other components. According to the companies surveyed, only around 18% of suppliers have fully adapted to the CRA requirements and provide the necessary information.

At the same time, well over 60% of companies expect the development of new or updated products to take longer. CRA compliance is therefore not only a regulatory requirement; it also has significant implications for product development, supplier management and internal responsibilities.

What impact do you expect on the market launch of new products?



Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

„The Cyber Resilience Act puts an end to the notion that manufacturers can simply pass on responsibility for insecure software components to suppliers. Anyone who brings a product to the European market under their own name bears responsibility for the cybersecurity of the entire product.“

— Jan Wendenburg, CEO of ONEKEY

BACKGROUND ON THE CYBER RESILIENCE ACT

The Cyber Resilience Act applies to devices, machines, and systems with digital components, as well as software and other connected products. These include, among other things, connected machines and control systems, routers, firewalls, and network devices; IoT and smart home devices; operating systems; apps; industrial control software; and cloud functions—provided they are necessary for a product's operation.

The CRA regulations will take full effect on December 11, 2027. As of that date, no new products with an internet connection may be sold in the 27 countries of the European Union if they do not meet the requirements of the Cyber Resilience Act. However, one key obligation has been in effect since September 11, 2026: Distributors of digital products must report actively exploited vulnerabilities and serious security incidents. With certain exceptions, this also applies to products already on the market.

For manufacturers, distributors, and importers, the CRA means they must comprehensively protect their products against hacker attacks and demonstrate and document their security. Violations of fundamental cybersecurity requirements or key manufacturer obligations are punishable by fines of up to 15 million euros or 2.5% of global annual revenue, whichever is higher

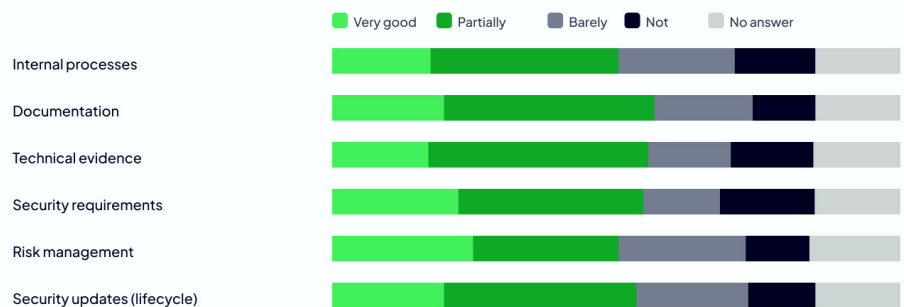


IMPLEMENTATION IS PROGRESSING SLOWLY

Although awareness of the CRA has increased, its deadlines and requirements are still far from being fully understood and implemented across industry. The overall picture of preparedness is therefore mixed. One-quarter of companies describe themselves as “very well prepared” in terms of risk management. The figure is 22% for security requirements, 20% for documentation and the required security updates throughout the product life-cycle, and 17% for internal processes and technical evidence.

Other companies have started addressing these areas but have yet to implement them fully. This applies to 39% for technical evidence and 37% for documentation. 34% have partially implemented internal processes and security updates, while 26% have done so for risk management. By contrast, around one-third of companies are not yet sufficiently prepared for the CRA in terms of internal processes, risk management or the management of security updates. 30% have barely begun addressing security requirements or technical evidence.

How well prepared is your organization for the CRA?



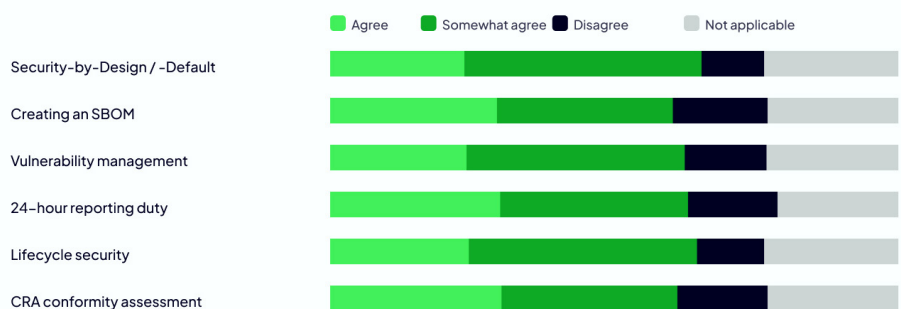
Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

MANDATORY REPORTING, VULNERABILITY MANAGEMENT, AND SECURITY BY DESIGN POSE MAJOR CHALLENGES

Companies view the requirement to report security incidents within 24 hours as the biggest challenge. 62% cite this requirement—which takes effect on September 11, 2026—as particularly problematic. For 30%, compliance assessment is a major hurdle—that is, determining whether their product portfolio already meets CRA requirements or if there is still work to be done.

An equal number of companies cite the creation of software bills of materials (SBOMs) as a key challenge. At least 60% have not yet resolved this issue. Vulnerability management also remains an unresolved issue for 62%; while nearly a quarter rank it among their biggest challenges on the path to CRA compliance.

Which CRA requirements currently pose the biggest challenge?



Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

„A Software Bill of Materials is much more than just an inventory list. It provides transparency regarding software components and dependencies, thereby laying the foundation for effective vulnerability management, rapid security updates, and the technical documentation required by the Cyber Resilience Act.“

— Jan Wendenburg, CEO of ONEKEY

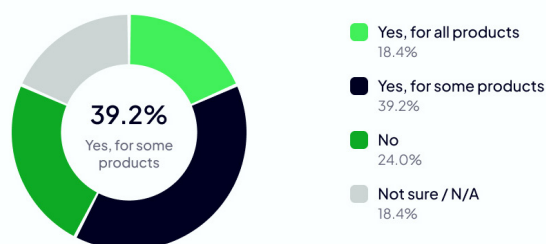
Two-thirds of the companies surveyed also report difficulties with “Security by Design / Security by Default.” This involves integrating cybersecurity into product development from the very beginning and shipping products with secure default settings. 24% consider this issue a critical factor. For nearly a quarter, security throughout the entire product lifecycle poses a serious problem, while another 40% view it as a surmountable hurdle.

SBOM: TRANSPARENCY AROUND SOFTWARE REMAINS INCOMPLETE

The Software Bill of Materials (SBOM) is a key tool for CRA compliance. It provides transparency regarding which software components and dependencies are contained in a product. If a security vulnerability is discovered, the SBOM can be used to determine which product versions are affected, what risks arise, and where an update is required. At the same time, the SBOM serves as an important foundation for the vulnerability management and technical documentation required by the CRA.

In practice, however, a complete software bill of materials is still far from being the norm. Only 18% of industrial companies have already created an SBOM for all affected products. 39% have at least partially inventoried the programs they use. 24% have not yet made any efforts in this direction.

Does your organization already create or use a Software Bill of Materials (SBOM)?

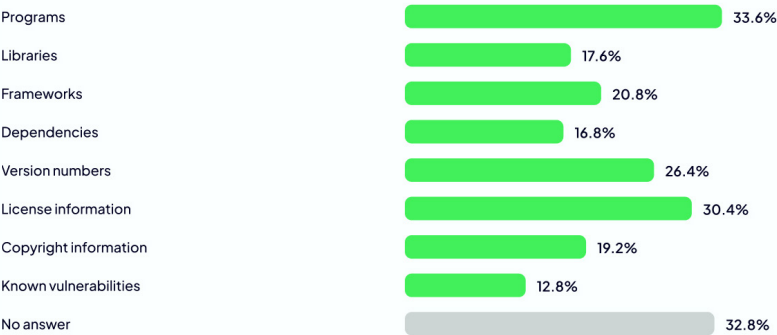


Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

The quality and completeness of existing bill of materials (BOMs) also leave room for improvement. The SBOMs of the surveyed companies do not even contain half of the required information. Programs are tracked by 34%, version numbers by 26%, frameworks by 21%, libraries by 18%, and dependencies by 17%. Supplementary information is also only partially available: known vulnerabilities in 13%, license information in 30%, and copyright information in 19%.

For CRA compliance, it is not enough to simply maintain a list of software components. The information must be complete, up-to-date, and machine-readable, and must include versions, dependencies, origin, license information, and known vulnerabilities.

Does your SBOM contain the following information?



* Multiple responses

Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY



THE SUPPLY CHAIN BECOMES A KEY FACTOR

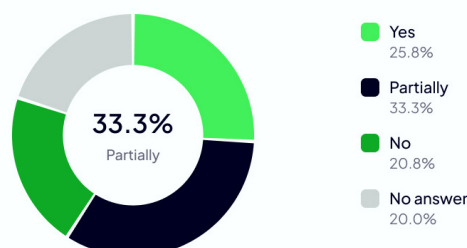
In addition to the SBOM, supply chain cybersecurity is taking center stage. Manufacturers must not only ensure the security of the software they develop themselves; they must also manage risks that enter the end product via third-party software, firmware, intermediate products, and other components.

Modern digital products consist only partially of in-house software. Operating systems, open-source libraries, communication modules, software development kits, containers, cloud components, and firmware from suppliers can make up a significant portion of the finished product. This creates multi-level dependencies: A library used directly may contain additional components that the manufacturer may not be aware of. As a result, a single vulnerability can affect numerous products and product versions across multiple supply chain levels.

The manufacturer remains responsible for the cybersecurity risks of the entire product. To address this, the manufacturer needs reliable information about which components are included, where they come from, and which product versions are affected by a newly discovered vulnerability.

One-quarter of German industrial companies already actively and consistently require CRA compliance from their suppliers. Another third does so to some extent. 21% have not yet taken any action in this regard. Supplier certifications or contractual assurances do not replace the manufacturer's own risk assessment.

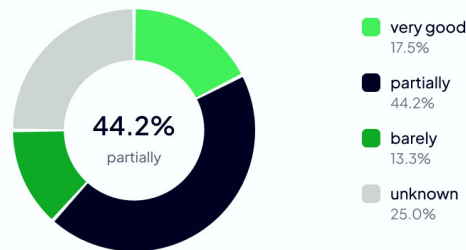
Does your organization already actively require CRA compliance from suppliers?



Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

Suppliers also have a lot of catching up to do. Only 18% have consistently adapted to the requirements and are providing the necessary information. 44% comply with the CRA requirements at least in part. 13% apparently consider the new EU regulation unnecessary, and a quarter are not even aware of it. European manufacturers often find that, particularly among suppliers from Asia, the CRA is still largely unknown or is viewed as a purely European matter.

How well prepared are your suppliers for CRA requirements?



Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

PR©CUREMENT AND SUPPLIER C©NTRACTS MUST BE ADJUSTED

The Cyber Resilience Act is therefore likely to change business relationships between manufacturers and suppliers. In addition to technical specifications, prices, and delivery dates, reliable security information will become more important. Cybersecurity requirements should therefore be taken into account as early as the procurement, supplier selection, and contract drafting stages.

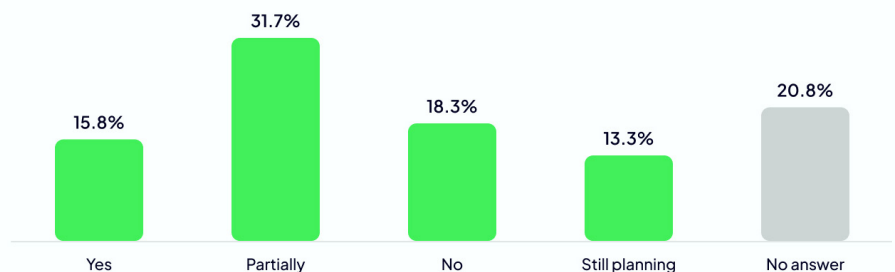
These include, for example, agreements on machine-readable SBOMs, reporting channels for vulnerabilities, response times, security updates, support periods, and the sharing of relevant information from upstream supply chain stages. Equally important is a standardized procedure in the event that a component is no longer maintained or a supplier ceases business operations.

When selecting suppliers, manufacturers should also verify which security and development processes are in place, whether software components and dependencies are documented in a traceable manner, how quickly information about new vulnerabilities is shared, and who provides security updates and for how long. The clear mapping of components to product and firmware versions, as well as contractually defined obligations regarding cooperation, information sharing, and updates, also play an important role.

CRA COMPLIANCE REQUIRES RESOURCES AND CLEARLY DEFINED RESPONSIBILITIES

Most companies will not be able to manage the transition on their own with existing staff and in-house resources. 61% have already set aside a budget for external support or are still planning to do so. Only 18% expect that they will not need external help.

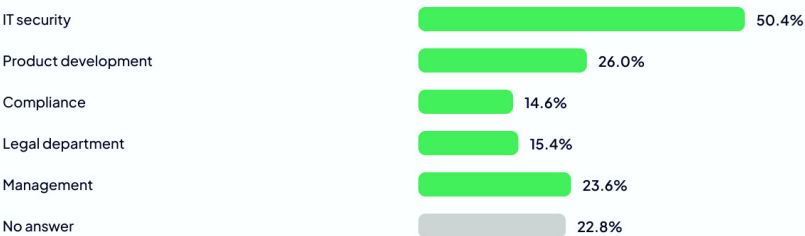
Has your organization already budgeted for CRA compliance?



Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

Responsibility is also broadly distributed at the departmental level. In half of the companies, this issue falls under the IT security department, while in 26%, it falls under product development. Nearly a quarter even see the primary responsibility as lying with senior management. 15% each assign responsibility to the compliance or legal department.

Which departments hold primary responsibility for CRA compliance?

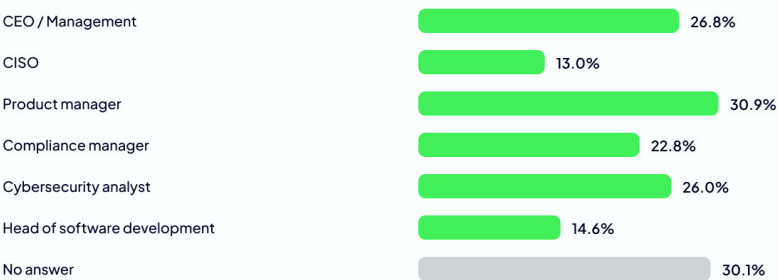


* Multiple respons

Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

The picture is similarly diverse when it comes to individual roles: 31% cite the product manager, 26% the cybersecurity analyst, 23% the compliance manager, 15% the head of software development and 13% the Chief Information Security Officer. In addition, 27% identify the CEO or executive management as responsible. Given the potential penalties and the implications for product development and market access, there is a strong case for treating CRA compliance as a company-wide responsibility.

Which roles are directly responsible for CRA compliance?



* Multiple respons

Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

IMPACT ON PRODUCT DEVELOPMENT AND MARKET LAUNCH

Depending on the industry, the CRA's requirements have a profound impact on product development and market launch. In particular, they mandate cybersecurity "by design and by default" embedded in the product, documented risk assessments, secure default settings, effective vulnerability management, and security updates throughout the entire intended support period.

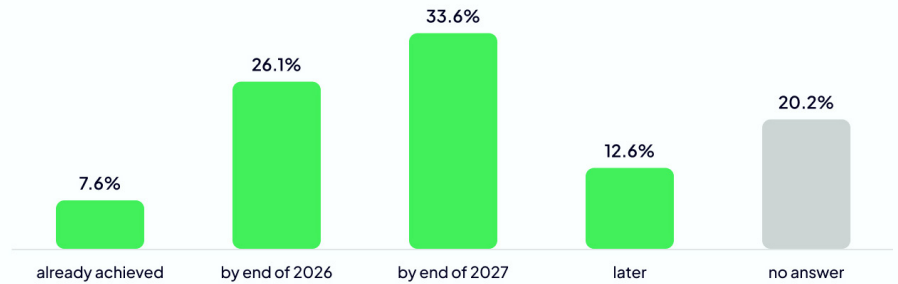
Existing products are generally exempt from these requirements. However, the EU cybersecurity regulation may also apply if significant changes are made. Grandfathering applies to individual product units that have already been placed on the market, rather than automatically to an entire product series or model.

Well over 60% of the companies surveyed therefore expect it to take longer to develop new or updated devices, machines, and systems. 28% even expect the development time to be significantly longer.

MANY COMPANIES AIM TO BE COMPLIANT BY 2027

Despite the challenges, many companies have set clear goals. One-third aim to achieve full compliance by the time the Cyber Resilience Act takes full effect on December 11, 2027. 26% are aiming to achieve this by the end of 2026. 8% believe they have already met this goal.

When do you expect full CRA compliance in your organization?



Source: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

The final push has begun, but implementation needs to accelerate in many areas. Regulatory deadlines are not the only reason. At the same time, the threat landscape is intensifying as cyberattacks become increasingly automated and AI-powered. Incidents involving OpenAI and Anthropic have shown AI models attacking real external systems beyond their test environments during security testing. Powerful AI agents are already capable of independently executing multi-stage attack chains and exploiting vulnerabilities.

In the future, this will affect more than just data centers and traditional IT systems. Connected machines, production facilities, and industrial control systems are also coming under greater scrutiny. Successful attacks in these areas can lead not only to data theft but also to production outages, process manipulation, and, in the worst case, physical damage. Implementing the Cyber Resilience Act is therefore not merely a compliance task but an important component of operational risk management.

„“CRA compliance doesn’t end with meeting regulatory requirements. It begins when cybersecurity becomes an integral part of product development and corporate strategy,” summarized Jan Wendenburg, CEO of ONEKEY.



onekey.com
+49 211 1587 41 04
info@onekey.com

Security
made
in
Germany

© 2026 ONEKEY. All rights reserved. Reproduction only permitted with the approval of ONEKEY. All brands listed are the brands of the respective owners. Errors, changes, and availability of the listed products, services, characteristics, and possible applications reserved. Software & services will be provided by ONEKEY. ONEKEY makes no guarantee for the information of third parties regarding characteristics, services and availability. ONEKEY reserves the right to make changes to products and services as a result of product development, even without prior notification. None of the statements and depictions represents legal advice or may be interpreted in such a manner. In case of deviations from the contract documents and general terms and conditions of ONEKEY and their affiliated companies and subsidiaries in conjunction with this document, the contract documents and general terms and conditions always have precedent over this document.

2026090001EN