ONEKEY.COM

IOT & OT CYBERSECURITY REPORT 2025

Time is running out: 68% of companies are still unfamiliar with the new Cyber Resilience Act

ONEKEY

CYBERSECURITY REPORT

EXECUTIVE SUMMARY

IoT & OT Cybersecurity Report 2025

Reading time: Approximate reading time: 15 min.

On the road to compliance with the EU Cyber Resilience Act (CRA), organizations should now be making a final push to meet the deadlines. Yet in the business world, there is little sign of urgency. A survey of 300 industrial organizations revealed that only about one-third (32 percent) are thoroughly familiar with the requirements of the EU Cyber Resilience Act. Implementation is correspondingly hesitant. Just 14 percent of the organizations surveyed have already launched extensive measures to ensure compliance with CRA regulations for their connected devices, machines, and systems.

"Up to now, many manufacturers of digital devices, machines, and systems have primarily focused on the functionality of their products, while paying less attention to vulnerabilities to cyberattacks. With the Cyber Resilience Act, it is now absolutely necessary to treat both aspects as equally important."

— Jan Wendenburg, CEO, ONEKEY

As part of the survey, ONEKEY wanted to identify the greatest challenges. For 37 percent of organizations, the top concern is the obligation to report security-critical incidents within 24 hours. Close behind, at 35 percent, is compliance with the principles of "Secure by Design" and "Secure by Default." For 29 percent of respondents, creating a Software Bill of Materials is the biggest hurdle. Almost as many organizations view maintaining oversight of software vulnerability management as their main problem. Only 12 percent of organizations have a complete overview of the software used in their devices, machines, and systems.

BACKGROUND ON THE NEW EU CYBER RESILIENCE ACT

The first obligations under the EU Cyber Resilience Act (CRA) will become binding in fall 2026, with all remaining requirements taking effect in 2027. From that point on, connected devices, machines, and systems that do not meet CRA requirements may no longer be sold or operated in the EU. The Cyber Resilience Act is an EU regulation, not a directive. This means it applies directly and immediately across all EU member states. Unlike NIS2, there will be no delays caused by national implementation. Time is therefore of the essence.

“Connected devices, machines, and systems that do not meet CRA requirements will no longer be permitted for sale or operation in the EU. Given development cycles of two to three years, there is an urgent need for action.”

— Jan Wendenburg, CEO, ONEKEY

In cases of non-compliance, organizations face steep fines of up to €15 million or 2.5 percent of global annual revenue, whichever is higher. In addition, there is the risk of personal liability for board members, executives, and other responsible parties. ONEKEY’s latest survey shows that while businesses have already begun taking steps toward implementing the Cyber Resilience Act, there is still a considerable need for action.

DIGITAL TRANSFORMATION EXPANDS THE ATTACK SURFACE FOR CYBER THREATS

The Internet of Things (IoT) and Operational Technology (OT) are at the heart of the digital transformation of industrial processes. At the same time, the attack surface for cyber threats is growing. As part of a comprehensive study, ONEKEY examined the current state of IoT and OT security in German-speaking countries. The survey included 300 executives from the fields of industry, IT, OT, and engineering. This report analyzes the key findings, assesses risks, and highlights potential courses of action.

A key focus of the survey was the Cyber Resilience Act, the EU regulation aimed at strengthening the cybersecurity of connected products. It requires manufacturers and distributors of digital products with internet connectivity (connected devices, machines, and systems) to implement extensive security measures.

OBLIGATIONS OF MANUFACTURERS AND DISTRIBUTORS

Under the Cyber Resilience Act (CRA), manufacturers must design their products to be secure from the outset ("Security by Design" and "Secure by Default") and ensure that they continue to meet CRA requirements throughout their entire lifecycle. This includes protection against unauthorized access, safeguarding data integrity and confidentiality, and guaranteeing the availability of functions.

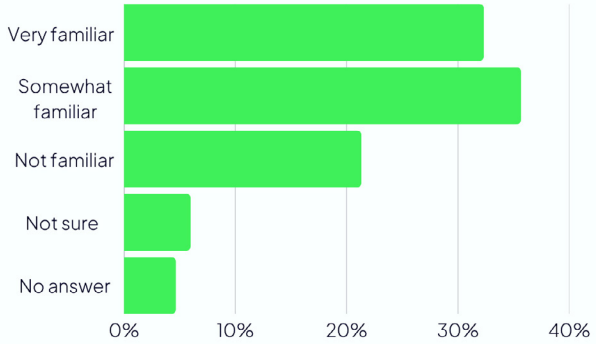
They are also required to report actively exploited vulnerabilities and severe security incidents affecting the safety of their products within 24 hours to the European cybersecurity authority ENISA and the relevant national CSIRT (Computer Security Incident Response Team).

In addition, providers must deliver regular security updates to fix known vulnerabilities and ensure the ongoing security of their products. This also involves comprehensive product documentation, including a Software Bill of Materials (SBOM), to ensure transparency and traceability of components. Compliance with CRA requirements must be documented and proven. Given that product development cycles often span several years, many organizations are already falling behind.

ONLY ONE-THIRD ARE FAMILIAR WITH THE CRA

According to the survey, just under one-third (32 percent) of organizations are thoroughly familiar with the requirements of the EU Cyber Resilience Act. Another 36 percent have at least looked into it. More than a quarter (27 percent), however, have not addressed the topic at all.

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

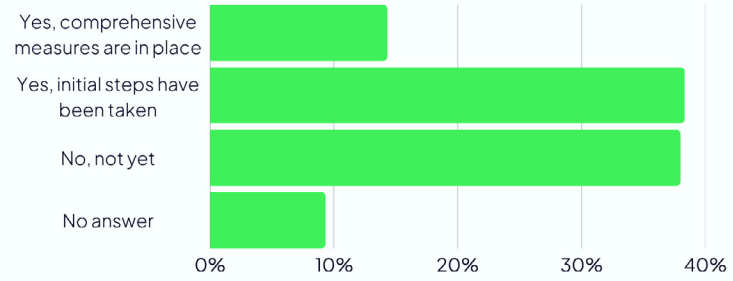


Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

SLOW IMPLEMENTATION

Implementation is sluggish. Only 14 percent (!) of the organizations surveyed have already launched extensive measures to ensure compliance with CRA regulations for their connected devices, machines, and systems. On the plus side, 38 percent have at least taken initial steps toward CRA compliance. However, just as many organizations have so far done nothing to meet the new EU requirements.

Has your organization already initiated measures to comply with the CRA for products with digital elements?



Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

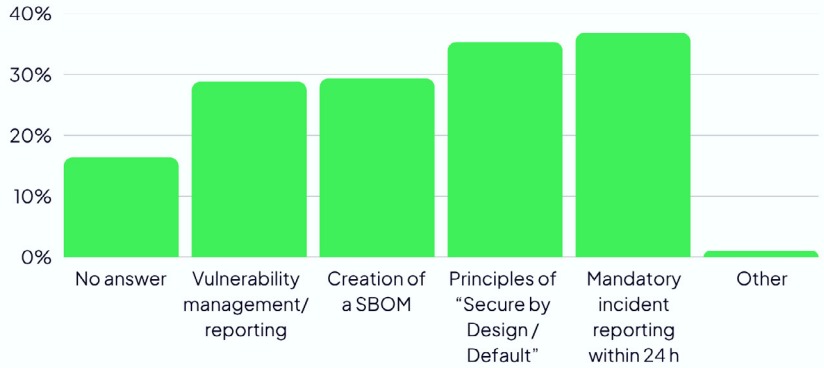
WORSENING THREAT LANDSCAPE

This reluctance is problematic not only in light of the strict legal requirements and potential consequences of non-compliance but also given the increasing threat posed by hackers and the potential damage involved. Authorities such as the German Federal Office for Information Security (BSI) and the Federal Criminal Police Office (BKA) expect the security situation to continue deteriorating in the coming years. In 2024 alone, the total damage caused by cybercrime incidents in Germany was estimated at €178.6 billion—an increase of €30.4 billion compared to the previous year.

SBOM WORRIES 29 PERCENT OF ORGANIZATIONS

According to ONEKEY's survey, the biggest challenge under the Cyber Resilience Act is the obligation to report incidents within 24 hours, cited by 37 percent of organizations. In second place, at 35 percent, is compliance with the principles of "Secure by Design" and "Secure by Default." For 29 percent, the creation of a Software Bill of Materials (SBOM) and the associated requirement to maintain oversight of all software components and their vulnerabilities is a major concern.

Which CRA-related requirements pose the greatest challenge for your organization? (Multiple answers possible)



Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

A Software Bill of Materials (SBOM) is a structured list of all software components contained in a digital product—including libraries, dependencies, and versions. It is essentially a "parts list" for software. The SBOM is critical: it enables transparency, speeds up vulnerability management, and is essential for a rapid response to security incidents. Without an SBOM, it is unclear whether a given security vulnerability affects the product in question—potentially with severe consequences for manufacturers, distributors, and customers. Establishing standardized SBOM processes is therefore a key step toward resilient software security, especially in production environments.

"The CRA requires a detailed listing of all programs, libraries, and dependencies with exact version numbers of each component, information on the respective licenses, and a documented overview including an assessment of all known vulnerabilities and security flaws." — Jan Wendenburg, CEO, ONEKEY

The survey also found that 44 percent of organizations have begun creating SBOMs for their product portfolios. However, only 12 percent (!) have completed this for all their products, while 32 percent have so far covered only individual products. One-quarter have not started at all, and another quarter either believe they are not affected or remain uncertain about their obligations.

SBOM: MANY ORGANIZATIONS STILL IN THE DARK

Does your organization currently use or create a Software Bill of Materials (SBOM) for products with digital elements, as required by the CRA?

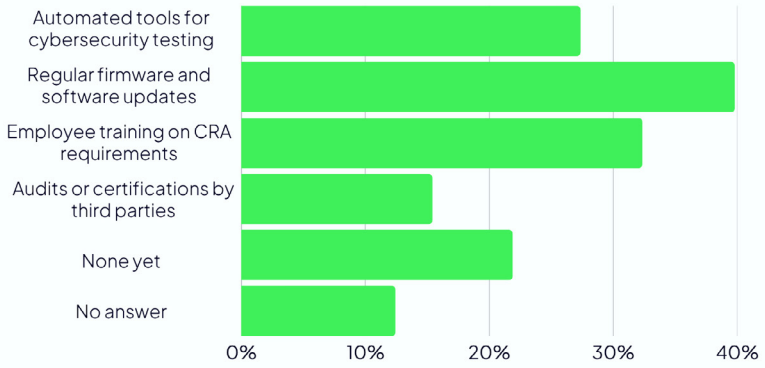
Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

Despite the clear requirement under the CRA to maintain a Software Bill of Materials, about half of organizations still lack a clear overview in this area. This is particularly striking given that transparency about software components and structured security processes are core building blocks of modern cyber resilience—yet in many companies, they are still not firmly established.

CRA COMPLIANCE: PROGRESS MADE, BUT URGENCY STILL LACKING

Although many shortcomings and gaps remain, the report shows that a significant number of organizations are moving toward CRA compliance. According to the survey, 40 percent regularly carry out firmware and software updates. 27 percent use automated tools for cybersecurity testing. 16 percent rely on third-party audits and certifications.

What measures has your organization taken to ensure compliance with the CRA? (Multiple answers possible)

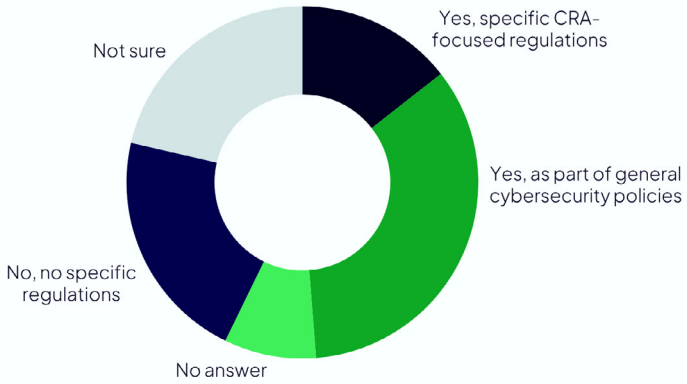


Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

CRA-SPECIFIC COMPLIANCE STILL THE EXCEPTION

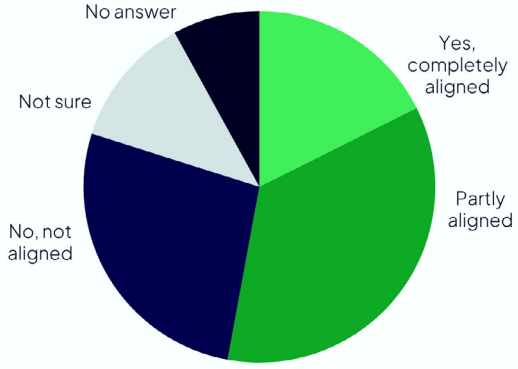
Only 15 percent of companies currently have CRA-specific compliance policies in place. However, more than one-third (34 percent) believe their general cybersecurity policies already cover the CRA's requirements. Meanwhile, 21 percent have not yet factored the Cyber Resilience Act into their compliance frameworks at all.

Does your organization have specific compliance regulations for CRA-related cybersecurity requirements?



Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

Are your organization's cybersecurity policies aligned with the CRA requirements for products with digital elements?

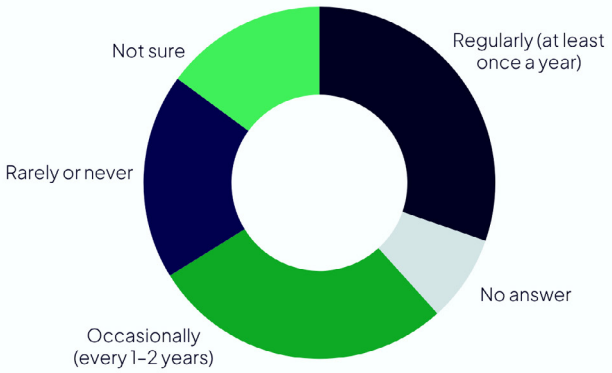


Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

NEARLY ONE-THIRD HAVE STARTED CRA TRAINING

Just under one-third (32 percent) of the organizations surveyed have begun training their employees specifically on CRA requirements. 30 percent provide such training regularly—at least once a year. Another 28 percent offer CRA-related qualifications occasionally (every two to three years). Nearly one in five (19 percent) provide no knowledge transfer on the Cyber Resilience Act at all.

How often are trainings or further education on the CRA conducted for the responsible team or employees?



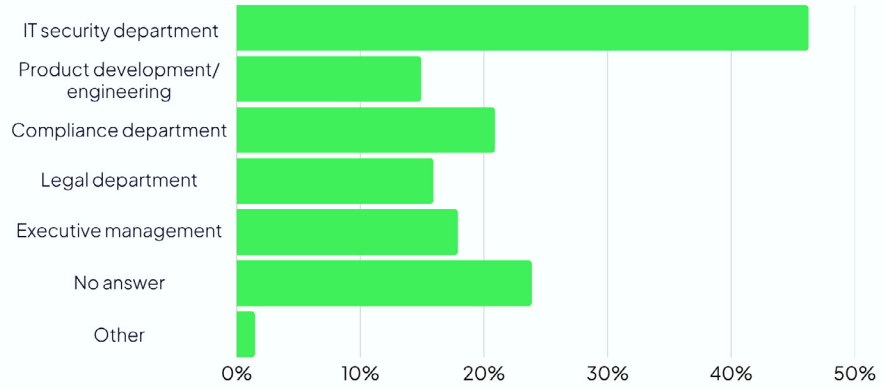
Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

RESPONSIBILITY DIFFERS ACROSS ORGANIZATIONS

When asked who is responsible for ensuring CRA compliance, organizations gave very different answers. In 46 percent of cases, the IT security department is in charge; in 21 percent, compliance takes the lead; in 16 percent, the legal department. At 18 percent of companies, top management handles it directly, while 15 percent have assigned responsibility to product development. In many cases, it is likely that responsibility for CRA compliance is shared across multiple departments.

“The EU has created a very comprehensive regulatory framework with the Cyber Resilience Act, ranging from technical standards to reporting obligations. Accordingly, the challenges for industry to fully implement the CRA are significant.”
— Jan Wendenburg, CEO, ONEKEY

Which departments or functions in your organization hold primary responsibility for complying with CRA requirements? (Multiple answers possible)

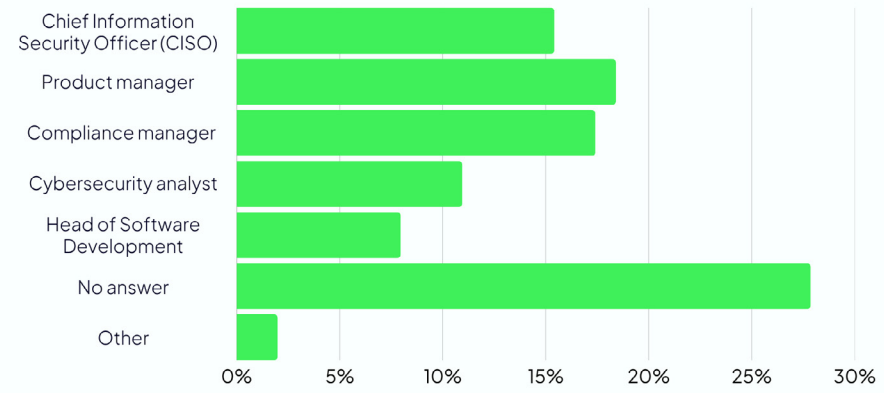


Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

UNCLEAR PICTURE OF RESPONSIBLE ROLES

A similarly diffuse situation emerges when looking at responsible roles. 18 percent of organizations assign CRA compliance to the product manager, 17 percent to the compliance manager, 15 percent to the Chief Information Security Officer (CISO), 11 percent to the cybersecurity analyst, and 8 percent to the head of software development. Here too, it is likely that responsibilities often overlap across teams and roles.

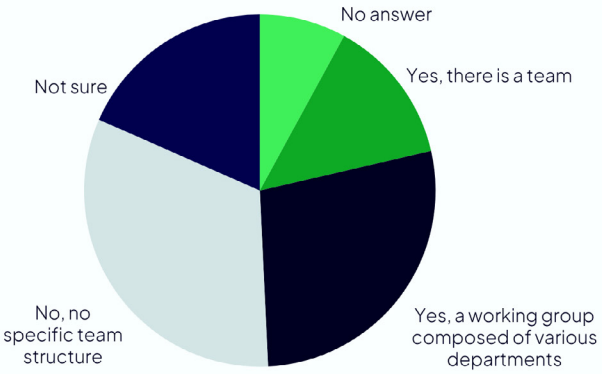
Which roles or functions in your organization are directly responsible for implementing CRA compliance? (Multiple answers possible)



Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

In practice, 28 percent of the organizations surveyed have formed a cross-departmental working group to make their company "CRA-ready." In 14 percent, a dedicated team is in place that focuses specifically on meeting CRA requirements. The most common team size is four to ten members (reported by 18 percent of respondents). Nearly one-third (32 percent), however, have not established any working group for the Cyber Resilience Act.

Does your organization have a dedicated team or working group focused on implementing the CRA?



Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

How large is the team or working group in your organization that is responsible for CRA compliance?

Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

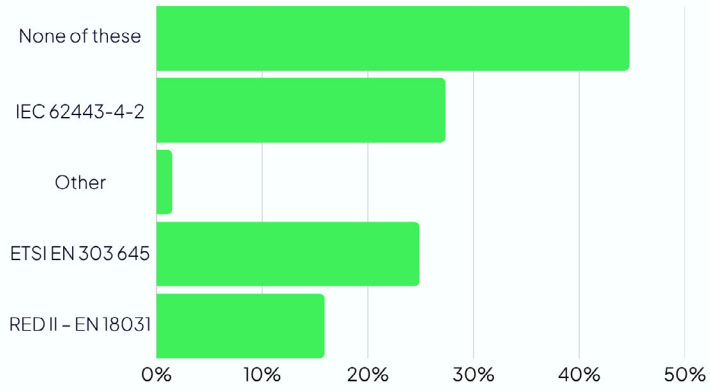
RECOMMENDATIONS FOR ACTION

Based on the study results, the following key recommendations emerge for organizations:

1. Secure by Design / Security by Default as a foundation

Align all product development for connected devices, machines, and systems consistently with cybersecurity principles across all phases—design, development, production, and maintenance.

Which CRA-relevant standards does your organization consider in product development? (Multiple answers possible)



Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

2. Create Transparency

Only through comprehensive SBOMs, regular vulnerability scans, and clear product documentation can organizations achieve the transparency mandated by the CRA.

3. Automated Security and Compliance Training

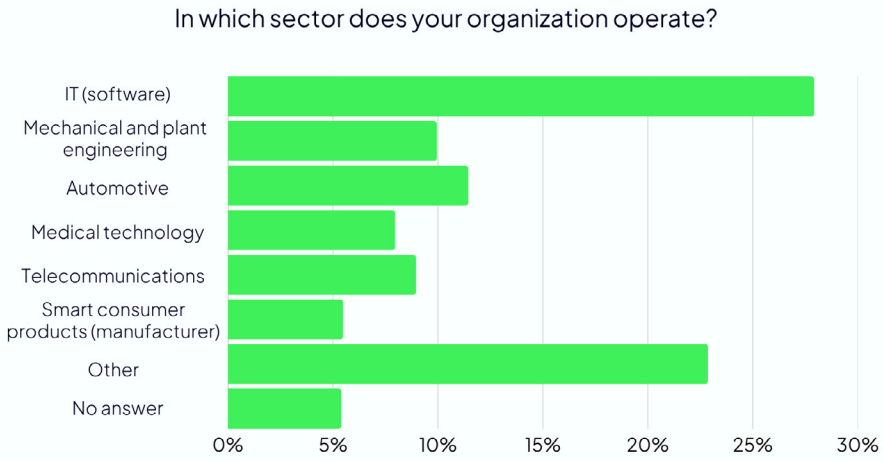
To meet CRA obligations—especially the reporting requirement and the assurance of cybersecurity throughout the entire product lifecycle—regular, ideally automated, checks of known and newly reported vulnerabilities are essential. This also includes assessing their relevance and documenting the results.

4. Clarify Responsibility

Appoint a dedicated Product Security Officer with IoT/OT expertise. Clearly defined roles and responsibilities across IT, OT, and development teams are also advisable in relation to the CRA.

5. Build Competence – Including with External Partners

Training, continuing education, and partnerships with specialized service providers are crucial—not least to compensate for the shortage of skilled professionals. Without external support and the use of automated solutions—particularly for creating and continuously maintaining complete Software Bills of Materials, as well as monitoring known and emerging vulnerabilities across all digital products—CRA compliance will be difficult to achieve.



Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

TIME TO ACT!

Around two-thirds of organizations are familiar with the Cyber Resilience Act, though half of them only partially. **It's high time for all companies to prepare for CRA compliance!**

More than half of the surveyed organizations have already taken initial measures to meet CRA requirements—but only 15 percent are well advanced in the process. **Implementation speed must increase!**

The security principle "Secure by Design / Secure by Default" is the greatest challenge, followed by the creation of an SBOM. Nearly one-third have at least produced an SBOM for some products, but fewer than 15 percent have one covering their entire product portfolio. **Action needed: align engineering with Secure by Design/Default and create SBOMs for all connected products as soon as possible!**

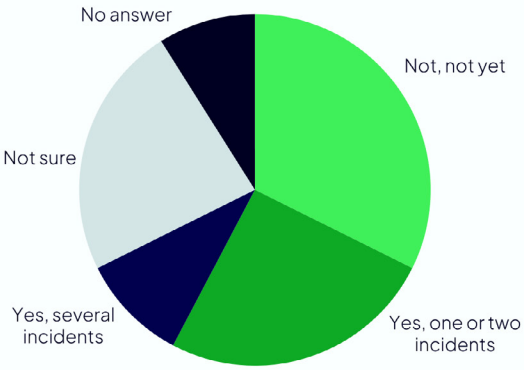
In nearly half of organizations, CRA-related compliance policies exist, but mostly in a general form. **Make CRA compliance a top priority!**

40 percent regularly perform firmware and software updates, and 27 percent use automated cybersecurity testing tools. **Shift to automated solutions—without them, CRA compliance will be impossible!**

One-third of organizations train their workforce on CRA compliance. **More training is urgently needed!**

More than one-third of organizations have already experienced security incidents due to non-compliance with CRA requirements. In almost half of the surveyed companies, responsibility for CRA compliance lies with the IT department. **But CRA compliance goes beyond IT—every relevant department must be involved!**

Has your organization already experienced cybersecurity incidents related to non-compliance with CRA requirements?



Source: OT and IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

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

SecurITy made in Germany

20250900IEN