News & Technologies

Cybersecurity Report 2025:

New Study Shows a Training Gap in Business Cyber Defence

ONEKEY IoT & OT Cybersecurity Report 2025: "Barely a third of organizations conduct Cyber Resilience Act training at least once a year."

Düsseldorf, January 15, 2026 — This year, the German economy should place a greater emphasis on cybersecurity training for its workforce. This is the conclusion reached in the latest "IoT & OT Cyber-security Report 2025" published by the Düsseldorf-based cybersecurity company ONEKEY. Starting this fall, most of the strict reporting requirements for security incidents outlined in the European Union's Cyber Resilience Act will take effect. By fall 2027, manufacturers, distributors, and operators of networked digital devices, machines, and systems must comply with the EU regulation.

In accordance with the CRA, organizations must demonstrate that their products meet basic cybersecurity requirements and do not contain any known vulnerabilities. Additionally, the CRA requires companies to provide regular security updates, promptly address vulnerabilities, and develop a comprehensive software bill of materials (SBOM). Violations can result in heavy fines.

Nevertheless, according to ONEKEY's "IoT & OT Cybersecurity Report 2025," fewer than one-third (30%) of the 300 companies surveyed held at least one training session per year on "cyber resilience" for their employees. Another 28 percent consider training on this topic once every one to two years to be sufficient. Nineteen percent answered "rarely or never" to the question about CRA training.

"The low level of training is all the more remarkable given that the threat level remains high," said ONEKEY CEO Jan Wendenburg. He is referring to police crime statistics (PKS), which list over 130,000 cybercrime cases in Germany. The damage caused by cyberattacks is estimated at around 180 billion euros.

Jan Wendenburg warned: "The ongoing increase in digitalization and networking, as well as the use of artificial intelligence by cybercriminals, will further exacerbate the situation." According to the "IoT & OT Cybersecurity Report 2025," over a third (35%) of surveyed companies have already experienced at least one cybersecurity incident related to noncompliance with CRA requirements. "The CRA's reporting requirements will take effect this fall," said the ONEKEY CEO, underscoring the approaching deadline.

ONEKEY offers a fully automated platform for product and cybersecurity compliance. It automates SBOM creation, vulnerability management, and compliance testing, saving companies time, money, and stress.

ONEKEY offers a practical CRA Readiness Assessment workshop for organizations new to the regulation. In introductory sessions, participants learn how the CRA specifically affects their operations and receive an individualized assessment plan tailored to their situation. A detailed process review then evaluates key areas such as software development and vulnerability management. In addition, a gap analysis pinpoints existing compliance shortfalls and outlines practical remediation measures. By the end of the workshop, each company receives a customized roadmap that clearly shows how to implement CRA requirements in a structured and efficient way.

ONEKEY is the leading European specialist in Product Cybersecurity & Compliance Management and part of the investment portfolio of PricewaterhouseCoopers Germany (PwC). The unique combination of the automated ONEKEY Product Cybersecurity & Compliance Platform (OCP) with expert knowledge and consulting services provides fast and comprehensive analysis, support, and management to improve

product cybersecurity and compliance from product purchasing, design, development, production to end-of-life.

Critical vulnerabilities and compliance violations in device firmware are automatically identified in binary code by AI-based technology in minutes without source code, device, or network access. Proactively audit software supply chains with integrated generation of Software Bills of Materials (SBOMs). “Digital Cyber Twins” enable automated 24/7 post-release cybersecurity monitoring throughout the product lifecycle.

The patent-pending, integrated ONEKEY Compliance Wizard already covers the EU Cyber Resilience Act (CRA) and requirements under IEC 62443-4-2, ETSI EN 303 645, UNECE R 155, and many others.

The Product Security Incident Response Team (PSIRT) is effectively supported by integrated automatic vulnerability prioritisation, significantly reducing time to remediation.

Leading international companies in Asia, Europe and the Americas already benefit from the ONEKEY Product Cybersecurity & Compliance Platform (OCP) and ONEKEY Cybersecurity Experts.

Weitere Informationen: ONEKEY GmbH,
Sara Fortmann, E-Mail: sara.fortmann@onekey.com,
Toulouser Allee 19A, 40211 Düsseldorf, Deutschland,
Web: https://onekey.com

PR-Agentur: euromarcom public relations GmbH,
Mühlhohle 2, 65205 Wiesbaden, Deutschland,
E-Mail: team@euromarcom.de, Web: www.euromarcom.de