**TÜV Rheinland: Cyber security requirements are growing rapidly**

Increasingly sophisticated cyber-attacks and a growing number of security vulnerabilities / Complex regulatory environment: CRA, NIS-2, RED / TÜV Rheinland’s expertise provides guidance / Interviews with experts at [www.tuv.com/cybersecurity-trends](https://www.tuv.com/landingpage/en/cybersecurity-trends_2024/meta-navigation/expert-interviews/?wt_mc=Mailing.Email.no-interface.CW25_I07_TRENDS.CW25_I07_TRENDS01_NL.textlink.&cpid=CW25_I07_TRENDS01_NL)

**Cologne, Germany, May 20, 2025.**New, increasingly complex regulations, ever more sophisticated cyber-attacks and a growing number of security vulnerabilities – cyber security is putting companies under increasing pressure. Experts from TÜV Rheinland, one of the world's leading providers of testing and inspection services, are now providing guidance on these three key cyber security trends in [expert interviews](https://www.tuv.com/landingpage/en/cybersecurity-trends_2024/meta-navigation/expert-interviews/?wt_mc=mailing.email.no-interface.cw25_i07_trends.cw25_i07_trends01_nl.textlink.&cpid=cw25_i07_trends01_nl) and highlighting approaches that can lead to an effective strategy for greater cyber security.

**CRA, NIS-2, RED: Complex regulatory environment for companies**

Take regulatory requirements, for example: The European Union's Radio Equipment Directive (RED) will be expanded to include cybersecurity requirements on August 1, 2025. From then on, devices sold in the EU with built-in radio technology must comply with the RED cybersecurity requirements. In addition, there is the second EU Directive on network and information security (NIS-2) and the Cyber Resilience Act (CRA), which affect an ever-increasing number of companies and products. “Globally active companies must also harmonize different regulations. This is a particularly big challenge, as some countries, such as the US, tend to favor risk-based approaches, while the EU often has stricter security requirements and reporting obligations,” explains Felix Brombach, Practice Leader for OT Security at TÜV Rheinland.

**Fundamental errors still widespread**

Cyberattacks are also becoming increasingly complex. In 2024, for example, multiple extortions were widespread among cybercriminals: attackers no longer limit themselves to encrypting data but also threaten to release sensitive information if a ransom is not paid. “In view of the threats, companies should avoid some fundamental mistakes that we still see, such as inadequate backups, insufficient employee training, outdated systems, non-existent incident response plans, and paying ransom,” reports David Allen, team leader for cybersecurity at TÜV Rheinland.

**More and more points of attack**

In addition to complexity, companies’ IT departments are also concerned about the ever-increasing number of potential points of attack for cybercriminals. The growing connectivity of Internet of Things (IoT) devices, cloud services, decentralized networks, and the use of AI are increasing security risks. Sectors such as healthcare, finance, and education are particularly at risk, according to Massimiliano Latini, cybersecurity expert at TÜV Rheinland: “Organizations are forced to adapt their IT security strategies accordingly—for example, through proactive security measures and the automation of security processes.”

Further information can be found in the interviews published at [www.tuv.com/cybersecurity-trends](https://www.tuv.com/landingpage/en/cybersecurity-trends_2024/meta-navigation/expert-interviews/?wt_mc=Mailing.Email.no-interface.CW25_I07_TRENDS.CW25_I07_TRENDS01_NL.textlink.&cpid=CW25_I07_TRENDS01_NL).

*150 years of making the world a safer place: TÜV Rheinland is one of the world's leading providers of testing and inspection services, with annual revenues of over 2.7 billion euros and approximately 26,000 employees in more than 50 countries. Its highly qualified experts test technical systems and products, enable innovation, and assist companies in their transition toward greater sustainability. They train professionals across numerous fields and certify management systems to international standards. With exceptional expertise in areas such as mobility, energy supply, infrastructure, and beyond, TÜV Rheinland provides independent quality assurance—not least for emergent technologies such as green hydrogen, artificial intelligence and autonomous driving. In doing so, TÜV Rheinland contributes to a safer and better future for everyone. Since 2006, TÜV Rheinland has been a signatory to the UN Global Compact, which promotes sustainability and combats corruption. The company's headquarters are located in Cologne, Germany. Website:* [*www.tuv.com*](http://www.tuv.com)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Media contact:

TÜV Rheinland, Press Office, Tel.: +49 221 806-21 48

Press releases as well as photo and video footage are available on request by email to contact@press.tuv.com or on [www.tuv.com/press](http://www.tuv.com/press).