IOT & OT CYBERSECURITY REPORT 2024

Surge in Cyberattacks on Industry: Urgent Action Needed for Stronger Protection

ONEKEY

CYBERSECURITY REPORT

EXECUTIVE SUMMARY

IoT & OT Cybersecurity Report 2024

Reading time: Approximate reading time: 15 min.

Industrial control systems, known as Operational Technology (OT), along with the Internet of Things (IoT) and Industrial IoT (IIoT), form the digital backbone of Industry 4.0. Today's production,l-ogistics, and operational processes are virtually unimaginable without OT and IoT. Connected devices, machines, and systems that continuously exchange dataare at the heart of modern industry. However, this growing connectivity and digitalization also brings new challenges: robust cybersecurity measures are essential, as IoT, IIoT, and OT systems often need to meet high security requirements despite vulnerable software. In 2024, the cybersecurity company ONEKEY surveyed over 300 IT deci-sion-makers and C-level executives about their perspectives and strategies in cybersecurity. The findings from this com-prehensive survey are presented in the OT & IoT Cybersecurity Report 2024.

Growing Awareness of Cyber Threats: Nearly 75% of companies recognize that hackers are increasingly targeting industrial con-trol systems and IoT devices.

Insufficient Protective Measures: Many companies lack ade-quate defenses against cyberattacks, with gaps in realistic risk assessment, effective prevention strategies, and actionable response capabilities.

Compliance Knowledge Gaps: Numerous companies are insuf-ficiently informed about relevant compliance requirements, with nearly half unaware of technical cybersecurity standards.

Outdated Firmware as a Vulnerability: Outdated firmware in devices and machines is increasingly exploited by hackers as an entry point. Attacks on unprotected firmware can be devastat-ing, potentially halting entire production batches.

Lack of Software Bill Of Materials(SBOM): Over half of compa-nies lack complete SBOMs, even though they are essential for effective cybersecurity.

Budget Constraints: 60% of companies rate their cybersecurity budget as inadequate oruncertain, with only 34% considering it "sufficient" or "significant."

Insufficient Cybersecurity Processes: Only about a quarter of companies rate the maturity of their cybersecurity processes as adequate, with many lacking measures to enhance security prac-tices and meet compliance requirements.

UNDERESTIMATED RISK: OT AND IOT

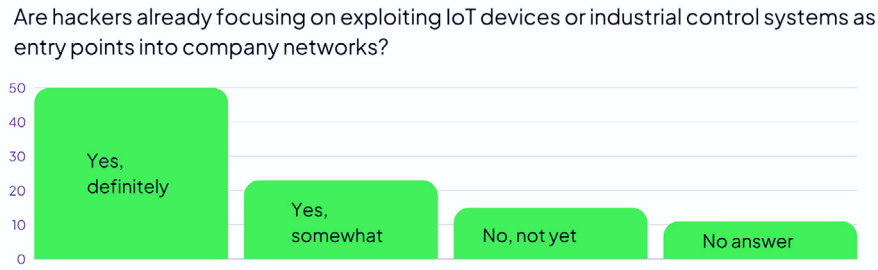
The study clearly shows that cybersecurity in OT and IoT poses significant risks, yet many companies are still under prepared. More than half of respondents (52%) have already experienced cyberattacks through OT or IoT devices, with just as many suspecting that cybercriminals are specifically targeting these devices as entry points. Nonetheless, OT and IoT cybersecurity is often considered less critical.

Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

“With over 2,000 new software vulnerabilities identified each month, companies that fail to keep their software updated aren’t asking if they’ll be targeted by cyberattacks, but when—and how severe the consequences will be.” – Jan Wendenburg, CEO ONEKEY.

Instead, many companies are focusing more on protecting payment and financial systems (42%), corporate networks and datacenters (39%), as well as customer data (36%). Email, cloud services, and appsare also perceived as greater threats, while the risks to OT (OperationalTechnology) and IoT (Internet of Things) are often underestimated.

As digitalization advances at the production and logistics level in German industry, a growing number of security gaps are emerging — creating new points of attack for cybercriminals.



Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

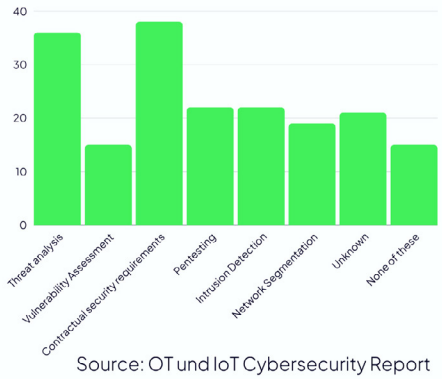
CYBER RESILIENCE: A REALISTIC SELF-ASSESSMENT

Over a quarter (26%) of companies consider their cybersecurity maturity in product and project development to be ‘adequate,’ thanks to a defined and active security process. An additional 12% have security processes in place but deem their control measures insufficient. Meanwhile, 9% of companies report having no such processes at all.

Companies focus on a variety of measures to enhance their cyber resilience: 36% conduct threat analyses, 23% use penetration testing, 22% rely on intrusion detection systems, and 15% focus onvulnerability assessments. Network segmentation to limit the impact of attacks is implemented by 19% of companies. Notably, 38% of companies consider the security guarantees of their IT service providers and suppliers to be the ‘most important’ measure.

Regarding budget allocation, one-third of respondents consider the funds for defending against cyberattacks to be ‘limited’ and see room for improvement. In 27% of companies, the cybersecurity budget situation is unclear. Only 34% have an ‘adequate’ or ‘significant’ budget to strengthen their cyber resilience.

What measures does your organization take to ensure the security of the IoT infrastructure? (Multiple answers possible)



Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

“Many companies appear to prioritize cybersecurity only after an incident has already taken place.” –Jan Wendenburg, CEO ONEKEY.

Less than a third (32%) of the companies surveyed in the study have implemented procedures to learn from security incidents and make necessary improvements. Given the ongoing threat landscape, predefined business processes that govern how to handle cyberattacks both during and after an incident should be part of every company's security repertoire.

On a positive note, a good third (34%) of companies conduct a thorough analysis and assessment of a security incident following a cyberattack, in order to derive concrete improvement measures.

LACK OF KNOWLEDGE OF LEGAL CYBERSECURITY REQUIREMENTS

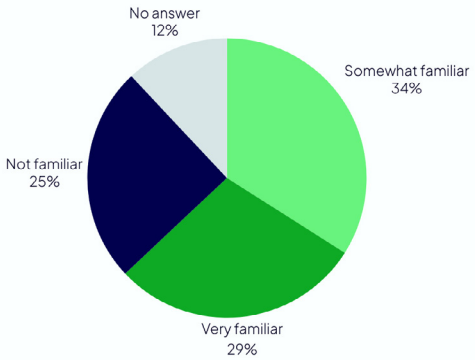
Starting in 2026/2027, the EU Cyber Resilience Act (CRA) will require all manufacturers of devices, machinery, andequipment selling products in the EU to meet enhanced cybersecurity requirements. However, the study reveals that many companies are not yet adequately prepared for this. Only 28% of the surveyed companies have specific compliance regulations for the security of industrial control systems or IIoT devices.

For a third (34%), OT or IoT security regulations are part of the company's general cybersecurity policies but are not specifically addressed. Alarmingly, 19% of companies have made no special provisions in this area. One-fifth of respondents were either unable or unwilling to provide information, indicating significant uncertainty and a high level of unknowns.

Less than a third (29%) of respondents report being familiar with the regulations and cybersecurity standards relevant to their industry. About a third (34%) have limited knowledge, while 25% have no knowledge at all.

Given typical development times of two to three years, companies that do not act in time risk being unable to sell their products in the EU starting in 2027 if they have not met the requirements by then.

Are you familiar with the cybersecurity regulations relevant to your industry?

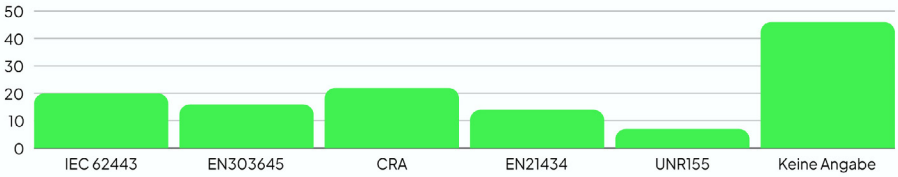


Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

Additionally, 46% of the surveyed companies were unable to specify which cybersecurity standards are relevant to their product development. The importance of these standards is often under estimated: only 23% consider the EU Cyber Resilience Act (CRA) to be relevant.

Other standards, such as IEC62443 (20%), EN 303 645 (16%), EN 21434 (14%), and UNR155 (8%), are also seen as important by only a minority. This highlights the significant information gap regarding compliance.

Which cybersecurity standards are relevant to your organization in product development?

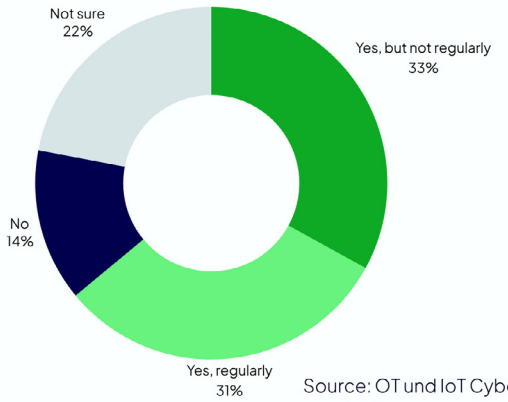


Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

INADEQUATE SECURITY TESTING AND PATCH MANAGEMENT FOR IOT DEVICES

When procuring IoT devices, only 29% of industrial companies conduct thorough security tests. 30% limit themselves to superficial tests or sampling, while 15% perform no security checks at all. There maining companies did not provide any information on this matter. A similar pattern emerges when analyzing device firmware: less than a third (31%) of companies conduct regular security tests to identify vulnerabilities in the embedded software. 47% test the firmware only occasionally or not at all, and 22% did not provide any information on this matter.

Is device firmware analysis — checking the IoT device's internal software for vulnerabilities — practiced in your organization?



Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

“Anyone who delays applying a patch exposes themselves to significant risk, as cybercriminals specifically exploitthe time window between discovery and resolution.” – Jan Wendenburg, CEO ONEKEY.

Regarding software updates, 33% of companies update their devices immediately after a patch becomes available. In contrast, 31% wait until the next scheduled release, while 10% provide no further updates after delivery. An additional 26% of respondents are unsure about their devices’ update policies.

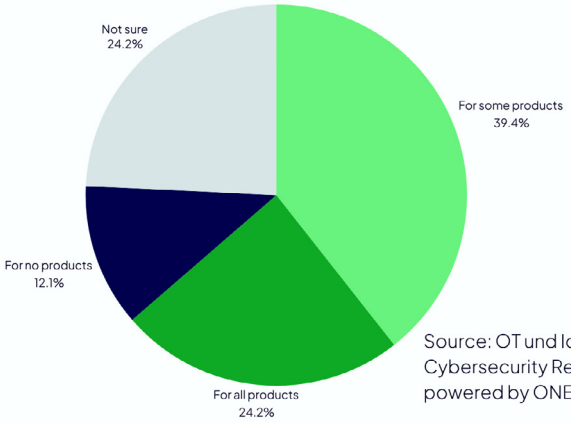
When asked if the cybersecurity of already deployed devices is checked, 28% of companies respond that they do so automatically. 30% conduct occasional manual checks, while 17% perform nofollow-up security assessments. However, waiting for scheduled updates poses significant risks, as cybercriminals often exploit the time window between discovery and resolution.

SBOM: IMPLEMENTATION STILL LACKING

According to the survey, fewer than a quarter (24%) of industrial companies maintain a complete Software Bill Of Materials (SBOM). While software for computers and networks is usually documented, many companies lack an overview of the software in devices, machinery, and equipment.

This is problematic, as outdated software in controlsystems is a common entry point for hackers. Typical examples include manufacturing robots, CNC machines, and building automation systems. These systems are connected to the company network, creating a significant attack surface. However, the majority of companies either have no SBOM or only an incomplete one.

If you use products with digital components (chips, hardware with embedded firmware, etc.) in your organization — do you have a Software Bill of Materials for them?



Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

TRAINING AND AUDITS: ESSENTIAL FOR STRONG CYBERSECURITY AWARENESS

A positive trend is emerging, but there is still significant room for improvement. 40% of industrial companies offer their employees regular cybersecurity training and workshops. 27% have integrated cybersecurity rules into their employee handbooks and company policies.

Additionally, 62% of the surveyed companies conduct regular cybersecurity audits. 24% rely on external assessments, 18% on internal audits, and 20% use a combination of both approaches. However, formore than a third of companies, it is unclear whether and to what extent regular cybersecurity reviews are conducted.

How are employees made aware of their role and responsibility in maintaining cybersecurity?

Source: OT und IoT Cybersecurity Report 2024, powered by ONEKEY | n = 308

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

SecurITy made in Germany

V20250117EN