GDV Gesamtverband der Versicherer

STUDY | CYBERINSURANCE

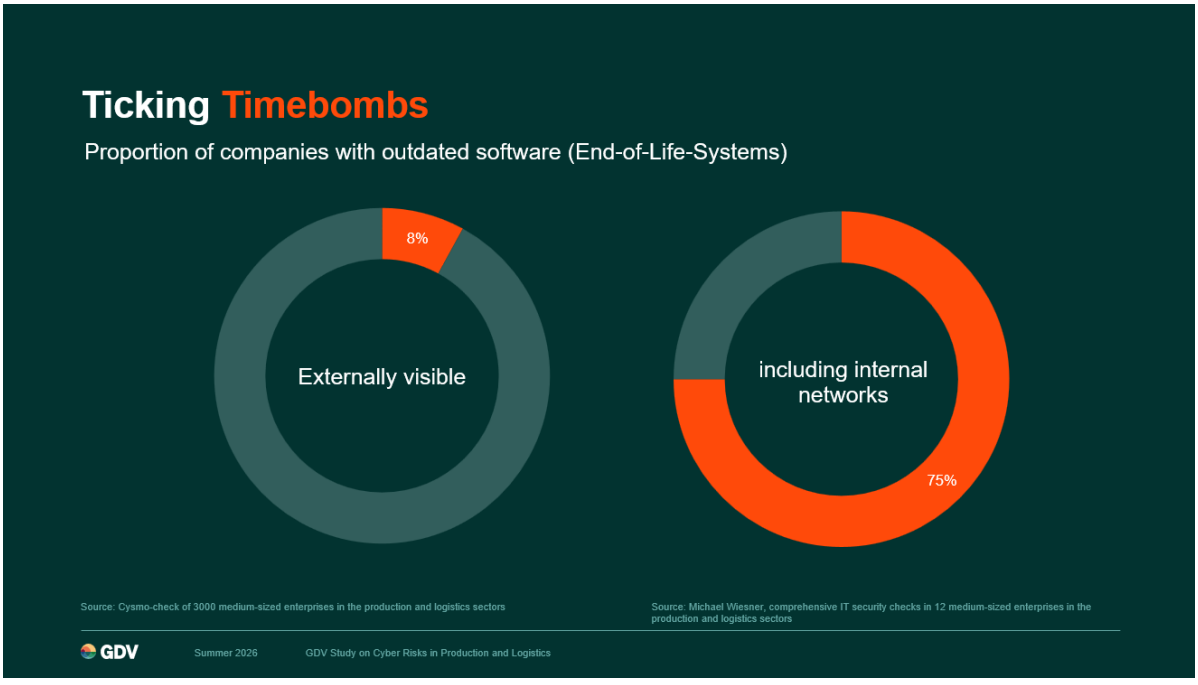
# Cybersecurity in manufacturing and logistics: Three actions for more resilient supply chains

## GDV Study reveals significant shortcomings in IT security

Cyberattacks targeting supply chains have the potential to cause significant damage to the German economy at large. Against this backdrop, a recent study by the GDV highlights the urgent need for action regarding IT security in small and medium-sized manufacturing and logistics companies:

- **Serious security vulnerabilities in IT infrastructure are** the norm rather than the exception in most companies. Commonly known vulnerabilities, which are regularly exploited to gain unauthorised access to systems and blackmail victims, are common in many corporate networks.

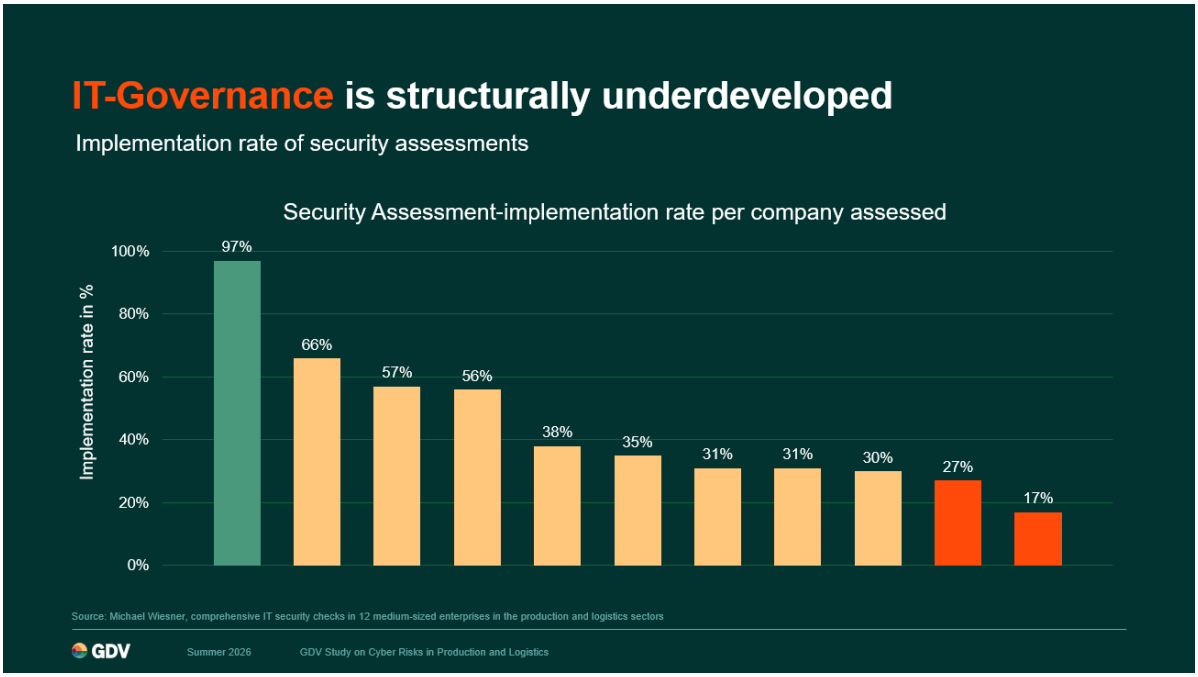
- The most significant problem is **outdated and unsupported software**. An initial analysis of externally visible software showed that more than 250 out of 3000 companies examined were using unsupported or outdated software. A deeper study assessing the internal networks of a dozen companies showed that three-quarters had security vulnerabilities with the highest severity rating (CVSS 10.0).




**Gesamtverband der Deutschen Versicherungswirtschaft e. V.**
Wilhelmstraße 43 / 43G, 10117 Berlin
Tel. 030 2020-5000, Fax 030 2020-6000
www.gdv.de, berlin@gdv.de

**Contact**
Oliver Hauner
Head of Property and Technical Insurance, Cyber, Loss Prevention and Statistics
**Authors**
Henrik Feltens, Dr. Christian Siemens

- **Basic organisational security frameworks and clear lines of responsibility are regularly absent**. Only one of the companies that underwent in-depth cybersecurity testing had a formal information security management system and carried out systematic risk analyses.




- These technical and organisational shortcomings are exacerbated by a **lack of risk awareness amongst employees**. In a phishing test, employees at one in every two companies tested disclosed their login details.

## Three Actions for Enhanced Cyber Resilience

Known, preventable vulnerabilities rather than novel, sophisticated attacks, are the main cyber threat facing manufacturing and logistics firms. In a deeply interconnected economy, the impact of such attacks does not remain limited to individual companies. Combined, these security vulnerabilities present a large-scale threat to Germany's overall cyber resilience and its status as a desirable place to do business. From the insurance industry's perspective, these findings highlight three policy priorities:

1. **Strengthening the cyber security of individual companies with the help of the BSI (German Federal Office for Information Security)**
   The BSI can play a greater role in actively protecting the economy against cyber risks. For this, it is necessary to:
   - Strengthen and further develop the BSI's preventive and coordinating role in ensuring the IT security of the German economy;
   - Expand the BSI's powers to actively detect vulnerabilities and malware as part of a preventative system;
   - Counteract the fragmentation of the regulatory landscape by granting the BSI greater powers as the national authority responsible for cybersecurity.

2. **Managing cyber resilience across supply chains**
   Companies must be aware of their critical cyber dependencies, such as on suppliers, IT service providers, cloud providers and shared software. Security requirements should be appropriately embedded in procurement, contract drafting and supplier management. The Cyber Resilience Act (CRA) and the NIS2 Directive provide important impetus in this regard. Considering the growing threat landscape, these approaches should be expanded on a risk-based basis.

3. **Working together to prepare for systemic events**
   Claims reports received by cyber insurers can provide a rapid and accurate picture of the level of damage to the economy. Combined with a qualitative assessment of the damage situation by key players from the public and private sectors, this information can provide a valid real-time overview of the situation. To improve the data landscape, GDV supports the creation of an appropriate legal framework and platform for the joint exchange of data between government, businesses and the insurance industry. This would enable the real-time exchange of anonymised data on waves of cyber-attacks, new vulnerabilities or escalating damage situations, whilst also being utilised for well-founded risk analyses and the effective implementation of preventive measures.

   Furthermore, the government, the business sector and the insurance industry must clarify a **joint crisis response** in advance of future emergencies. It is essential that all stakeholders share a common understanding of how and which shared response capacities (e.g. IT forensic experts) are to be accessed. Joint tabletop exercises and crisis simulations can ensure that the available resources are prioritised and deployed where they provide the greatest benefit to society.

---

**Source Data**

For this GDV study, publicly available information on the IT systems of 3,000 medium-sized companies in the manufacturing and logistics sectors was collected and analysed. Twelve companies volunteered to take part in in-depth technical and organisational audits.