VDMA

VDMA Study

Industrial Security and Product Piracy

2024

Note

Naturally, we treated the information provided by the participants with the usual discretion. You will therefore find the results in anonymised and summarised form in the following chapters. If you have any further suggestions or questions about the analysis for the next study on industrial security and product piracy, please contact us.

Attorney Dr Friedrich-Philipp Becker
Lawyer (in-house lawyer) / Intellectual property law, IT law, copyright law, UWG
Tel: +49 69 6603-1309
E-mail: friedrich-philipp.becker@vdma.org

Holger Paul
Head of Communications
Tel: +49 69 6603-1922
e-mail: Holger.Paul@vdma.org

Steffen Zimmermann
Head of VDMA Competence Centre Industrial Security
Tel: +49 69 6603-1978
e-mail: Steffen.Zimmermann@vdma.org

VDMA
Lyoner Str. 18
60528 Frankfurt am Main

www.vdma.org

Status: 10.04.2024

Table of contents

1 Introduction

Every two years, the VDMA conducts a study on product and brand piracy among its member companies. For over 20 years, reliable figures and information have been collected to provide a picture of the threat posed by counterfeiting, piracy and illegal copying in our industry. This year, the study was expanded to include the topic of industrial security for the first time in order to take into account the increased digital networking of products and the associated digital threats to mechanical and plant engineering. This is confirmed by the survey results: 96 per cent of the companies surveyed use cybersecurity measures to protect their business premises against attacks. As a result, several questions on the topic of product piracy were omitted in this year's questionnaire in order to keep it to a manageable size.

Definition of product piracy

The study relates solely to unauthorised copying. Unauthorised copying (referred to here synonymously as product piracy or plagiarism) is defined as:

- reproduction in violation of special protection rights (e.g. trademarks, patents) or
- reproduction without infringing special protection rights, but which infringes copyright and/or has been copied in an anti-competitive manner.

Counterfeiting is anti-competitive if, in addition to the imitation, an unfair act also occurs. This unfair act is usually a deception about the manufacturer of the original product (risk of confusion) and the associated exploitation of the good reputation.

Definition of Industrial Security

Industrial security is the protection of technical systems in production, manufacturing and intralogistics against basically unknown attacks and disruptions with the aim of maintaining the business process in operation. Technical systems are defined as machines and systems, their industrial control components, network components, sensors and actuators as well as the services connected to the systems.

Attacks and malfunctions of technical systems are caused by people or the system's surroundings (environment). For a better understanding, this can be reduced to "protecting the machine from people".

Industrial security should be understood as a process that provides protection against failure, loss of expertise, espionage and manipulation of machines, systems and industrial data. Security incidents from the "office environment" (IT/cybersecurity) are also relevant if they have an impact on machines or systems.

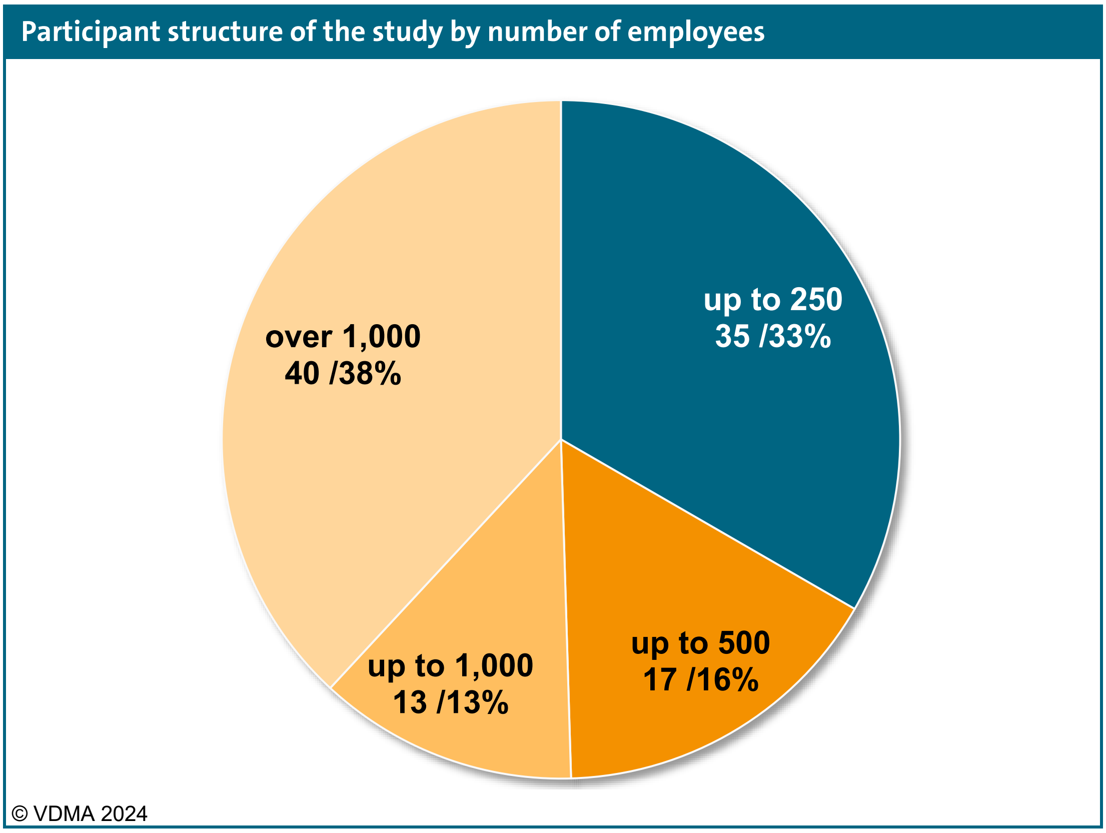
Participant structure 2024

This year, 105 VDMA member companies took part in the study on industrial security and product piracy during the data collection period from the beginning to the end of February. Compared to the last study in 2022, the number of participants has thus risen significantly from 68, which may be partly due to the addition of the topic of industrial security.
Naturally, the sample size per question fluctuates, as not all participants respond to all questions. The respective sample size is therefore indicated for the individual questions.

Compared to the last study, the absolute number of responses attributable to small and medium-sized enterprises has remained largely identical. Their share has thus decreased significantly by 13 percentage points to 33 per cent. The majority of the additional feedback was distributed among companies with more than 250 employees. While the percentage share of companies with more than 1,000 employees remains largely the same (+1 percentage point), companies with employee numbers between 250 and 1,000 are thus more prominent.

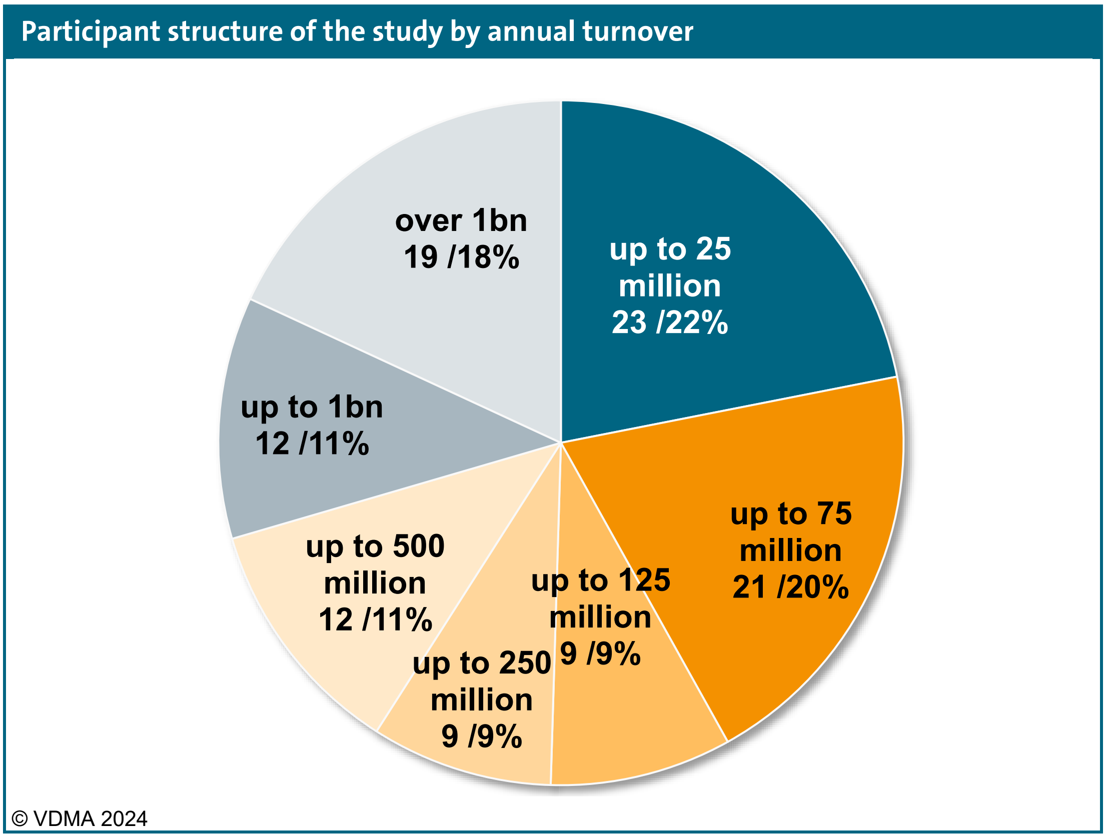
The exact participant structure by number of employees and annual turnover can be seen in the following two charts.

Participant structure of the study by number of employees



Breakdown of study participants by number of employees. N=105

Participant structure of the study by annual turnover



© VDMA 2024

Breakdown of study participants by annual turnover. N=105

2 Management Summary

This year, the study on product piracy was expanded for the first time to include questions from the field of industrial security.

The companies surveyed reported a record low in the number of companies affected by product and/or brand piracy: **46 per cent of the companies surveyed in the German mechanical and plant engineering sector stated that they were affected by product or brand piracy**. While this means that around every second company is still affected, this represents a **decrease of 26 percentage points**. This is a positive development after a significant increase in the number of measures taken in the previous study. It is possible that this decline was additionally reinforced by the fact that the inclusion of the new topic of industrial security motivated companies to participate for which industrial security is of great importance, but which are not affected by product piracy.

The high relevance of industrial security is also reflected in the responses: **96 per cent of respondents protect their business premises with at least one cybersecurity measure.** In addition, 59 per cent have signed a cyber insurance. 6 per cent of respondents have already had to make use of such an insurance.

This is also reflected in the willingness of companies to get involved in local or regional **cyber alliances**: **13 per cent are already involved and 50 per cent can imagine getting involved in principle.**

In line with the decline in the number of people affected by product piracy, the damage caused by product or brand piracy has also fallen significantly compared to previous studies: **the estimated damage amounts to 4.1 billion euros per year and is therefore 2.3 billion euros lower than recently.** A turnover in this amount of damage would secure almost 16,000 jobs in the industry.

The People's Republic of China is once again the undisputed leader as the country of origin of counterfeits with 82 per cent. Despite a decline in the number of reports, Germany remains in third place among the countries of origin with 16 per cent, behind India with 18 per cent.

Counterfeiting remains a constant security risk

Counterfeit products can clearly imply a safety risk: **two out of three companies report that counterfeit products pose a risk.** Around one in two counterfeits pose a risk to the system, and **in 40 per cent of cases it implies a risk to people, for example the operator of a system.**

Help: Guidelines and standards as a first source of information

VDMA papers on "Product and know-how protection", "Measures at trade fairs" and "Industrial security" offer affected companies support in selecting and implementing suitable protective measures. Further information can be found in the current list of publications at the end of the study.

The most important results of the VDMA study Industrial Security and Product Piracy 2024:

- **Around one in four companies has been affected by a significant cybersecurity incident in the past two years.**
- **96 per cent of respondents secure their business premises with at least one cybersecurity measure.** In addition to regular backups and updates of operating systems and applications, 80 per cent of the companies surveyed use measures to detect attacks in order to be able to initiate countermeasures at an early stage.
- The willingness to get involved in a local or regional cyber alliance is high: **13 per cent are already involved and 50 per cent can imagine getting involved in principle.**
- **46 per cent of companies in the mechanical and plant engineering sector are affected by product piracy** (2022: 72 per cent)
- **The estimated damage caused by product piracy in the fiscal year 2023 amounted to 4.1 billion euros**, a significant decrease of 2.3 billion euros compared to the 2022 study**. The average damage for affected companies also fell to 3.5 per cent of annual turnover, down from 4.9 per cent.**
- The loss of sales of 4.1 billion euros corresponds to around 16,000 jobs (2022: 29,000).
- The People's Republic of **China clearly tops the list of countries of origin of counterfeits with 82 per cent. India follows in second place with 18 per cent**, ahead of Germany in third place (16 per cent).
- At 58 per cent, direct competitors appear less frequently than before as plagiarists or customers of plagiarism (2022: 70 per cent). **On the other hand, there has been a significant increase in professional large-scale plagiarists (42 per cent) and state-owned companies (18 per cent), with an increase of 40 and 63 per cent respectively.**
- **Customers and suppliers are no longer relevant plagiarists:** after recent increases, customers now only account for 6 per cent (2022: 26 per cent) and suppliers were not mentioned by any company.
- In terms of infringements of intellectual property rights, **brand piracy (49 per cent) has now overtaken unfair copying (44 per cent) to take second place.** The infringement of other rights, such as copyright, has risen again by 9 percentage points to 37 per cent compared to the previous study. The **increase in the infringement of utility models and designs is particularly marked.**
- The two categories of "components" and "external appearance (design)" remain the most frequent forms of plagiarism in around 60 per cent of cases. So-called "soft" plagiarism (catalogues, brochures, product photos) occurs less frequently and has once again risen to the level of four years ago. **Plagiarism of websites and online shops, operating instructions and technical documentation, consumables and digital services has increased significantly.**
- **Counterfeit products demonstrably remain a safety risk:** 41 per cent of companies report counterfeit products that pose a risk to operators or users. **More than half of those surveyed (54 per cent) believe that the counterfeits discovered pose a risk to the safe operation of the system.**

The VDMA acts

Product piracy and cyber attacks are a huge threat to the innovative strength and competitiveness of our industry. The dangers of piracy, loss of expertise and cyberattacks such as ransomware are proving to be very diverse in mechanical and plant engineering. The digital transformation in particular is creating new challenges for the protection of data and information, both in product development and in the operation of machines and systems. At the same time, digital services and integrated protective measures are a good way to differentiate yourself from counterfeiters with added value, make it more difficult to easily copy products and ensure the integrity of the supply chain.

We advise companies to adopt a comprehensive defense strategy that is adapted to the company's situation and individual product risks in order to deal with cyber attacks and product piracy in the long term. Various coordinated measures should be combined to create a customized protection concept in accordance with ISO 22384 ("Cyber-Physical Product Security"). In the field of product piracy, legal protection measures should always be taken in the form of property right applications in the respective markets. It is virtually impossible to enforce rights without an IP application. Organizational and technical measures must also be considered, involving both the company's own employees and its suppliers, dealers and customers.

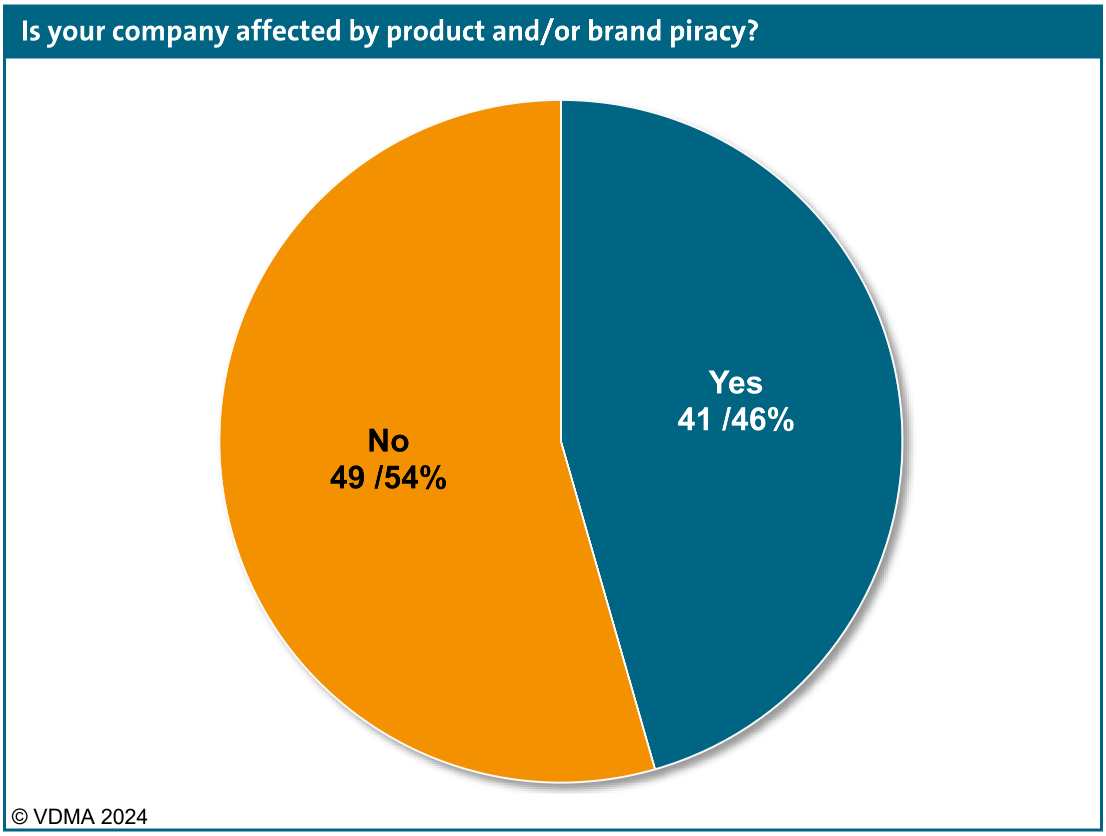
The VDMA actively supports its member companies in various areas:

- The legal department provides advice and information on legal issues.
- The VDMA working group "Industrial Property Protection" brings together affected member companies on organizational and legal measures.
- Through our offices in Berlin and Brussels, we are continuing to increase the pressure on the German government and the European Union to take more decisive action against product piracy.
- The VDMA working groups "Industrial Security", "NIS2" and "Information Security" brings together member companies to gain knowledge and share experiences in the field of digital attacks and protective measures.
- The VDMA played a leading role in ISO 22384 "Guidelines to establish and monitor a protection plan and its implementation".
- The VDMA is the deputy chairman of the German mirror committee of ISO/TC 292 "Security and resilience", the NIA-02-01 "Measures for the authenticity and integrity of products".
- Annual user days on the topics of "Information Security (IT/OT)" and "Product Security" offer member companies up-to-date information on regulation, standardization and insights into tried-and-tested solutions.

3 Affectedness in product piracy

While product piracy has been a constant and enormous threat to the innovative strength and competitiveness of our industry in previous studies, this study shows for the first time a **significant decline of 26 percentage points to a historic low of 46 per cent.** As pleasing as this decline is at first glance, the result nevertheless shows that **every second company surveyed** is **still affected by product and/or brand piracy.**

The study does not provide any direct conclusions as to the cause of this decline. However, it should be noted that the topic of industrial security was included in the study for the first time, which potentially motivated companies to participate for which industrial security is a high priority but which are not affected by product piracy.

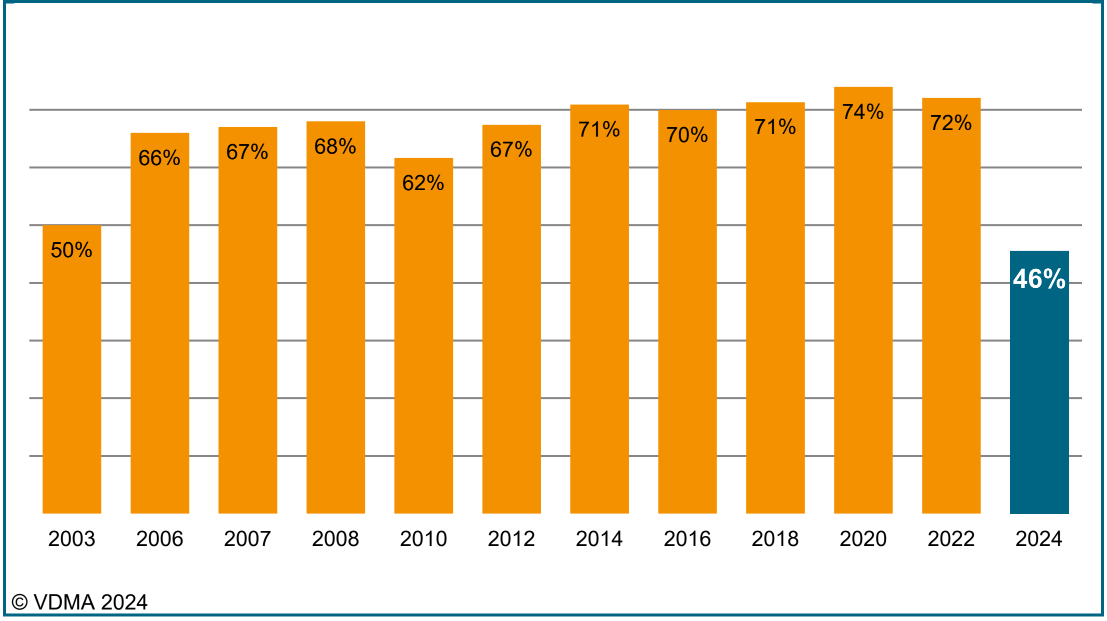


Is your company affected by product and/or brand piracy?

© VDMA 2024

Proportion of companies affected by product and brand piracy. N=90

Companies affected by product and brand piracy in mechanical and plant engineering in a year-on-year comparison



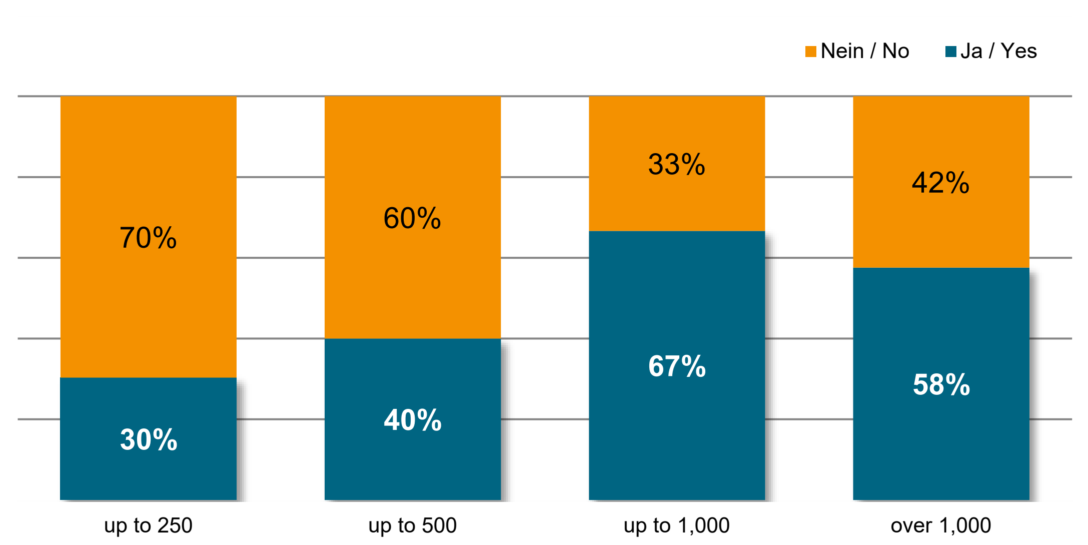
Percentage of companies affected compared to previous years. N=90 (2024)

A year-on-year comparison clearly shows the significant decline: for the **first time in ten years, the proportion of companies affected by product and/or brand piracy has fallen below the threshold of 70 per cent and, at a historic low of 46 per cent, is even lower than the figure at the beginning of the study in 2003.**

Accordingly, the efforts and activities against product and brand piracy, which increased significantly in the last study, appear to be making themselves felt. However, the results on the question of the type of counterfeiting also show that the focus is shifting to categories that have not yet played a major role. **Activities on both the business and political side must therefore not be reduced under any circumstances, but must also adapt to the new circumstances.**

The breakdown of companies affected by product and/or brand piracy by company size reveals familiar trends. Broken down by both the number of employees and annual turnover, the incentive for counterfeiters to share in this success increases with the size of the company. However, the general decline in affectedness is also reflected here, meaning that a lower proportion of companies of all sizes reported being affected by product and/or brand piracy.

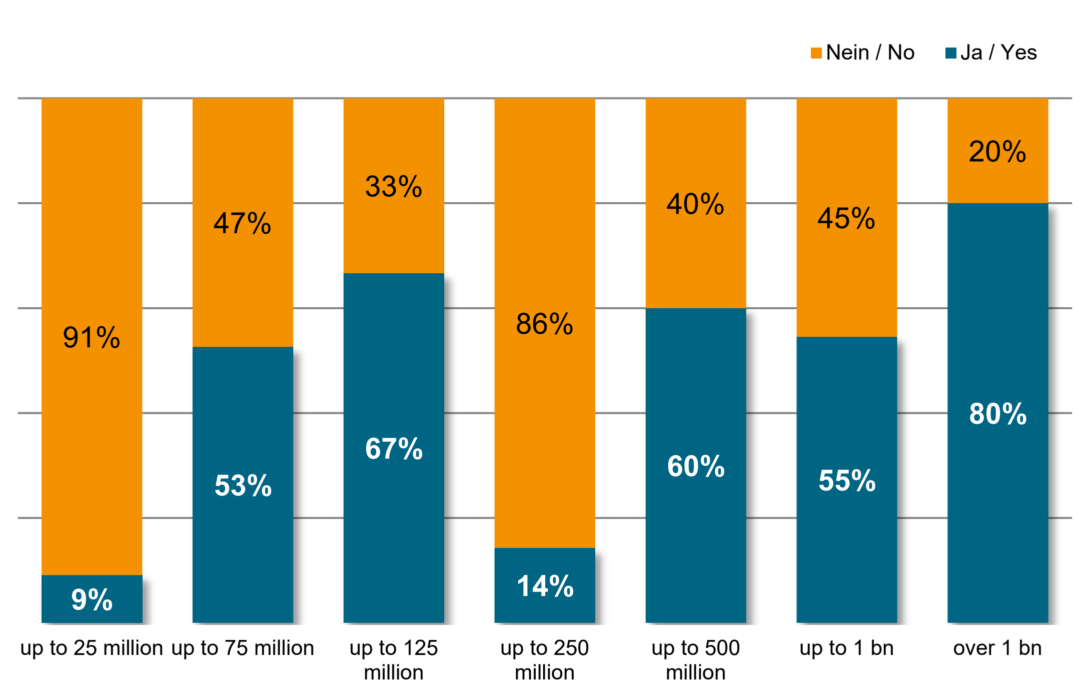
Companies affected by company size (number of employees)



© VDMA 2024

Proportion of companies affected by product and brand piracy by number of employees. N=90

Companies concerned by annual turnover in EUR



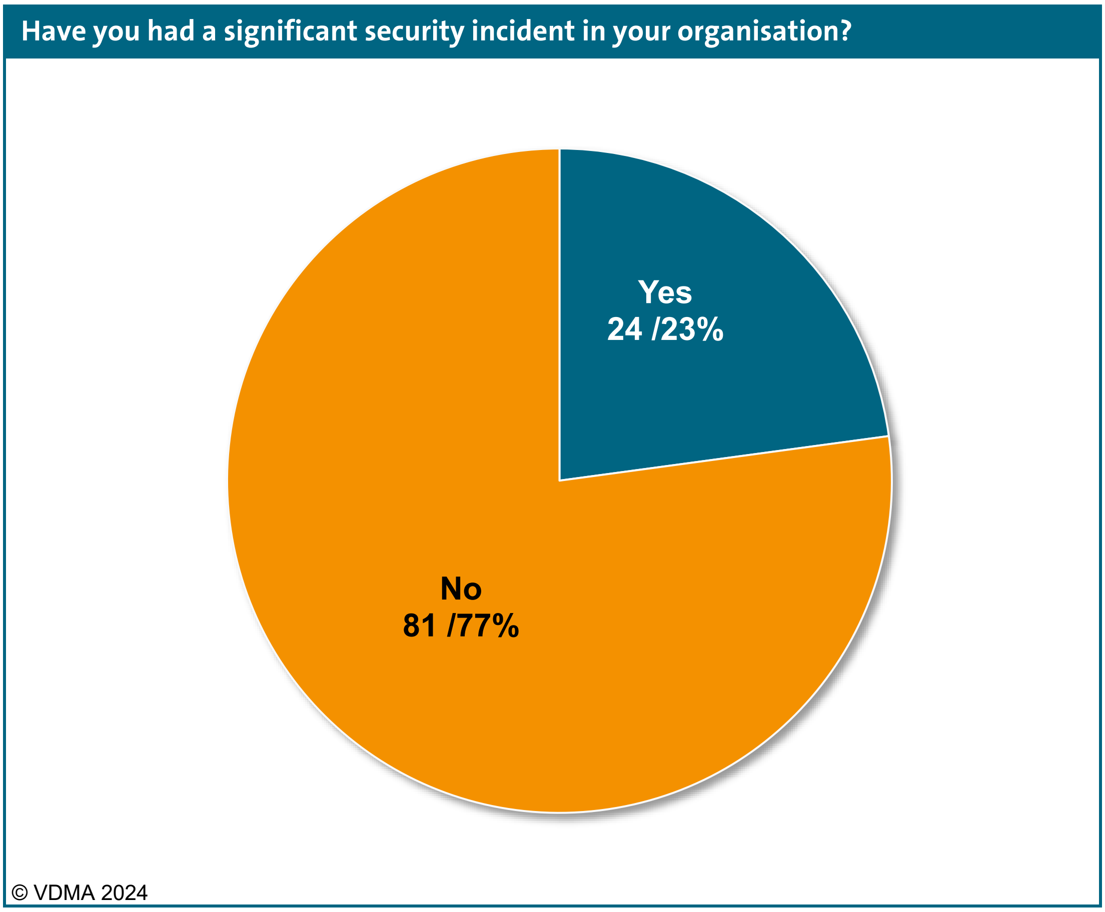
© VDMA 2024

Proportion of companies affected by product and brand piracy by number of employees. N=90

4 Affectedness in industrial security

This year, questions from the field of industrial security were included in the study for the first time. Even if this topic area appears to be separate from classic product and brand piracy at first glance, the two topics are nevertheless intertwined. For example, cybersecurity incidents can take a destructive direction, such as the infestation of ransomware, or they can lead to industrial espionage and thus to an outflow of expertise.

When asked whether a **significant cybersecurity incident** had occurred in the company in the past two years, **around one in four of the companies surveyed answered in the affirmative**.


Have you had a significant security incident in your organisation?

© VDMA 2024

Proportion of companies that have experienced significant cybersecurity incident. N=105

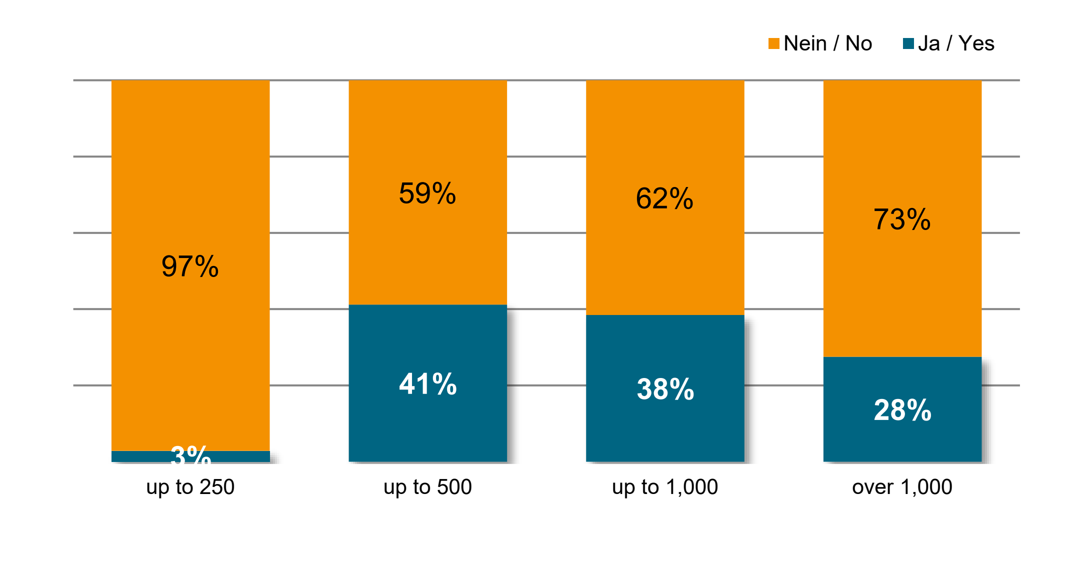
Definition of significant cybersecurity incident, according to Art. 23, paragraph 3 of the NIS2 Directive:

A security incident is considered significant, if:
(a) it has caused or is likely to cause serious disruption to the operation of services or financial loss for the entitiy concerned;
b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Broken down by company size, the question about a significant cybersecurity incident shows a similar picture to the question about being affected by product and/or brand piracy.

While small companies with fewer than 250 employees or an annual turnover of less than 25 million euros report almost no significant incidents, both the attack surface and the attractiveness for attackers increase with company size, so that on average one in three companies surveyed reports a significant cybersecurity incident.

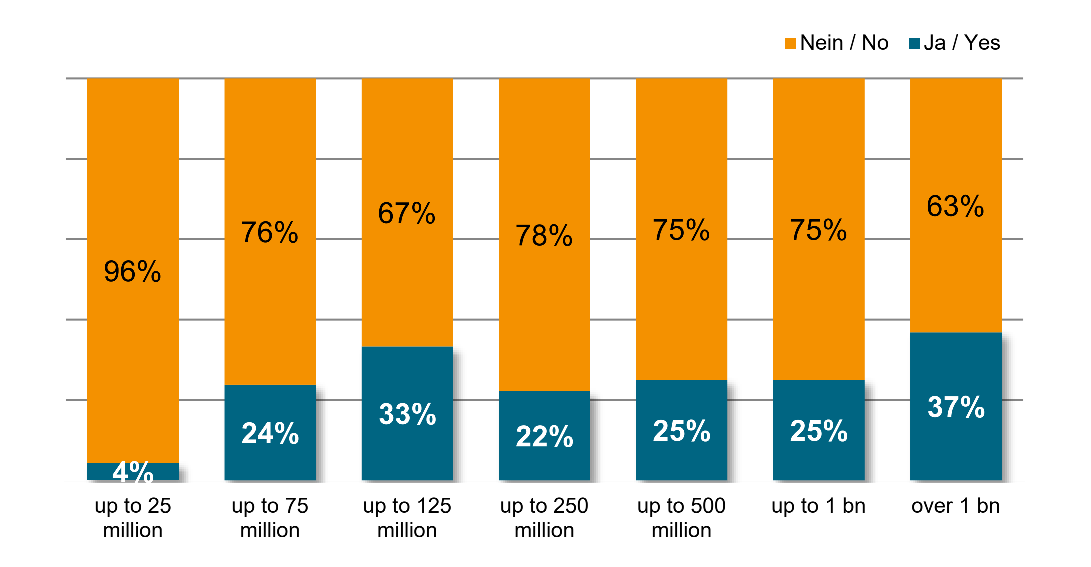
Significant cybersecurity incidents by company size (number of employees)



© VDMA 2024

Percentage of companies with at least one significant cybersecurity incident by number of employees.
N=105

Significant cybersecurity incidents by annual revenue in EUR

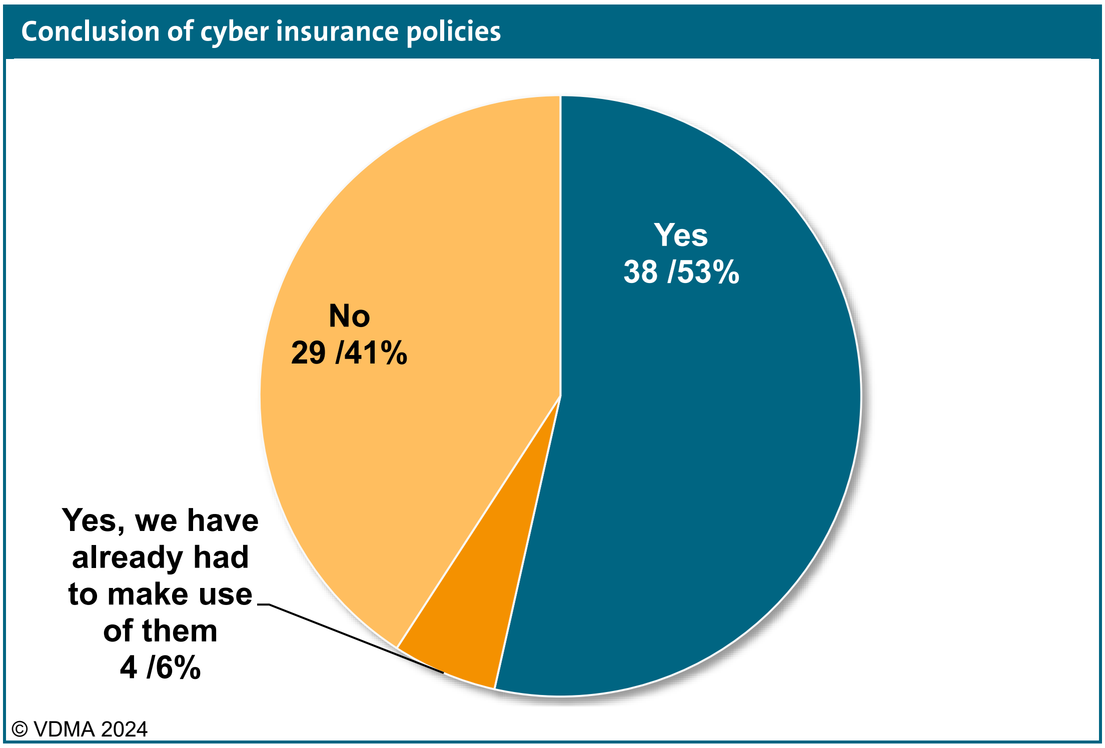


© VDMA 2024

Percentage of companies with at least one significant cybersecurity incident by annual turnover. N=105

Damage caused by cybersecurity incidents is sometimes difficult to predict or quantify. For this reason, there are cyber insurance policies that can be used to control and regulate such consequences.

More than half of respondents (59 per cent) answered in the affirmative to our question as to whether the company had taken out cyber insurance. **In 6 per cent of cases, this cyber insurance had already been made use of.**
None of the respondents had previously had cyber insurance, but had cancelled it.



Conclusion of cyber insurance policies

© VDMA 2024

Existence and utilization of cyber insurance. N=71 (2024)

VSMA, the VDMA's insurance broker, reports the following from its experience with cyber insurance in mechanical and plant engineering in its "VSMA Market Forecast 2024"[1]:
"*The constantly increasing risks continue to have a negative impact on the cyber insurance market. The restrictive underwriting policy of insurers already observed last year is continuing.*

Premiums and deductibles are currently being brought into line with a higher market level, with increases of up to 30 per cent across the market as a whole; in the case of risks involving claims, increases of up to 150 per cent are possible.

In order to renew existing cyber insurance policies or take out new ones, minimum standards in the area of IT security must be met. The IT/cybersecurity maturity level is crucial for many insurers and is sometimes comprehensively reviewed."

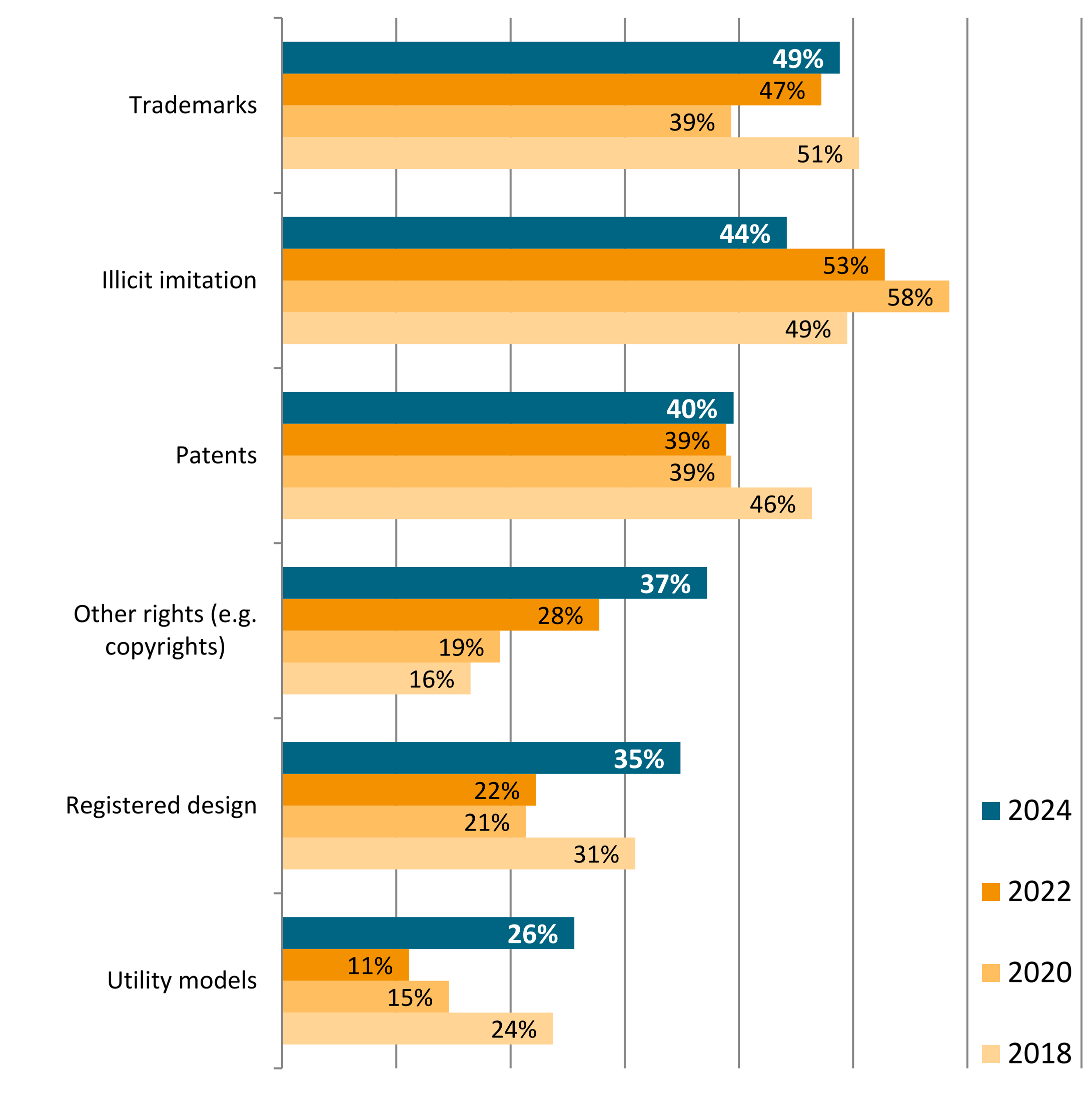
[1] https://www.vsma.de/bestellung-vsma-marktprognose/

5 Infringement of industrial property rights

When asked about the type of infringement of intellectual property rights, a steady decline of 9 percentage points to 43 per cent can still be seen compared to the last study. With another slight increase, **trademark piracy is now the number one property right infringement in around half of the reported cases.**

While there have been no significant changes in patent infringements compared to the last study, **infringements of other rights, designs and utility models have increased significantly.** The first two cases thus account for more than one in three cases. The infringement of utility models in particular shows a trend reversal with a significant increase to one in four cases.

Types of property right infringements through product and brand piracy



© VDMA 2024

Types of property right infringements. N=43 (2024, multiple answers possible)

6 Typical types of plagiarism

The fact that plagiarism can involve many different forms of imitation and counterfeiting is once again evident this year in the answers to the question about the type of plagiarism.

After falling by 7 percentage points, counterfeiting of external appearance is now only in second place among the typical types of counterfeiting at 56 per cent. **At 58 per cent, plagiarism of components is once again in first place.**

After the last study showed a decline in plagiarism of catalogues, brochures and product photos, these types of plagiarism are still in third place among the typical types of plagiarism with an increase to 36 percent.

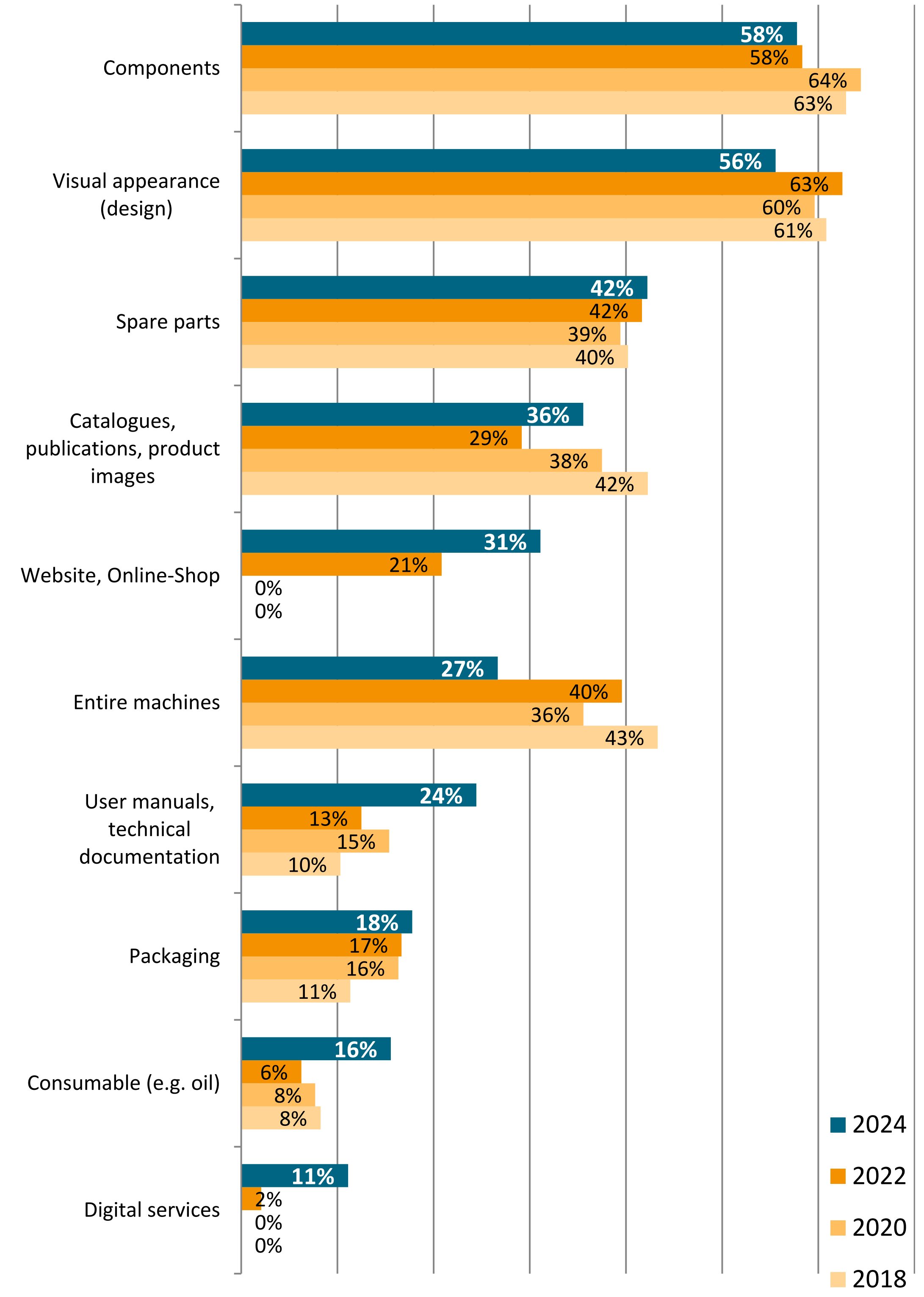
In the last study, we asked about website and online shop plagiarism for the first time, with one in five companies reporting this. This figure has increased significantly by 10 percentage points to almost one in three companies. **A similar trend can be seen in the case of plagiarism of digital services, which was observed by five times as many companies compared to the last study, bringing the figure to 11 per cent.**

Plagiarism of operating instructions and technical documentation slipped from one of the last places into the middle of the field, being **reported by around one in four companies.**

The only significant decline was seen in the plagiarization of entire machines. After 40 per cent in the last study, this type of plagiarism was only observed in just over one in four companies.

There have been no significant changes in counterfeit components, spare parts and packaging.

What was plagiarised?



Types of plagiarism. N=45 (2024, multiple answers possible)

7 Plagiarists and their clients

One question in the study aimed to establish who produces and distributes the counterfeits and who commissions them.

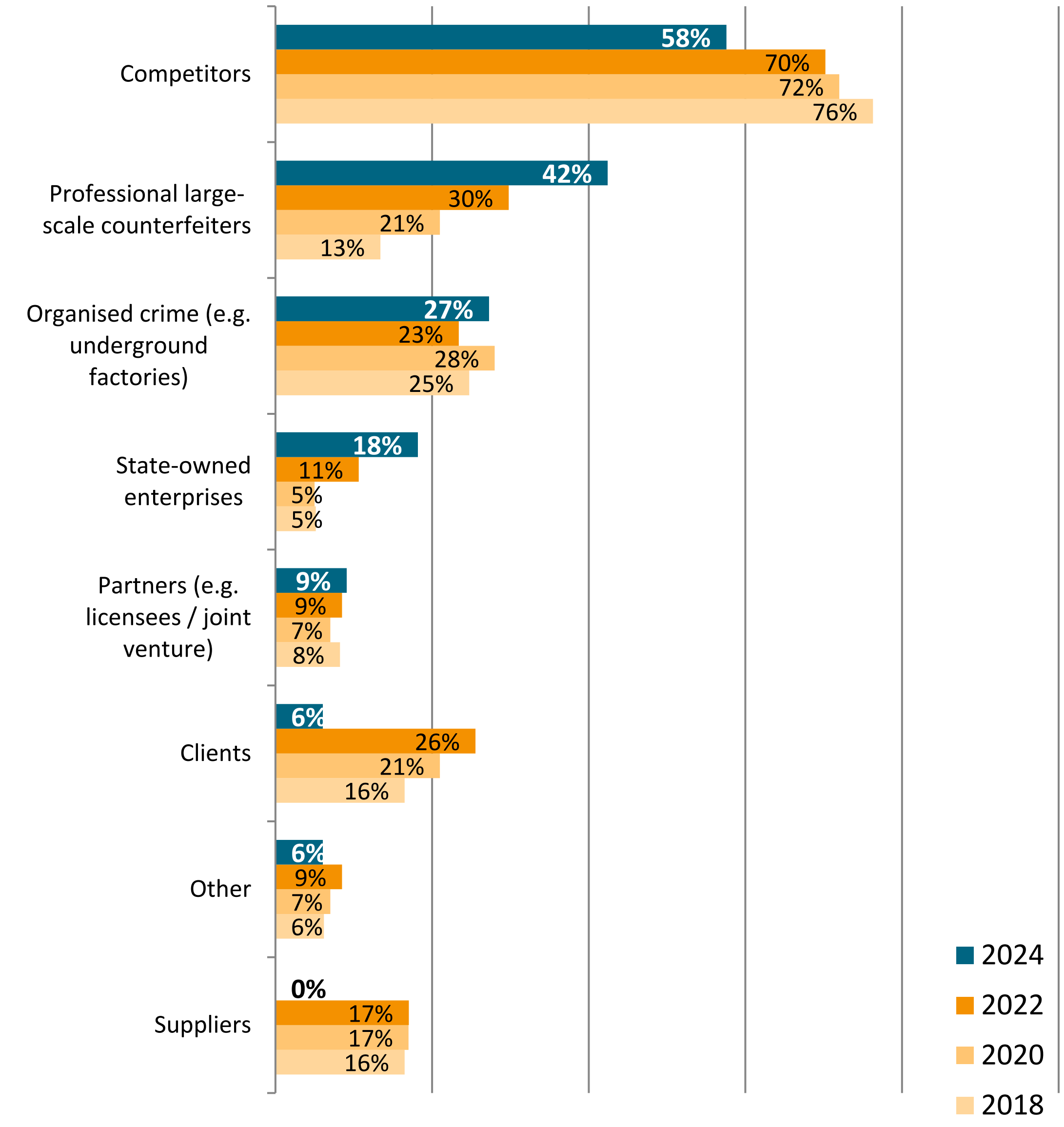
Direct competitors remain in first place among plagiarizers. However, with a significant decline, they are now only mentioned by 58 per cent of companies. **In contrast, professional large-scale plagiarists have become significantly more important**, with 42 per cent of the companies concerned naming them as the originators of plagiarism, continuing the clear growth trend that has been in place for the past six years.

A comparable trend can be seen in state-owned companies, which are now steadily moving further into the spotlight with 18 per cent.

While there were no significant changes in organized crime and direct business partners, there were notable decreases in the category of customers and suppliers: **none of the companies affected reported suppliers as a source of counterfeiting, and** with a decrease of 77 percent, **only 6 percent reported direct customers.**

Investments in protective measures for trade and business secrets may pay off here. Circumventing these protective measures usually requires a great deal of effort, which can primarily only be mustered by professional large-scale plagiarists, organized crime or state-owned companies.

Plagiariser, if applicable, principal of plagiarism



Plagiarists and, if applicable, their clients.

N=33 (2024, multiple answers possible)

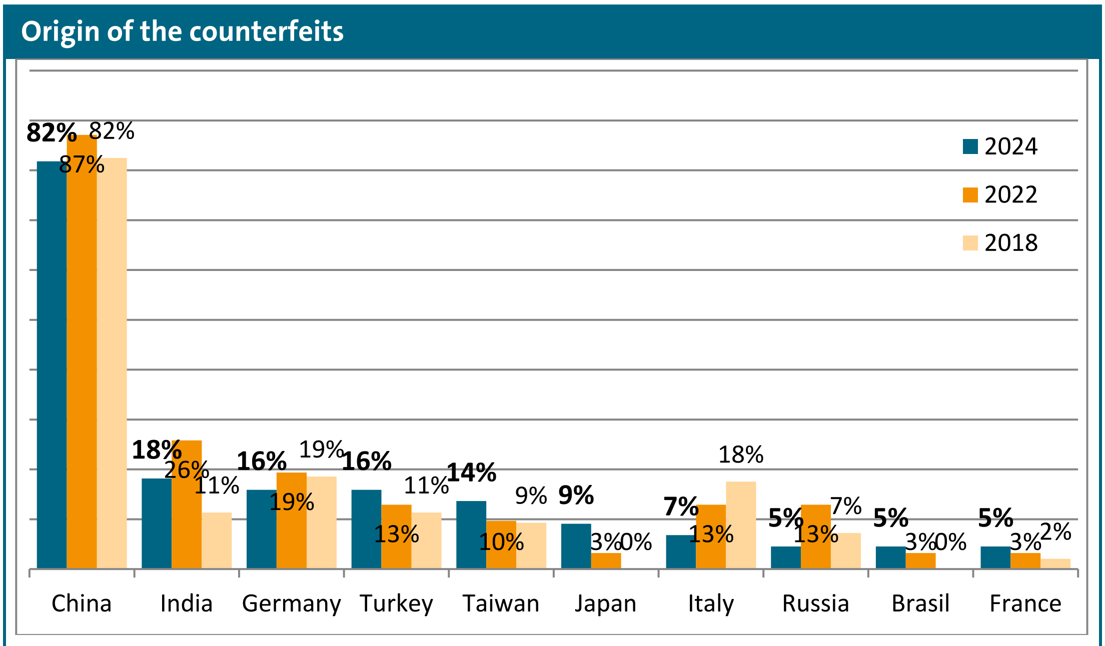
8 Origin of counterfeits

The People's Republic of China remains the undisputed leader when it comes to the origin of counterfeits: **with a slight decline, 82 per cent of the companies in the survey named China as the country where counterfeits are manufactured.**

Despite a decline to 18 per cent, **India** follows **in second place**, having Germany slide one spot for the first time in the previous study to take third place (16 per cent this time).

The figures for 2020 are not included in the analysis, as this study only asked about the country of distribution and not the country of origin of counterfeits.

Origin of the counterfeits



© VDMA 2024

Countries of origin, TOP 10 mentions

N=44 (2024, multiple answers possible)

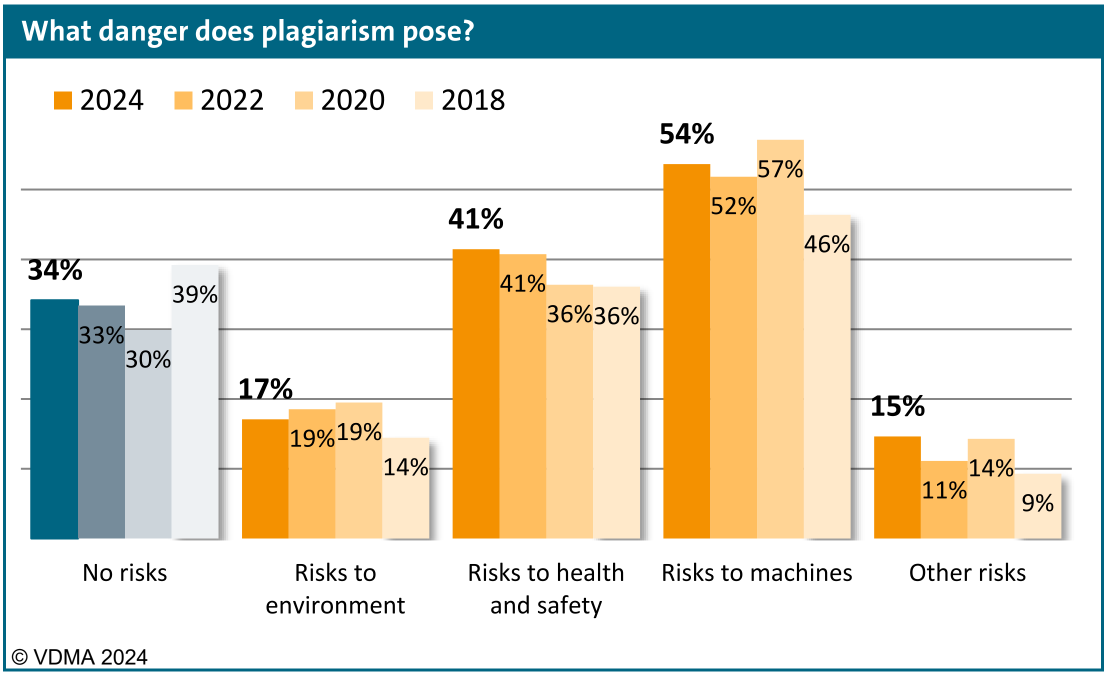
9 Dangers of plagiarism

Since the study in 2016, we have been asking about the potential risks posed by the counterfeits discovered, for example for people due to missing or non-functional safety equipment or for the system due to poor-quality spare parts.

There were no significant changes this year: **in more than half of the cases, the use of a counterfeit product poses a risk to the system**, for example due to increased wear and tear when using low-quality spare parts. **In more than 40 per cent of cases there is also a direct risk to persons**, for example to the operator of the machine.

Only in around one in three cases does the plagiarism pose no particular danger.

In some cases, the original manufacturers also saw risks for their own company, for example through damage to their reputation due to reduced reliability or lower quality in the case of counterfeit products, competitive disadvantages or general economic losses.



Risk potential of discovered counterfeits. N=27 (2024, multiple answers possible)

For this reason alone, care should always be taken to ensure the safe and reliable operation of machines and systems to prevent counterfeit products from creeping in. Especially with regard to the health and safety of your own employees, but also for financial reasons, as system failures or customer complaints can result in follow-up costs and damage to your image.

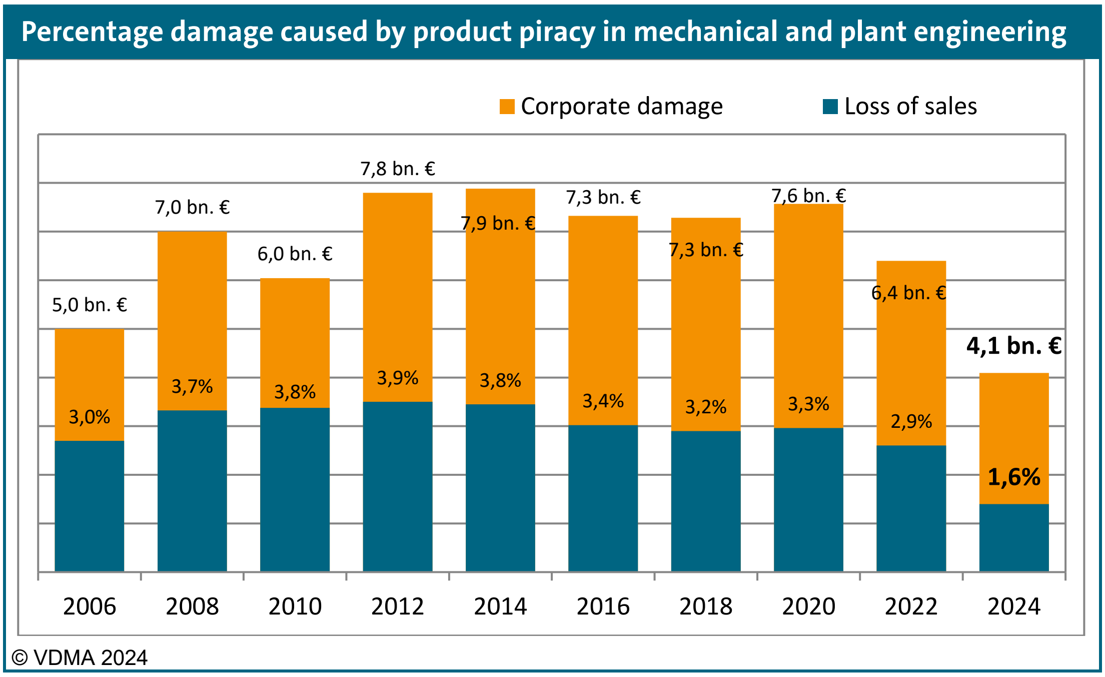
10 Company damage due to plagiarism

In this chapter, we address the question of the estimated company damage caused by product and brand piracy. The self-assessment of company damage is based not only on the pure loss of sales, but also on any subsequent damage to image, incorrect claims under warranty, product liability or similar and was stated by the study participants as a percentage.

Together with the value for the annual turnover of the German mechanical and plant engineering industry[2] from the previous year, an absolute figure can be calculated for the company damage caused by product and brand piracy. The VDMA's regular surveys and analyses provide a good estimate of how the damage caused by product piracy has developed in recent years.

The estimated business losses incurred by German mechanical and plant engineering companies in 2023 continued the general downward trend since 2014, jumping to a record low of 1.6 per cent in parallel with the significant decline in the number of affected companies.

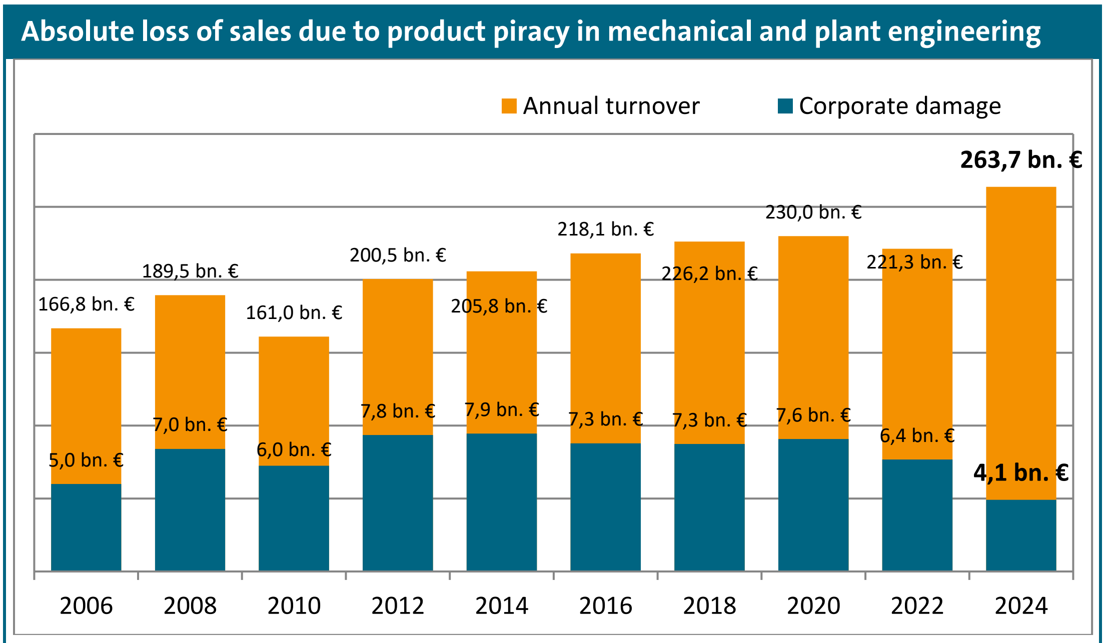
As the annual turnover of the entire industry rose to 263.7 billion euros in the same period, the absolute company loss fell slightly less, but still significantly, to 4.1 billion euros. **A turnover share of this amount corresponds to around 16,000 jobs in mechanical and plant engineering.**



Company loss in EUR and loss of turnover in per cent by product piracy in Germany. N=47 (2024)

[2] Source: Federal Statistical Office/VDMA, companies with more than 50 employees.

Absolute loss of sales due to product piracy in mechanical and plant engineering



© VDMA 2024

Industry turnover of the previous year and damage by product piracy in Germany. N=47 (2024)

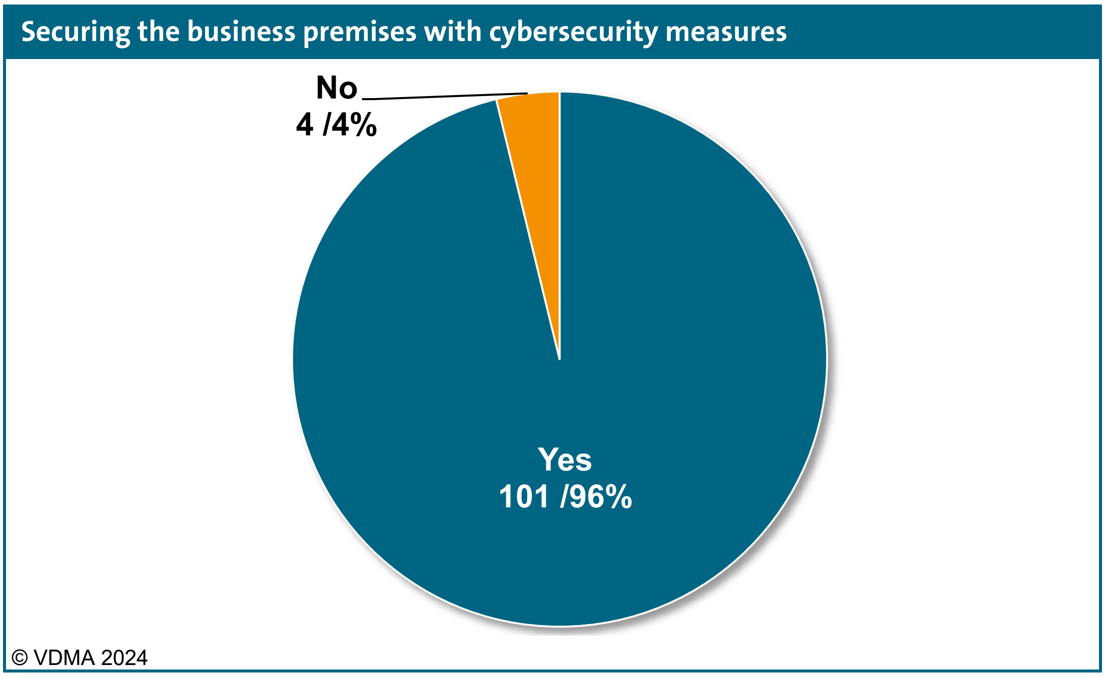
The loss of turnover of 1.6 per cent reflects the overall average of the study participants. This means that not only affected companies are included, but also companies that have not suffered any losses in the past two years.

If only those companies that have actually reported a loss of sales due to product piracy are included in the calculation, the average loss of sales is naturally higher and reaches an average value of 3.5 per cent.

11 Measures in industrial security

Chapter 4 presented the percentage of companies surveyed that have been affected by a significant cybersecurity incident in the last two years.

We asked about the cybersecurity measures that companies are taking to secure their business premises. The impressive summary: **96 per cent of the companies surveyed implement at least one cybersecurity measure.**



Securing the business premises with cybersecurity measures

© VDMA 2024

Proportion of companies that implement at least one cybersecurity measure. N=105

Specifically, **95 per cent of companies already use backup measures to** prevent the loss of important documents, settings data or know-how. **Updates for both operating systems and application software are also regularly implemented by more than nine out of ten companies surveyed.**

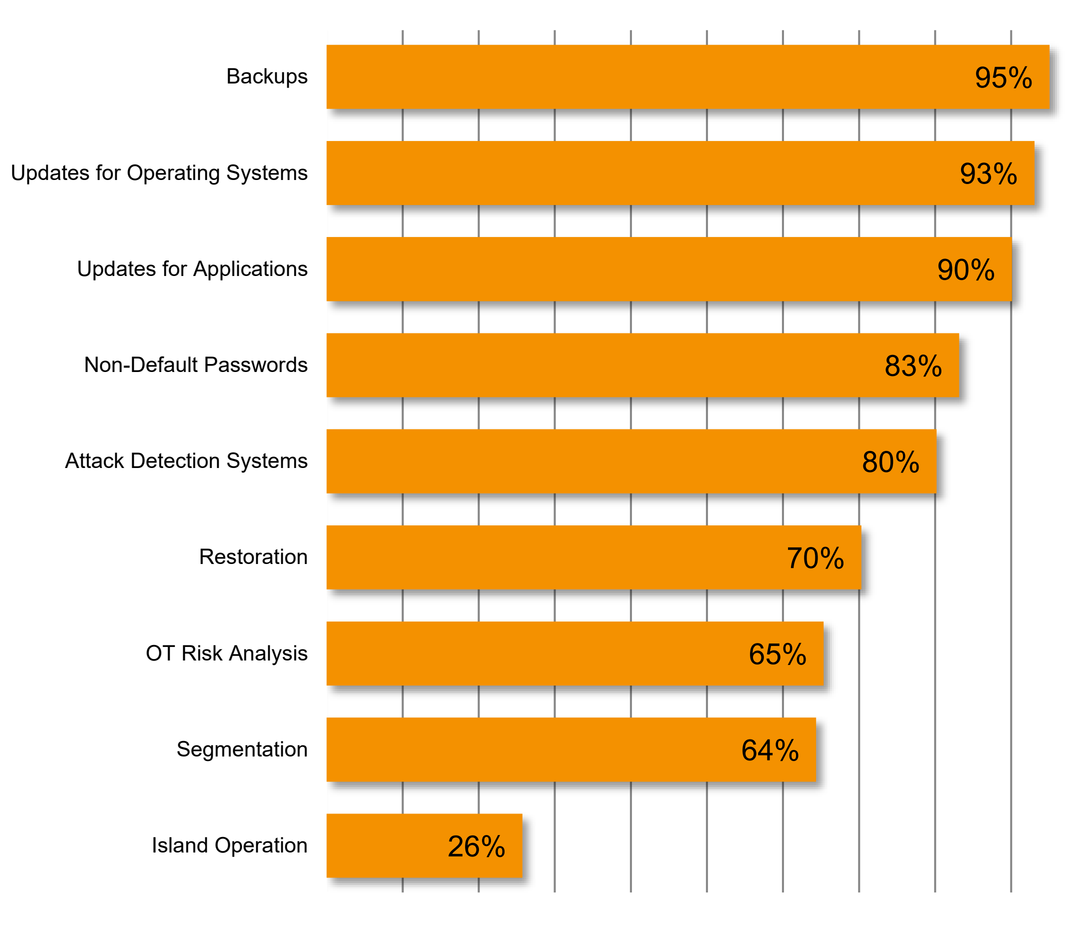
It is surprising that only 70 per cent of the companies surveyed implement data recovery as a cybersecurity measure, whereas backups were mentioned by 95 per cent. **However, a backup strategy without suitable recovery processes can quickly prove inadequate in an emergency.**

Active attack detection, i.e. the early detection of attackers in order to initiate further countermeasures and minimise major damage, is implemented as a measure by four out of five companies.

The fact that **only 83 per cent of respondents stated that they do not use standard passwords** but instead personalise their passwords is somewhat disconcerting. Metaphorically speaking, this means that almost one in five companies have the key permanently in the door lock.

The cybersecurity measure of „island operation“, which means significantly more intervention in the business premises and operating processes, but can also offer appropriate protection, is implemented by one in four of the companies surveyed.

Cybersecurity measures to protect the business premises against attacks



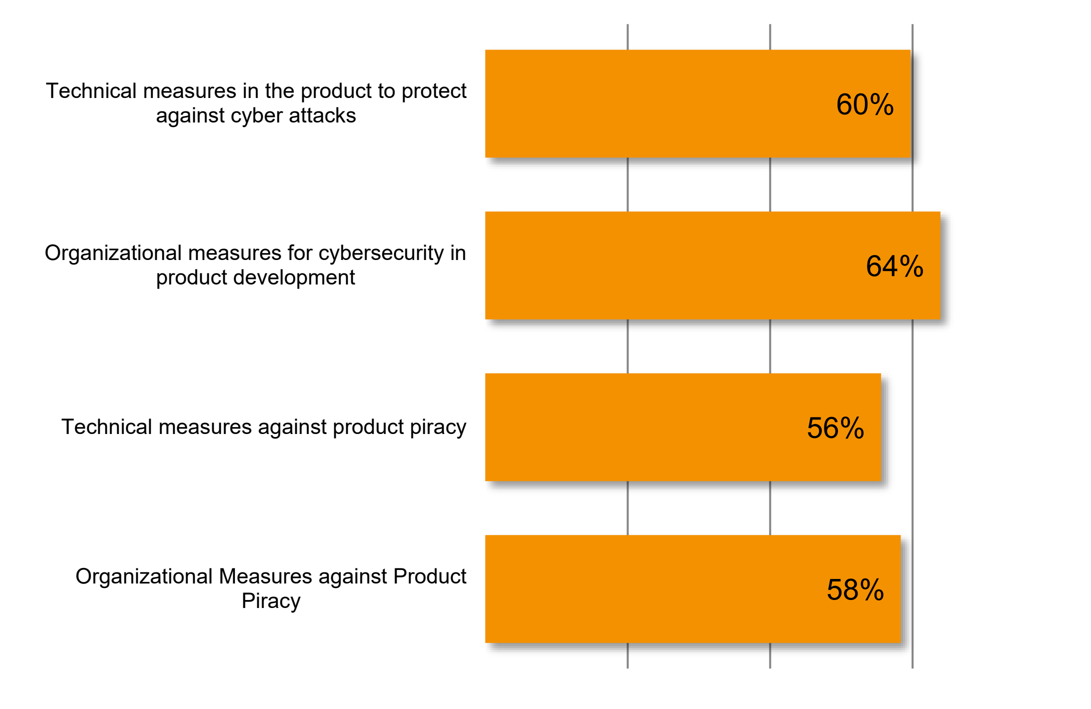
Cybersecurity measures taken to secure the business premises. N=101

In addition to the measures for safeguarding the operating site, we also asked about measures for product safety in product development.

On the one hand, this shows that protection against cyber attacks is slightly more important to the companies surveyed than taking measures against product piracy. Secondly, it can be seen that organisational measures are implemented slightly more frequently than technical measures in both cases.

However, due to the sample size of 72, the individual differences are not significant. **Nevertheless, it is clear that around three out of five companies take product protection measures.**

Product protection measures in product development



© VDMA 2024

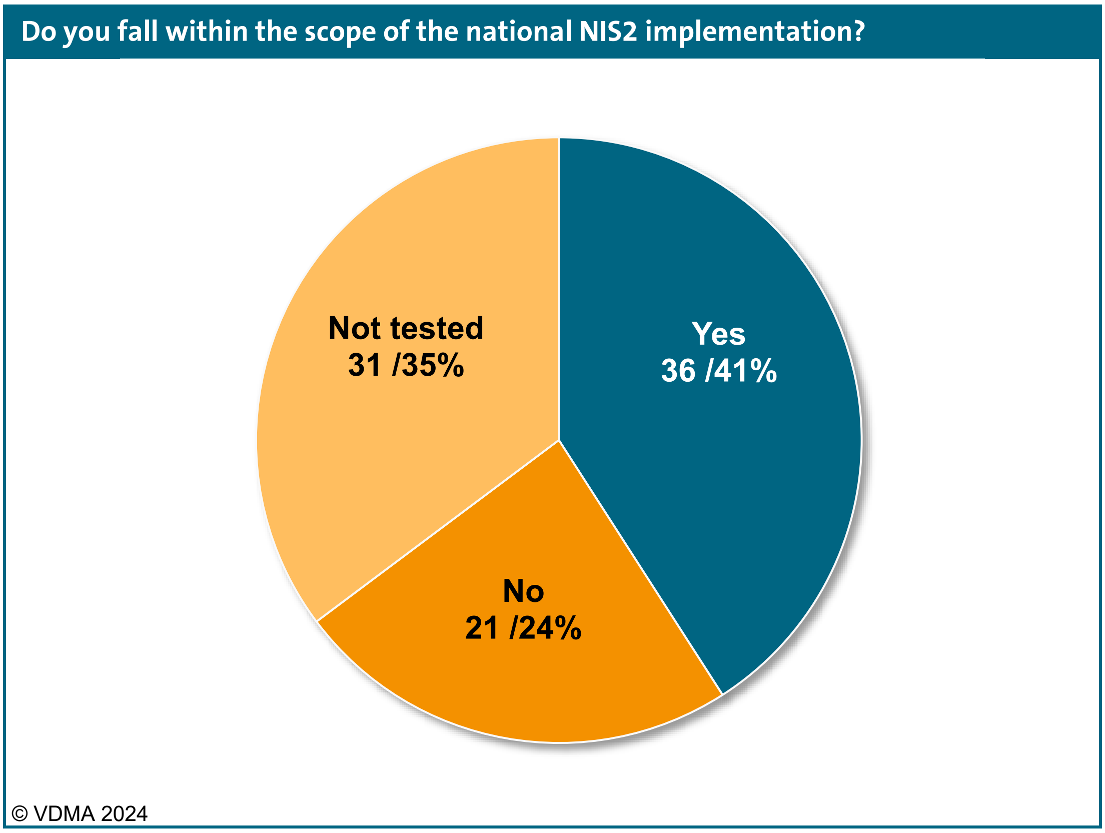
Proportion of companies that take product protection measures in product development. N=72

12 Standards in industrial security

The Network and Information Systems Directive 2 (NIS2) is an EU directive that came into force on 16 January 2023 and must be transposed into national law in the member states, in Germany through the NIS2- Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG) . NIS2 extends the scope of application from classic critical infrastructure (KRITIS) to other important facilities. Mechanical engineering has been included in the scope of application for other critical sectors and is therefore directly covered by NIS2.
We therefore asked which of our member companies fall within the scope of national NIS2 implementation.

Around a third (35 per cent) of the companies surveyed stated that they had not yet checked whether they fall within the scope of application. **Of those companies that have already carried out the review, almost two thirds (63 per cent) fall within the scope of application.**

The VDMA itself analyzed the companies with a negative test result again and found that only six of the 21 companies actually do not fall within the scope of NIS2 implementation.
The 15 companies that do not consider themselves to be within the scope of NIS2 were contacted by the VDMA and explicitly informed that they were affected. **Taking into account the cross-check by the VDMA, this results in a NIS2 impact of approx. 90 per cent**. 71 per cent of the companies with a negative assessment came to an incorrect conclusion.



Do you fall within the scope of the national NIS2 implementation?

© VDMA 2024

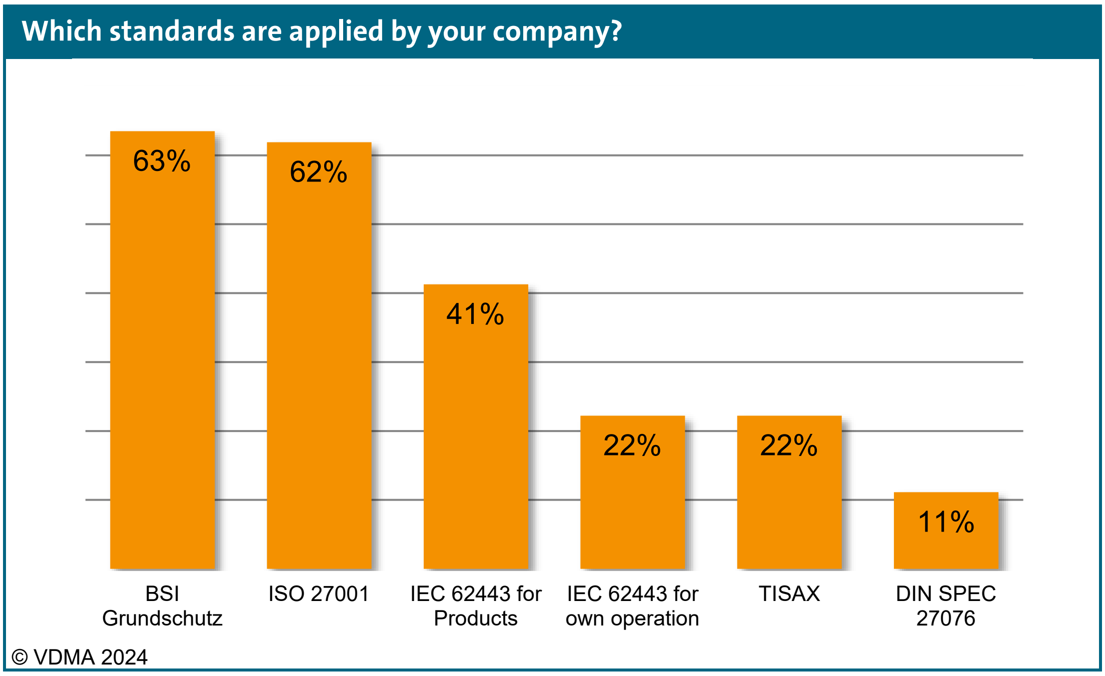
Scope of national NIS2 implementation. N=88

Requirements for industrial security come not only from politics and the national and international legal landscape, but also from technical and organizational standards, some of which are required to be implemented by customers or business partners.

In response to our question, the companies stated that the “**IT-Grundschutz” from the Federal Office for Information Security and the ISO 27001 standard are the most widespread standards, which are used by almost two out of three companies.**

The IEC 62443 standard, applied to the company's own products, follows in third place with 41 per cent.

IEC 62443, applied to the company's own operations, and TISAX, a widespread standard in the automotive industry, are implemented by just over one in five of the companies surveyed (22 per cent each).

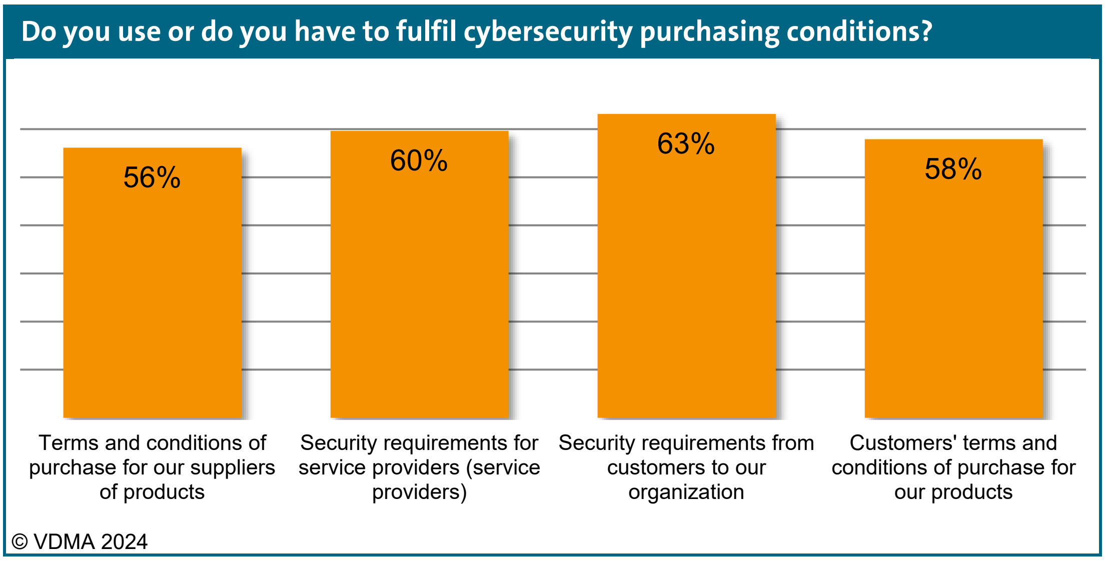


Implementation of relevant standards in the field of industrial security. N=63

The fact that compliance with standards is demanded by both customers and business partners is shown by the feedback from companies in response to our question as to whether they demand conditions and specifications from their suppliers or service providers, or whether they themselves receive specifications from customers for their organization or products.

In all categories, these questions were answered in the affirmative by around 60 per cent of companies, which corresponds well with the implementation of BSI basic protection and the ISO 27001 standard.

Do you use or do you have to fulfil cybersecurity purchasing conditions?



© VDMA 2024

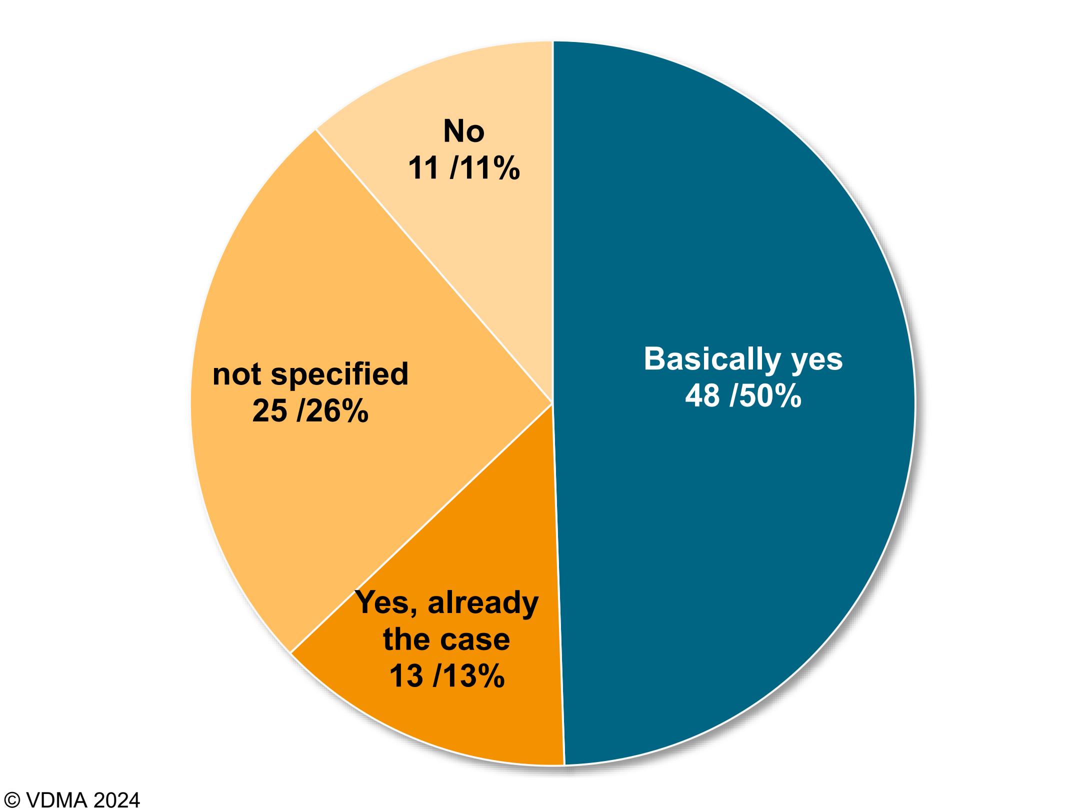
Specifications on purchasing conditions in the area of industrial security. N=57

13 Alliance for cybersecurity

In the event of a cyberattack, in addition to their own capacities or service providers, companies could also fall back on alliances or alliances formed in advance, for example to support each other with appropriately trained IT personnel.
As part of the study, we therefore asked specifically about the willingness to get involved in such a local or regional cyber alliance.

The vast majority of the companies surveyed would either be willing to do so in principle (50 per cent) or are already active in a cyber alliance (13 per cent). In contrast, only one in ten companies currently rules out such involvement.

Would you get involved in a cyber alliance?



Opinion on involvement in a local or regional cyber alliance. N=97

14 The VDMA acts

Product piracy

The VDMA's activities against product piracy have developed continuously since they began with this study in 2003. While the initial focus was on informing and sensitizing politicians and society, the current measures concentrate on improving law enforcement and the exchange between affected companies.

In 2010, the VDMA established the Product and Expertise Protection Working Group (AG Protect-ing) to further develop the product protection innovations researched in the mechanical engineering sector. Following its successful work, the working group was merged into the **"Industrial Property Protection" working group** in 2016.
The VDMA working group "Industrial Property Protection" connects and informs interested VDMA member companies about the latest developments in industrial property protection and offers a confidential space for exchanging experiences on legal, technical and organizational activities.

Industrial Security

The VDMA Informatics department has been responsible for the broad field of information security since 2006. The foundation of the "Information Security" working group in 2008 still forms the basis and was supplemented in 2012 by the exchange on security in production and automation (now "Industrial Security").
The latest activity is the "NIS2" working group founded in 2023, in which small and medium-sized companies work together to develop their understanding of the NIS2 directive.

In 2019, the "Industrial Security" working group started the essential work in the important area of "Supply Chain Security". Cybersecurity in the supply chain only works if everyone involved makes their contribution and if the requirements and measures are harmonized. This requires cross-association cooperation with the BSI, the suppliers in the ZVEI and bitkom as well as with the customer groups.

The standardized questionnaires for the specific procurement of machines, a general supplier questionnaire or the cooperation in the VDMA working groups as well as the mapping from ISO27001 to NIS2 are a successful reflection of this.

Legal protective measures

For most companies, legal protection forms the basis in the fight against product piracy. We inform our member companies in brochures and presentations about legal options for protecting innovations and provide sample contracts. In personal meetings, we discuss problem cases and help with the registration of property rights and contractual formulations.

Our co-operation with law firms in the most important foreign markets enables us to provide fast and competent advice locally.

15 Further training programmes

As a training academy, the „VDMA Maschinenbau-Institut, MBI“ offers a wide range of training programmes on the subject of industrial security that are not restricted to VDMA members.

ISA qualification programme to become an IEC 62443 Cybersecurity Expert

The number of security incidents is also constantly increasing in mechanical engineering. This is why the MBI, in cooperation with **ISA Europe** and the **Fraunhofer IOSB, is offering** the official qualification programme for the training of "**Cybersecurity Experts**".
In four consecutive seminars, the ISA training content is supplemented by specific aspects of networked machines and systems. For advanced users, there is the 5-day compact course leading directly to the "Cybersecurity Expert" qualification.

Security by design for machines and systems

Thinking about cybersecurity as early as the development process - that is the starting point of Security by Design. The seminar was developed in collaboration with **Fraunhofer IEM** and **Fraunhofer IOSB** specifically for mechanical engineering and explains how the principles must be applied in practice. It is based on IEC 62443 and the VDMA specifications on supply chain security.

Protect production facilities against cyber threats

This seminar enables operators of industrial production systems to protect them against cyber attacks and other threats. It will teach which measures should be taken in accordance with the IEC 62443 series of standards.

Cyber crisis exercise for mechanical engineering

This seminar uses a ransomware scenario to practise the worst-case scenario in the event of a cyber attack and provides a blueprint for solid crisis management.
The legal requirement for adequate crisis management awaits companies with the implementation of the NIS 2 directive. Companies in the mechanical and plant engineering sector that will have to fulfil cybersecurity requirements in the future can use the blueprint to implement the obligations - an essential building block for future NIS 2 compliance.

Further information is available at:
https://www.maschinenbau-institut.de/themen/digitalisierung-innovation/

16 Imprint

VDMA
Lyoner Str. 18
60528 Frankfurt am Main
E-mail: kommunikation@vdma.org
Internet: www.vdma.org

Year of publication
2024

Picture credits
VDMA

Graphics
VDMA

VDMA
Lyoner Str. 18
60528 Frankfurt am Main

Phone +49 69 6603-0

E-Mail:
kommunikation@vdma.org
www.vdma.org

www.vdma.org