Allianz Trade

TREND REPORT 2023

Yearly fraud survey in the Netherlands and Belgium

How many businesses and organisations were victims of fraud?

Which fraud is most common?

What measures are companies taking?

How big are the damages?

Who are the typical fraudsters?

What are the main misconceptions about fraud?

1. Introduction

Allianz Trade is an expert on fraud. Following on from our fraud surveys in other countries, a fraud survey was conducted for the first time in the Netherlands and Belgium in 2022. We conducted this survey again in 2023. This annual survey shows the current state of affairs in the field of fraud. The survey focuses on various forms of fraud, the damage that companies suffer and the measures that are taken. This gives a picture of the resilience and vulnerability of the business community in the Netherlands and Belgium. Because the survey takes place annually, it is possible to register current fraud developments. In addition, the survey also aims to provide insight into the insurance needs of companies in the field of fraud.

2. Accountability

Commissioned by Allianz Trade, the survey was carried out by MetrixLab in the spring of 2023. A total of 355 companies and organisations participated in this survey (200 in the Netherlands, 155 in Belgium). Forty-eight per cent are B2B businesses, 35% B2C and 17% government & non-profit. All businesses and organisations have an annual turnover of at least €10 million and have at least 50 employees. For the survey, the participating companies answered an online questionnaire.

The roles and functions of the respondents are very diverse: from CEOs, CFOs to controllers and HR managers. They are all fully or partially responsible for risk management and coverage in their company. The participating companies represent a wide range of industries: from transport to retail, from metal to textile industry. The top 5 industries that are most represented are as follows: financial services 17%, ICT 17%, government 12%, construction/installation 9% and business services 9%.

Allianz Trade
's-Hertogenbosch / Brussels, june 2023

3. The results

The survey shows that 79% of companies have recently experienced internal or external fraud attempts. Of this 79%, a majority actually suffered damage.

Even though a large majority confirms that they have been victims of fraud and suffered damage, 84% still indicate that they consider themselves to be sufficiently protected. There seems to be an unjustified sense of security here. People fell well protected but they are not well protected. What plays a role here is that many companies prefer not to wash their dirty laundry in public.

Of all companies that have experienced internal and external fraud attempts, a majority actually suffered damage.

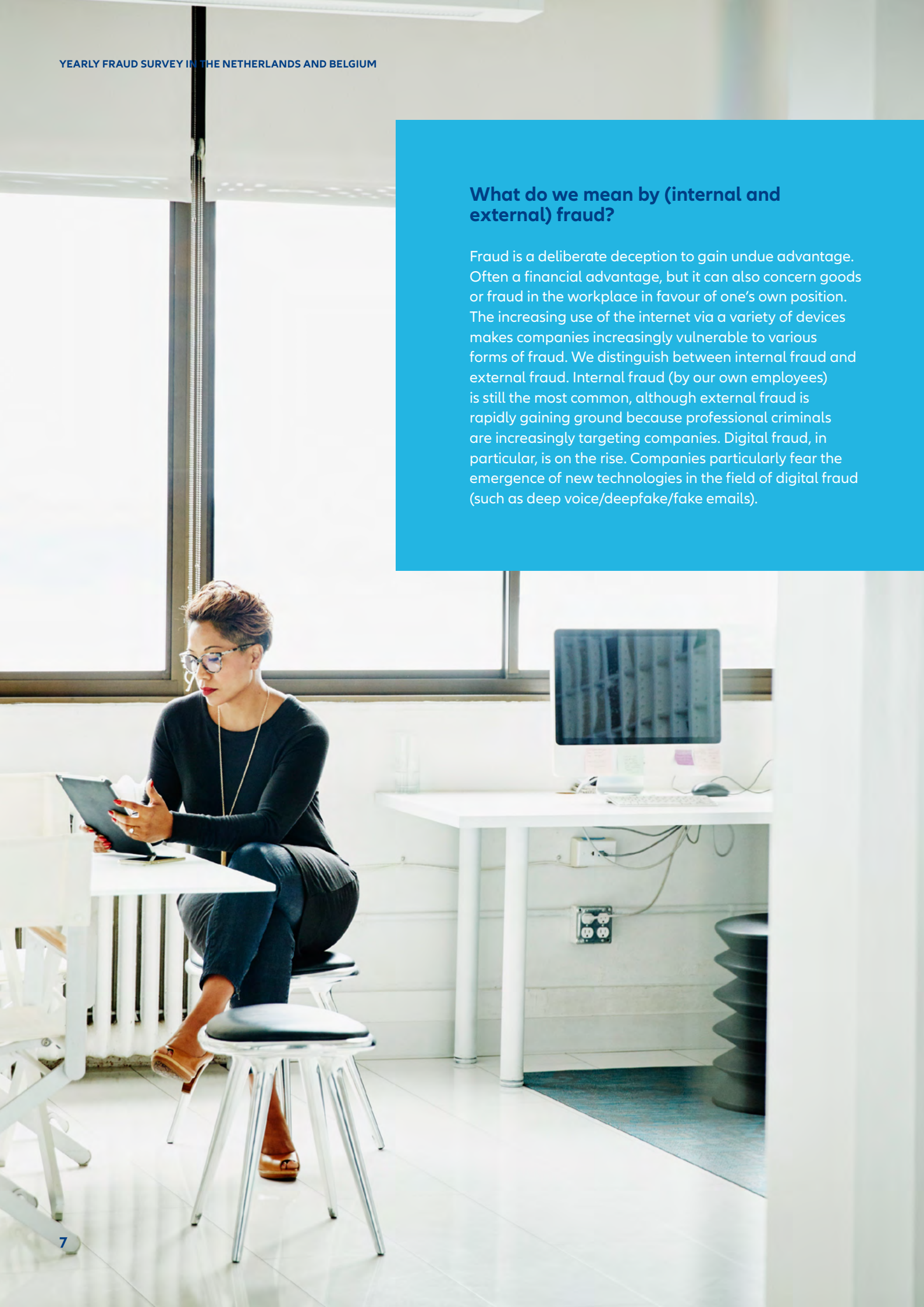
The fear of losing (online) data in particular

What are companies most concerned about when dealing with fraud and scams? A large majority mainly fears the loss of (online) data and other forms of cybercrime:

- 'One of my biggest concerns is that hackers could gain access to the company database.'
- 'Damage to reputation and its financial consequences.'
- 'Cybercrime.'
- 'Lack of knowledge of employees. Too much trust.'
- 'Phishing emails, scams, employees who commit fraud.'
- 'Theft of property and/or intellectual property.'
- 'Computer hacking requiring a ransom.'

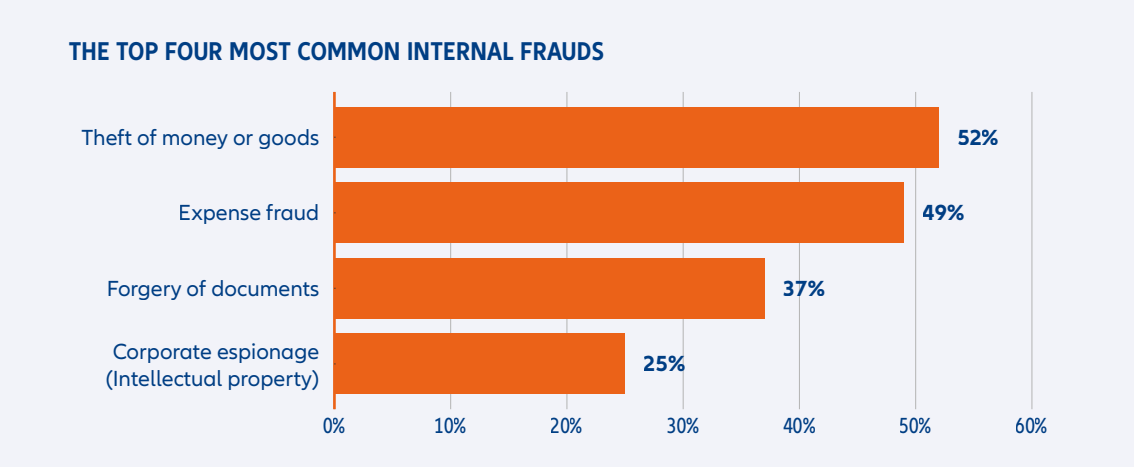
What do we mean by (internal and external) fraud?

Fraud is a deliberate deception to gain undue advantage. Often a financial advantage, but it can also concern goods or fraud in the workplace in favour of one's own position. The increasing use of the internet via a variety of devices makes companies increasingly vulnerable to various forms of fraud. We distinguish between internal fraud and external fraud. Internal fraud (by our own employees) is still the most common, although external fraud is rapidly gaining ground because professional criminals are increasingly targeting companies. Digital fraud, in particular, is on the rise. Companies particularly fear the emergence of new technologies in the field of digital fraud (such as deep voice/deepfake/fake emails).



3.1. Internal Fraud

Although much media pay attention to cybercrime, fraud is most committed by internal employees.



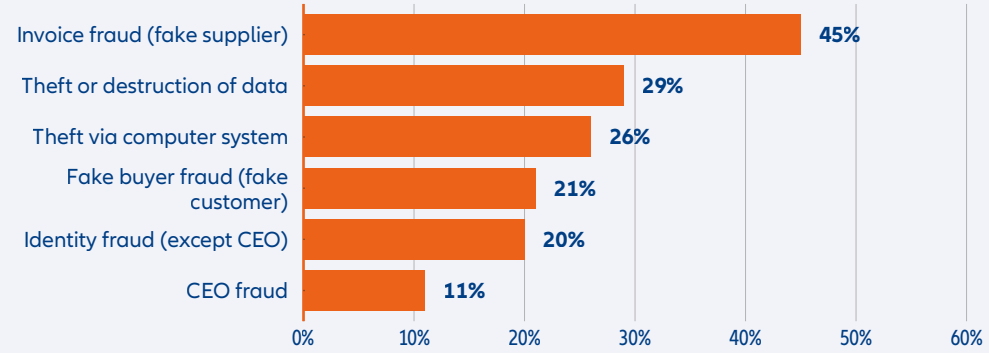
It is notable that expense fraud clearly occurs more in the Netherlands than in Belgium (56% vs 38%)

Internal fraud mainly concerns the theft of money or goods and expense fraud.

3.2. External Fraud

In the case of external fraud, false invoice is far the most common form.

MOST COMMON EXTERNAL FRAUD



Fake buyer fraud
With fake buyer fraud, a scammer pretends to be an (existing) customer. The fake buyer orders goods and has them delivered to a different address (not the customer's real address). The fraudster can also intercept the goods before delivery under false pretences (e.g. via the carrier).

Fake supplier fraud
With fake supplier fraud, the scammer pretends to have supplied goods/ services (which is not the case) and sends an invoice for this. This also includes advance payment fraud in which the fraudster asks for payment in advance. The false invoices can hardly be distinguished from real invoices. Often only the bank account number (and the name) differ. These false invoices often involve relatively small amounts. The scammer hopes that the false invoice will be handled 'blindly' in the daily hustle and bustle of the administration department.

Identity fraud
With identity fraud criminals pretend to be someone else (for example, as if they are a customer or colleague). Identity fraud clearly occurs more often in the Netherlands than in Belgium (29% vs 8%). If the fraudster pretends to be the CEO, it is called CEO fraud.

Tips to prevent internal and external fraud

1: Make fraud discussable.
Making staff aware is one of the most important measures. By making fraud a topic for discussion internally, employees are less likely to fall for false emails or other disguises.

2: Create an open business culture.
CEO fraud is most successful within highly hierarchical companies. It must be possible for employees to ask their manager questions and to request confirmation of a deviating payment request. The shorter the lines between employees and managers, the less the chance of CEO fraud.

3: Build in check moments.
Build in more check moments in the work and processes. Much misery can be prevented with a healthy dose of suspicion. Consistently check details, such as the address and the names of contact persons/ authorised signatories. When in doubt, verify data with your trusted contacts by phone.

4. Use the four-eyes principle!
Make arrangements for transferring larger amounts with the help of authorization schemes and the four-eyes principle.

3.3. Internal fraudsters: often men who employed for a short time

Internal fraud is committed considerably more often by men than by women (64% vs 20%). They are often men who have been employed for less than five years.

Which departments commit the most fraud?
Finance scores highest with 36%. In second place is Commerce, where it is notable that fraud is committed more often in this department in Belgium than in the Netherlands (34% vs 14%). In third place is Operations with 26%.

Longer employment? Less chance of fraud
The longer men are employed, the less chance of internal fraud. Internal fraudsters are often employed for a relatively short time (1 to 5 years).

In 36% of the cases, the fraudster works in the Finance department

3.4. 15% of fraud damages exceed €200,000

Almost half the fraud damages are between €1 and €50,000. In this category, it is notable that the loss items for internal fraud are often higher than for external fraud.

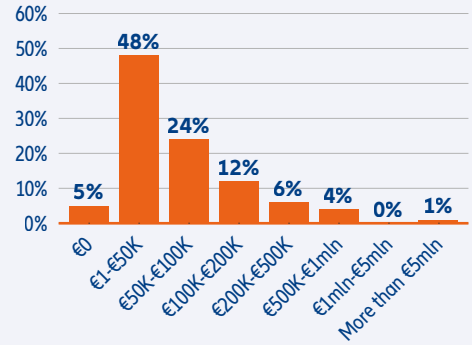
In more than 20% of the fraud cases, damages are between €50,000 and €100,000. 12% are between €100,000 and €200,000. 15% are to more than €2,000,000, of which 4% are between €500,000 and €1,000,000. One per cent are more than €5,000,000.

A fraud insurance covers the major impact of fraud.

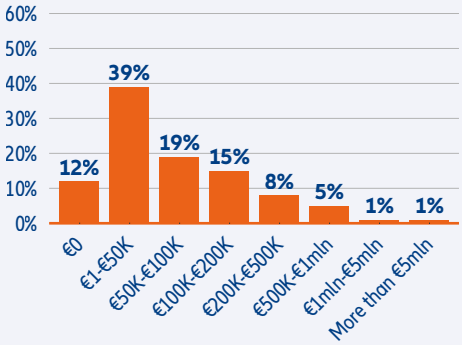
Of all companies that experienced internal or external fraud attempts, a majority actually suffered damage.

DAMAGE SUFFERED

Internal fraud



External fraud



3.5. Fraud: often not reported to the police

Three-quarters of the companies that were confronted with fraud have engaged external partners once or more to stop or deal with fraud. Almost half this group (43%) say they have sometimes approached the police for this. Conversely, this means that 57% of fraud cases are not reported to the police.

Lawyers engaged more often in Belgium
An ICT company is most often called in when there is fraud in an company. It is notable that a law firm is engaged more often in Belgium than in the Netherlands (43% vs 20%). In Belgium, more help is engaged overall (84% vs 68%). Dutch companies more often solve it internally, on their own (in 32% of the cases).

More external help called in than in 2022
Compared to the fraud survey of 2022, businesses and companies tend to engage an external party more quickly. In the previous survey, 44% said they sometimes engage external help. That percentage is now 75%.

One in four companies handles fraud internally.

3.6. What do companies do to prevent fraud?

What methods do companies use to prevent internal and external fraud? Measures mentioned most often include increasing fraud awareness among employees, extra control from the administrative organisation and screening of employees. If we look at other measures, it is notable that Dutch companies use two-factor authentication and the four-eyes principle.

Security tests
In Belgium, companies perform penetration tests more often to assess the security of their network/system. They also more often deploy ' red teaming' campaigns in which they have an external fraud specialist or hacker test in practice how easy/difficult it is to enter the company and break into their systems.

Companies with more than 1,000 employees make relatively more use of workshops and tools to increase employee awareness.

It is mainly large companies that take action to prevent and detect fraud.

3.7. Companies see an increase in digital vulnerability in particular

The majority of companies see fraud as an increasing risk in general. They cite digitisation, automation and new technology as the causes. But here too, people see the risk more for their 'neighbour' than for themselves (see beginning of Chapter 3). Particularly in smaller companies, it is easy to think 'it won't happen to me' or 'I know my employees' or 'our firewall is good enough'. Three-quarters of large companies (more than 5,000 FTE) see fraud as an increasing risk for themselves.

- 'Digitisation creates more opportunities to commit fraud.'
- 'I think that in the growing online market and especially the lack of knowledge of this among the older generations, there is an increasing risk of fraud and phishing.'
- 'There are a lot of direct emails to employees, each with links and access points to our network.'
- 'People are getting smarter and technology is also becoming more advanced for criminals.'
- 'Everything is going digital and that is good, but very susceptible to fraud.'
- 'IT and automation make work easier, but make fraud easier too. The flow of data is becoming so large that it is difficult to check it.'

3.8. More companies perform fraud risk analysis

The fact that businesses perceive fraud as an increasing risk can also be deduced from the number of fraud risk analyses that companies have carried out. 64% of companies say they do that (in last year's survey that percentage was 37%). Companies engage parties such as ICT businesses, internal teams, external consultancy firms and accountancy firms for this purpose.

When asked why businesses did not carry out a fraud risk analysis, we hear answers such as:

- 'Urgency was not high enough, because it is preventive.
- 'We see no added value. The frauds we have encountered are not stopped by this type of analysis.'
- 'No financial resources.'
- 'We do it internally through our own ICT and audit department.'

Fraud risk analyzes are mainly focused on digital fraud and financial administration.


MATCHING
MATCHED
ID 96421654174
Hashcode RTY4 1DSE BTW4 ZWQ1
##READING .....
/:FSGKLJJ33 13244%#S 1315FHRS A3124#31D14412D
/:31245FFR44 %#3110 0134
/:AW3232FGG8##3214 FGTG;J1134
/:32132144HSD %%PKKKJ 13444881 ZAZ3
/:JSFE1134 841%S11 #32144
/:JUDJ434% GLK##::AA7 S4777431145 8SFR 1
/:OO1001 ASW475#7414 SSFE% FGJJJ1154 314845
/:SDW31115 1AS5WD11 S2QQQ11 S2213%A #ZS411
ACCESS GRANTED
##READING .....
/:FSGKLJJ33 13244%#S 1315FHRS A3124#31D14412D
/:31245FFR44 %#3110 0134
/:AW3232FGG8##3214 FGTG;J1134
/:32132144HSD %%PKKKJ 13444881 ZAZ3
/:JSFE1134 841%S11 #32144
/:JUDJ434% GLK##::AA7 S4777431145 8SFR 1
/:OO1001 ASW475#7414 SSFE% FGJJJ1154 314845
/:SDW31115 1AS5WD11 S2QQQ11 S2213%A #ZS411

3.9. Homeworking: greater risk of fraud

The coronavirus crisis is now almost two years behind us. Working from home has become commonplace. And according to the respondents, this has increased the risk of fraud. 50% of companies answer 'yes' to the question whether employees working from home has increased the risk of internal and external fraud for the company. Last year that percentage was still 34%.

More sensitive to fraudsters

It does not concern only internal fraud, for example time fraud/expenses fraud (less control possible when working from home), but also external fraud. Employees who work 'isolated' at home are more susceptible to fraudsters. At work, when in doubt, it is easier to consult a colleague who works in the same room.

Why does working from home increase the risk of fraud?

- 'Any way you look at it, there is simply less control over what people do at home. So, there is a higher risk of fraud.'
- 'Security at home is not as good as at the office.'
- 'At that moment you sometimes miss an extra check if, for example, someone is in doubt, you cannot take a look. In addition, more and more is now happening digitally, which also entails an extra risk."
- 'There is less overview of employees, and they therefore have a greater chance of committing fraud.'
- 'We work according to hourly wages, it is impossible to check whether, for example, the actual contractual hours are being worked.'

50% of companies say homeworking increases the risk of internal and external fraud.

Many companies are taking measures in the digital sphere

Of all companies that see working from home as an increased risk (50%), 68% have taken measures. This mainly concerns measures in the digital sphere.

What has been adapted?

- 'Two-factor authentication.'
- 'VPN.'
- 'Firewalls and antivirus.'
- 'We have blocked quite a few websites. Https is a must and configured.'
- 'Update antivirus and email protection regularly.'

Companies that do not take measures say:

- 'It is not seen as an increased risk.'
- 'No financial resources.'
- 'It was not necessary.'
- 'We need to look further into it.'
- 'Reliable employees in the business.'

3.10. Next three years: more investment in fraud prevention

Almost 30% of the companies say they will invest more to limit the risk of fraud. These companies invest more money in security audits of their IT systems and in training to increase fraud awareness among employees.

Top five investments
IThe top five of investments to limit the damage caused by fraud also includes taking out insurance. It is notable that 32% of the companies in Belgium opt for this, 16% in the Netherlands.

More and more companies have emergency plans
In 2022, 33% of companies said they had a emergency plan in place in case fraud came to light. That percentage has grown to 58% in one year.

58% have an emergency plan in case of fraud.

3.11. Many misunderstandings about the way of insuring against fraud

49% of the companies think they have covered all damage due to fraud with insurance. That is based on an erroneous assumption. For example, there are companies that assume that a business liability insurance offers sufficient cover against fraud or that credit insurance offers solace. That is incorrect. There are also many misunderstandings about the coverage of fraud insurance and cyber insurance.

Cyber insurance and fraud insurance complement each other

It is often thought that cyber insurance protects against all digital fraud. This is not the case. Take the damage caused by a ghost invoice that a fraudster sends by email; for example, it is not covered by cyber insurance. Conversely, fraud insurance does not cover the ransom demanded to decrypt your systems and make them usable again.

Cyber insurance

A cyber insurance protects companies against damage caused by a cyberattack and against liability for damage to third parties. Think of damage due to an invasion of their privacy if data is stolen, damage if confidentiality is violated due to a hack, damage due to costs due to stolen data, damage due to loss of turnover because a company is not operational for a certain period of time, or damage due to cyber extortion and costs of software or data recovery.

Fraud insurance

A fraud insurance protects companies against damage caused by fraudulent employees, damage caused by criminals posing as suppliers or buyers and thus unjustly embezzling goods or funds from companies. Also, criminals can impersonate employees or even the director (CEO fraud); damages resulting from this are also covered by fraud insurance. Also, the costs that companies incur to repair systems or limit reputational damage.

Almost half of all companies wrongly believe that cyber insurance provides sufficient protection against digital fraud. As a final element of their risk prevention, businesses can take out fraud insurance in addition to cyber insurance, credit insurance and business liability insurance in case preventive measures prove to be insufficient.

More Belgian companies plan to take out insurance than Dutch companies (35% vs 25%).

Fraud insurance versus cyber insurance

The table below shows the possible coverage of fraud and cyber insurance. This overview serves to broadly show the difference between the two types of insurance. Conditions differ per insurer. No rights can therefore be derived from this overview, always check the conditions of the insurance.

Fraud insurance	Cyber insurance
• (Identity) fraud, scam, forgery, theft by internal employees. • (Identity) fraud, scam, forgery, theft by third parties. Examples: CEO Fraud, Social Engineering, Deepfake/Deep Voice, Invoice Fraud, Fake Buyer Fraud, Payment Stream Redirection. But also theft of passwords or redirecting to other websites in case of fraud. • Costs (in case of fraud): repair/cleaning of the IT systems, telephone hacking, rescue costs, costs of reputation damage, legal costs, contractual fines and a provisional payment.	• Destroying/shutting down IT systems. • wRepair costs/restoration of the systems. • Business loss due to a cyber incident (usually limited at 180 days). • Damage for liability of stealing data (breach of privacy/confidentiality), costs of internal investigation. • Compensation for payment of ransom/ digital extortion. • Cyber theft (usually capped to, for example, EUR 50,000). • Support by IT specialists in case of a hack and legal/forensic support.

Business liability insurance

According to the law, directors must do their utmost to limit and prevent risks. The same applies to the fraud risk. Has enough been done about that? If not, directors can be held liable if the fraud leads to bankruptcy, for example.

The survey shows that 48% have taken out a business liability insurance. 29% indicate that they want to do this.

Business liability insurers are increasingly requiring companies to also take out fraud insurance. Without this insurance, they no longer cover the entire directors' liability risk.

Conclusions

1 There is a false sense of protection and security around fraud. 84% consider themselves sufficiently protected against fraud and scams. People feel protected, but in practice 79% of companies experienced internal or external fraud attempts. A majority of them also suffer damage.

2 The biggest concerns of companies with regard to fraud and scams are the loss of (online) data and other forms of cybercrime.

3 Three-quarters of the companies have used an external partner to detect or handle fraud/scams at least once. In the majority of fraud cases, companies succeed in detecting or handling it internally.

4 Internal fraud is committed considerably more often by men than by women (64% vs 20%). They are often men who have been employed for less than five years.

5 15% of fraud damages exceed €200,000. Almost half the fraud damages are between €1 and €50,000. In this category with the 'lowest' damages, it is notable that the losses of internal fraud are often higher than for external fraud (48% vs 39%).

6 Fraud is often not reported to the police. Of the companies dealing with fraud, 57% do not report this to the police.

7 Risk of fraud due to homeworking has increased. 50% of companies answer 'yes' to the question whether employees working from home has increased the risk of internal and external fraud for the company. Last year that percentage was still 34%.

8 Almost 30% of companies say they will invest more to limit the risk of fraud. The most popular investments are IT security audits and raising internal awareness. Furthermore, more than half the companies already have an emergency plan.

9 There are many misunderstandings about insurance that covers the damage caused by fraud. Many companies mistakenly believe that they are covered for all fraud damages (from theft to cybercrime.

Do you want to know more about our solutions of trade credit insurance, guarantee or fraud insurance? Contact our team. Our experts will be glad to help you.

+32 (0)2 790 24 15

contact.belux@allianz-trade.com

www.allianz-trade.be