Checkmate through AI? White-collar crime and strategies to counter it

How criminals are getting more professional than ever in their scams and what moves companies can make to protect themselves.

ALLIANZ-TRADE.DE

Checkmate through AI?

Just imagine, you step onto a chessboard where the chessmen are not wooden figures, but consist of code. And your opponents are not just human beings but machines which act with the speed and precision of a supercomputer. Welcome to the new era of AI-supported white-collar crime, where the borders between reality and deception are rapidly becoming blurred.

On the following pages we will take you on a journey through the newest developments in the criminal world, which are fuelled by AI tools. Artificial intelligence brings enormous efficiency gains for companies – but it is a double-edged sword. For at the same time, it enables criminals to strike with unprecedented sophistication and efficiency without them necessarily having specialist expertise. "Hacking as a service", together with deepfake tools, is one of the products most commonly found on the well-stocked shelves of the darknet.

The numbers sound alarming: according to the World Economic Forum (WEF),[1] the global increase in trade in deepfake tools on the darknet from the beginning of 2023 till 2024 rose, believe it or not, by 223%. As a result, cybersecurity experts registered an explosive rise in voice-phishing attempts.[2] Criminals try with so-called "vishing" to infiltrate IT systems and to harvest employees' access data, for instance via fake calls to the IT help desk.

But spoofed invoices too, thanks to AI, are almost impossible to distinguish from the original today, and losses through identity fraud, both as "fake president" scams and buyer fraud, are also on the rise according to Allianz Trade loss statistics.

Social engineering and deepfakes are some of the sharpest weapons in the fraudsters' arsenal, who plan their moves with the precision of a chess grandmaster. That is why we will not only deal with the various types of fraud in the following pages, but also with how companies can recognize and counter these highly professional attacks, so as not to suddenly find themselves in checkmate.

TABLE OF CONTENTS

[1] World Economic Forum Global Cybersecurity Outlook 2025
[2] CrowdStrike Global Threat Report 2025

2.8 billion euros

That is how high losses from white-collar cime were in Germany in 2024. A total of 61,358 cases were registered – a plus of 58 %r

Source:
Bundeslagebild Wirtschaftskriminalität 2024

223 %

That is the extent of the worldwide growth in the trade in deepfake tools in the darkweb between the 1st quarter of 2023 and the 1st quarter of 2024

Source: World Economic Forum Global Cybersecurity Outlook 2025

98 %

of organizations in the DACH Region report a rise in multi-channel attacks leveraging email, messaging apps, social media, and deepfake voice calls.

Source: Sosafe Cybercrime Trends 2025

442 %

This was the worldwide rise in voice-phishing (vishing) attempts between the first and second half-year 2024.

Source:
CrowdStrike Global Threat Report 2025

81 %

of worldwide attacks on compromised systems did not involve malware.

Source:
CrowdStrike Global Threat Report 2025

White-collar crime: AI alert

Losses caused through white-collar crime continue to show a substantial rise. Artificial intelligence can help to make efficiency gains – but it also plays into the criminals' hands. Using generative AI tools, they can refine their social engineering attacks and tailor them precisely to companies and individual employees in them. The majority of attacks do not involve virus infection – people are the weak link and the gateway into the company.

62 %

of companies in Germany see negligence by employees as a contributory factor which encourages e-crime.

Source:
KPMG e-Crime Report 2024

2.7 billion USD

in losses were caused to 21,442 companies worldwide through social engineering; phishing / spoofing doubled.

Source: FBI Crime Report 2024

83 %

of losses registered by the FBI in 2024 were due to e-crime scams.

Source: FBI Crime Report 2024

218 %

rise in losses from fake president scams in 2025.

Source: Allianz Trade loss statistics

59 %

of German companies see their very existence threatened by cyber-attacks. Only 50 % consider their own company very well prepared.

Source: Bitkom Studie Wirtschaftsschutz 2025

57 %

of forged documents are digital.

Source: KPMG Study: Generative AI in IT Forensics and Digital Investigations 2025

From Allianz Trade loss statistics

Fidelity insurance (also name Business Fraud Insurance) from Allianz Trade covers companies against financial losses caused by targeted criminal acts – both by "internal perpetrators" (e.g. employees, temporary workers) and also by external third persons (e.g. criminals or so-called "social engineers"). A glance at the Allianz Trade loss statistics gives some fascinating insights and illustrates current trends.

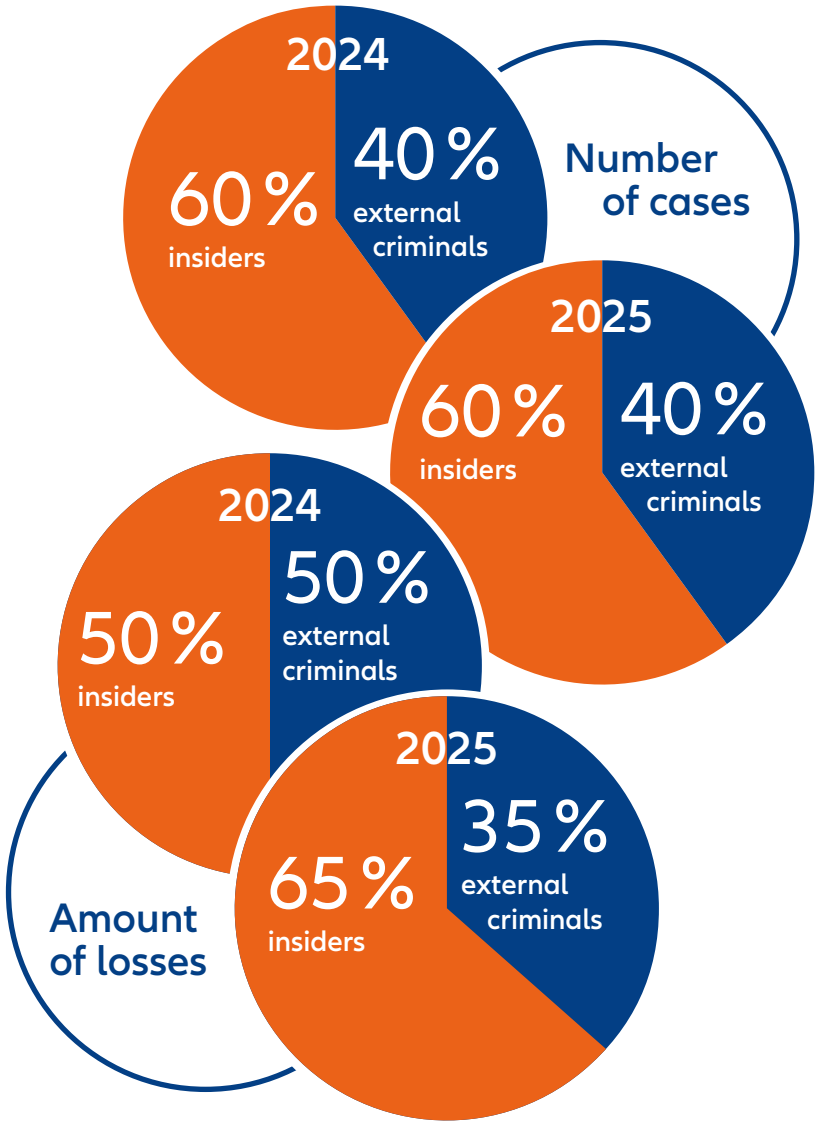
AI alert: White-collar criminals are becoming ever more professional

Artificial intelligence (AI) plays into the hands of white-collar criminals: they are becoming ever more professional, strike ever more often – and cause ever greater financial losses. In particular, it is the external criminals who have substantially increased their activities.

In terms of the loss amounts (amounts of losses reported in euros), insiders and external criminals drew level for the first time (50% each) in 2024.

This trend, however, returned to normal in 2025, and the insiders, with some 65%, bagged the largest amounts –external criminals accounted for 35% of losses in the last year.

It was "insiders", however, i.e., a company's own employees, who caused not only the highest, but also most of the losses in 2025. This truth, uncomfortable for companies and frequently underestimated, thus remains the reality: both in 2024 and in 2025, insiders were responsible for some 60% of reported losses in each case, external criminals for "only" 40%.



Source: Allianz Trade loss statistics

The art of manipulation: Social engineering still on the rise

Social engineering refers to scams in which the perpetrators manipulate people. In particular, we are talking here about payment and buyer fraud as well as the so-called fake president scam, where the criminals masquerade as the boss of a company (therefore also known as the Fake CEO scam) and instruct employees to remit large sums onto fraudulent accounts for alleged business transactions.

These types of fraud accounted for about half (55%) of the external cases reported to Allianz Trade in 2025 and some 78% of the loss volume involved. Their average share in recent years stood at about 50% of cases and some 44% of the loss volume.

A cat-and-mouse game between attackers and defence mechanisms

The "people-hackers" are increasingly refining their techniques of manipulation, also with the help of AI tools. The trade in deepfake tools in the darknet is booming[3]. Companies try to adapt their defence mechanisms as fast as they can – but it remains a cat-and-mouse game in the arms race between scam tactics and defence mechanisms (see also the interview on p. 9), which is reflected in the numbers:

2023 initially marked a negative record in the frequency of social engineering scams. There was a short breather in 2024 at a still high level: numbers of cases declined by 20%. Nevertheless, loss amounts still went up by 15%.

[3] World Economic Forum Global Cybersecurity Outlook 2025. The worldwide growth in trade in deepfake tools in the darknet rose by 223 % between the 1st quarter of 2023 and the 1st quarter of 2024.

Loss amounts hit a new record high in 2025

The criminals took the lead again in 2025 and hit a new record high. The amount of losses reported in social engineering scams shot up by 60%, largely driven by major losses in fake president and buyer (fake identity) fraud – a type of scam which, while it had caused a large number of losses in previous years, tended to cause smaller losses.

The case numbers of all social engineering scams were also up by 13% year-on-year in 2025. Buyer (fake identity) fraud, in particular, in which goods streams are diverted to fake delivery addresses, experienced a real revival in 2025 after a significant reduction in the year before, and replaced payment fraud as the favourite scam of social engineers.

+ 13 %
Increase in numbers of social engineering scams 2025 v. 2024

+ 60 %
Rise in loss amounts 2025 v. 2024

Source: Allianz Trade loss statistics

Perfection through AI leads to record losses in "fake president" fraud

Despite its great familiarity, "fake president" fraud is not going out of fashion. Both in 2024 (-12%) and in 2025 (-13%), although case numbers declined, the sums lost tripled in 2024 (+200%) and even shot up by a further 81% in 2025. That means: when the storm hits, it blows the roof off.

The losses are currently on average in the single-digit millions, while major losses in some cases reach the high two-digit millions, just as when the scam first started at the beginning of the 2010s.

This suggests that, although the attacks have become more selective, thanks to AI they are being carried through extreme professionality, and are therefore often very successful. Criminals often adopt a multi-stage plan and operate as a first step with phishing or voice-phishing, so-called "vishing"[4]. With these techniques, criminals try to infiltrate IT systems and to harvest employees' access data, for instance via fake calls to the IT help desk. In addition they try to obtain internal company information in order to make their subsequent attacks as credible as possible (see also p. 7).

The new favourite: buyer fraud usurps the throne from payment diversion

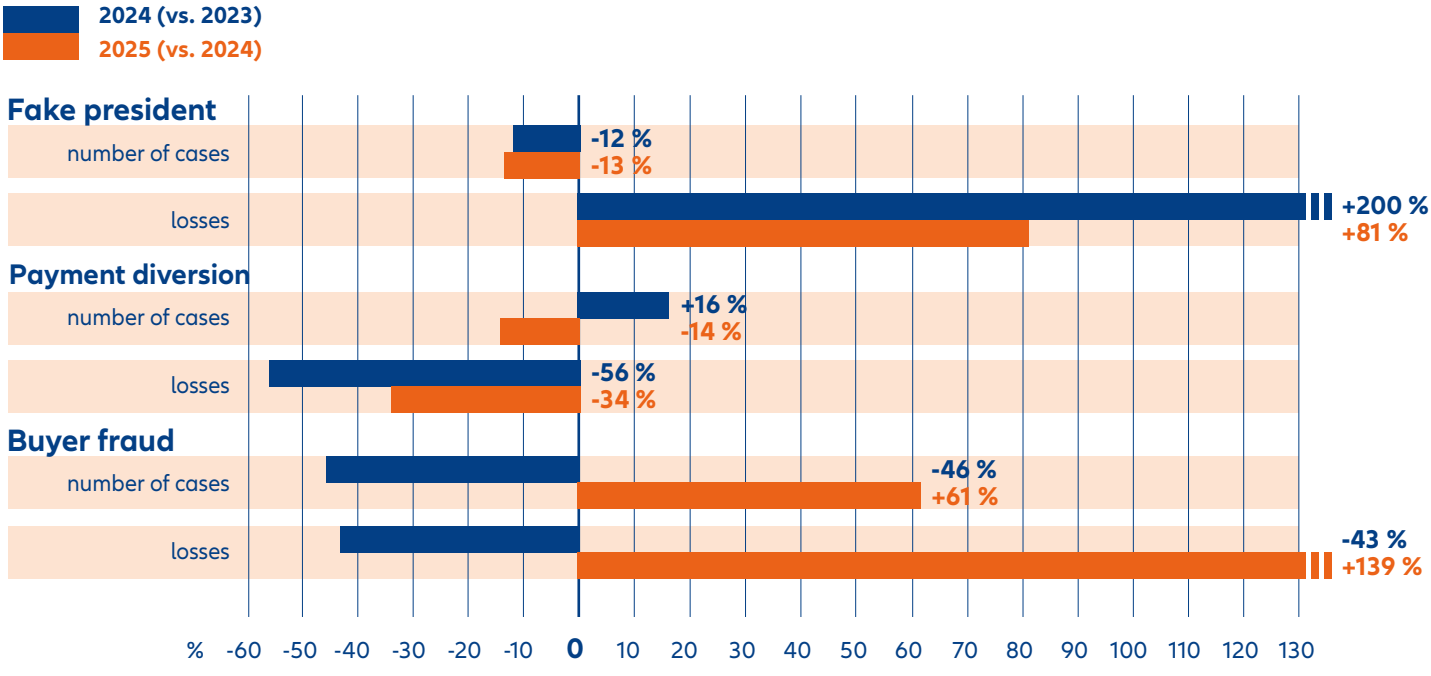
In buyer (fake identity) fraud, there was a steep decline in popularity with attackers in 2024 after a record number of cases in 2023 (-46 %). In 2025, however, there was a revival with rising case numbers (+61 %), in conjunction with a sharp increase in loss amounts (+139 %), driven above all by an unusually high number of major claims.

Buyer fraud posted most cases among the three social engineering scams in 2025 and thus replaced payment diversion, the previous year's frontrunner.

Case numbers in payment diversion went down by 14% in 2025, the volume of losses even decreasing by about a third (-34%) due to the absence of major claims.

[4] CrowdStrike Global Threat Report 2025: The worldwide increase in voice-phishing.) attempts between the first and second half-years in 2024 was 442 %. Criminals try with so-called "vishing" to infiltrate target networks and to harvest employees' access data, often using social engineering techniques. In keeping with this approach, 81% of attacks worldwide on compromised systems did not involve malware, but used stolen access data and legitimate tools which were obtained e.g.. via vishing.

Trends in numbers: change in case numbers and loss amounts



Source: Allianz Trade loss statistics

PHISHING 2026

THE UNDERESTIMATED DANGER AND ITS FATAL FOLLOW-UP CRIMES

Author: Dirk Koch

Dirk Koch is a partner in the law firm ByteLaw Rechtsanwälte in Frankfurt and a Certified Ethical Hacker (CEHv11). He specializes in the field of cyber- and IT-security cybercrime, consultation and reaction in the event of attacks and security loopholes and investigation, IT forensics, data protection and data security.

Phishing has long since developed beyond the crude frauds in the early years of the Internet. Today it resembles more sophisticated chess moves in which cyber-criminals select their targets with surgical precision and try to put their opponents into checkmate in a few moves.

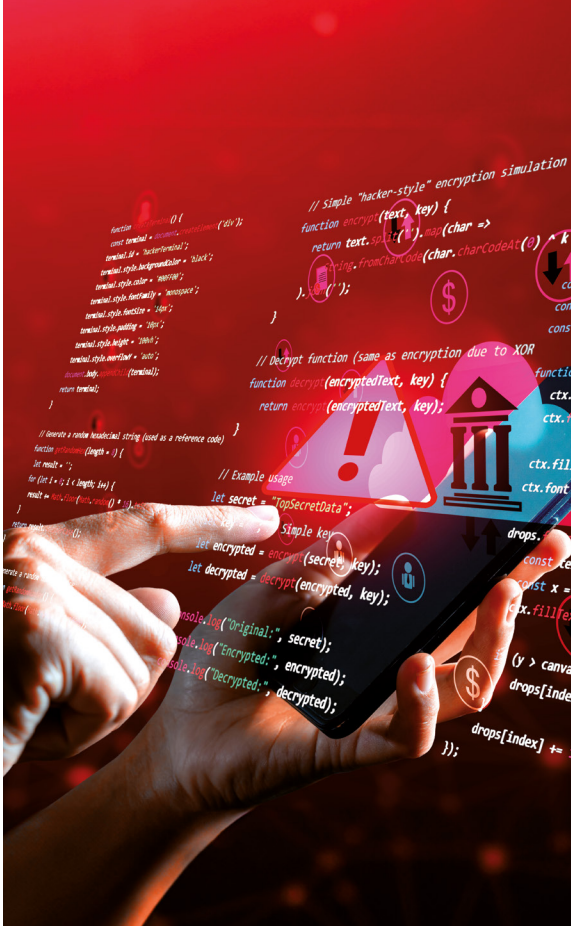
These fraud attacks, often supported by artificial intelligence, pose a threat to companies worldwide. But the greatest danger is not lurking in the first click, but in the insidious crimes which follow it.

After a successful phishing foray, the second phase of the attack begins. Particularly popular here are social engineering scams.

These scams are the underhand traps which snap shut after a successful phishing attack and can push companies over the financial precipice. That is why it is all the more important to realize and understand the current threat level, the technical background and effective defence mechanisms and above all to put them into practice.

The trap snaps shut: phishing and vishing open the floodgates

Phishing and also voice-phishing, so-called "vishing" continue to be the most common entry points for cyber-attacks. Modern phishing emails look deceptively authentic and are a wolf in sheep's clothing. They are flawless in spelling and design, and often come from compromised sender addresses to which the scammers have obtained direct access. The use of AI tools, too, enables them to create deceptively real deepfake phone calls and videos, which can mislead even the most experienced employees.



After the initial successful phishing or vishing attack, the second phase begins: in so-called "business email compromise (BEC)", scammers hijack real company email accounts and manipulate the ongoing communication. In payment diversion the perpetrators alter the bank account data in invoices or payment orders. Without reconfirmation, millions can flow onto the perpetrators' accounts. In the fake president or CEO fraud 2.0, they pressure employees to make remittances immediately by means of deepfake video calls or AI voice calls. A single successful attack of this kind can lead to a loss running into the millions in this way.

Defence strategies: How companies can get on an equal footing

To protect themselves, companies need to adopt both technical and organizational measures.

On the technical side, phishing-resistant multi-factor authentication (e.g. via hardware tokens or passkeys instead of SMS-TAN) as well as email protection via security procedures such as SPF (Sender Policy Framework)[5], DKIM (Domain-keys Identified Mail)[6] and DMARC (Domain-based Message Authentication Reporting and Conformance)[7] are essential. The use of AI-based filters as well as a zero-trust architecture, in which every single access is checked, can help to recognize attacks at an early stage and limit the damage.

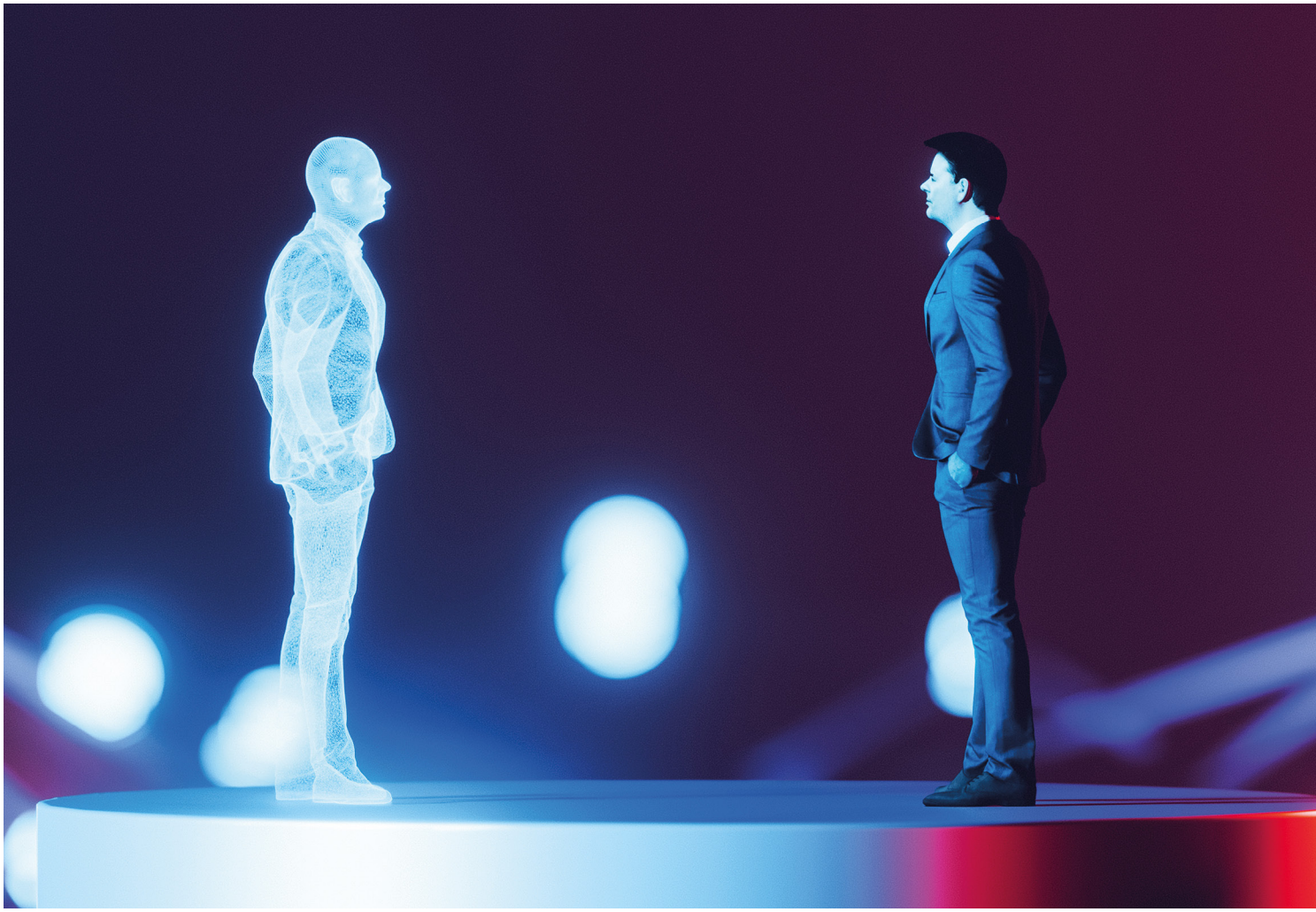
As regards organizational procedures, you should constantly check processes for clearing payments, implement the dual control principle with high payments (and "live it"!) as well as so-called "out of band confirmation", i.e., altering payment data should only be accepted after a checking phone call to the number you already know and which was registered at the initial contact. On top of this, regular awareness-raising programmes to train employees, especially dealing with the newest AI-based scams such phishing, social engineering and deepfakes, are crucial. Technical safeguards provide fundamental baseline protection, which should be supplemented within the organizational framework by awareness-raising measures for the workforce, such as specifically targeted and focused instructions and training courses. Progress in technical solutions is important, yet it is the vigilant awareness of employees which is a decisive factor for overall security.

Watch out! Liability trap: Missing safeguards can have a fatal effect

Companies are legally obliged to manage social engineering risks proactively and to report incidents. The absence of safeguards can be seen as organizational negligence and lead to substantial fines as well as liability claims against the management.

In 2026, phishing is in many places a familiar, albeit severely underestimated danger. At the same time it is not merely an IT problem, but the gateway into a company and thus a strategic risk. It is the one move which can put the king in checkmate. The great danger lies in the subsequent moves after the first click, from manipulated payment processes to deepfake fraud – and, if the worst comes to the worst, checkmate.

[5] SPF (Sender Policy Framework) is an email security standard which protects domains against spoofing by specifying a list of authorized servers (via DNS entry) which may send emails on behalf of the domain; the receiving email servers check this entry to confirm its authenticity and to reduce spam and phishing in this way.
[6] With DKIM (Domain Keys Identified Mail), domain owners can sign emails from their domain automatically. The DKIM signature is a digital signature. Using cryptography, it verifies mathematically that the email really comes from the domain.
[7] DMARC (Domain-based Message Authentication Reporting and Conformance) tells the email server what it should do with an unsuccessful DKIM or SPF; mark the email as spam, deliver the email in spite of the failure or delete the email completely.



INTERVIEW WITH THE EXPERTS

People remain the weakest link – and AI finds the loopholes.

Social engineering scams, in which people are manipulated by criminals, have for many years caused massive financial losses to companies. And there is no end in sight – on the contrary. ChatGPT has changed the world : an innovation which has brought huge efficiency gains, a reduced workload and several new opportunities on the one side, also plays into the hands of criminals on the other – since it opens up a host of new ways for them to simplify their work too.

To illustrate what these are, here is an interview with two Allianz Trade experts **Marie-Christine Kragh,** Global Head of Fidelity and **Tom Alby,** Chief Digital Transformation Officer.

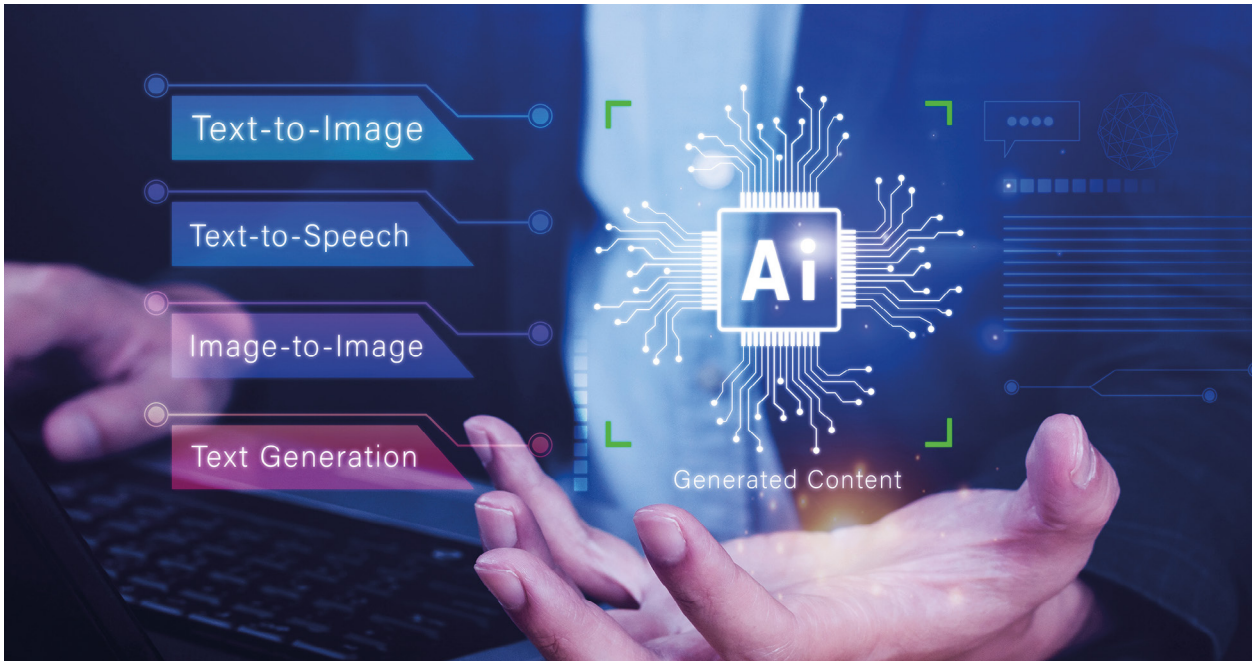
Why has social engineering not gone out of fashion even after so many years?

Marie-Christine Kragh: Because it works by touching us humans in our innermost core, it plays with our emotions. "Well-made" social engineering insinuates itself at the exact point where we have connecting points – for instance, where we feel appreciated, an intrinsic need every one of us has. But pressure can also play a decisive role, or evoking an apparent critical situation. For instance, when the alleged CEO contacts someone, he stresses that he is getting in touch with them because personal reliability is extremely important in this matter and they are someone he trusts implicitly. That triggers an immediate feeling of being something special – and that is when pressure is put on, e.g. with the allusion that strict contractual confidentiality must be kept and speed is of the essence. A company can have the best firewall available, yet it is all but useless faced with an experienced social engineer: people continue to be the weakest link. The triad of time pressure, triggering of emotion and the request to cut corners on standard procedure should set the alarm bells ringing.

Tom Alby: And artificial intelligence helps the fraudsters to zero in on the loopholes and to press the right buttons. With ChatGPT and other large language models, criminals have been handed the technical platform to carry out their attacks on a silver platter. Using them, it is child's play to train AI for their purposes. To take just a simple example: I feed a couple of emails from the CEO into the AI and a few prompts later, I have a text which sounds exactly like the boss: the form of address, the tone and the style fit exactly, and the email appears entirely credible. And it is precisely this apparent authenticity which invalidates the normal processes and rules. With GPT variants such as FraudGPT or WormGPT, criminals can create their own fraud assistant.

And what about voice cloning & co.?

Alby: We are reaching a new stage of evolution there. A few years ago, voice cloning was a technique for absolute specialists and the quality was often doubtful. Today, you virtually only have to press a button and anyone can do it "off the peg" using AI tools which you can get for next to nothing or even completely free on the internet – and which come deceptively close to the real thing. Large language models can meanwhile be run without any problem on local computers. Their output can then be transmitted via an API to a voice cloning tool, so that such attempted scams are scalable. This opens up several new horizons for fraudsters - the barriers have never been so low, and they now need even fewer skills to mount really effective attacks.



Kragh: The use of artificially generated voices and images to foster trust is a powerful tool. A well formulated email is one thing, but when the fake boss speaks with what seems to be his real voice, or also looks genuine, and perhaps even his real office seems to be the background, that is an entirely new dimension on top, which can often dispel all doubts even in staff who have been trained to spot fraud.

Does that mean that we must now expect a wave of fake president scams?

Kragh: Since our first Fake President case six years ago, which according to our assessment used audio deepfakes and where an employee fell for the "fake boss", we have only seen isolated cases of this type – the big storm has not transpired. That may now be gradually changing, however: The World Economic Forum in its Global Cybersecurity Outlook 2025 estimates that the global trade in deepfake toolstools in the darknet tripled between the beginning of 2023 and 2024.

Alby: A company's own employees are an attractive target for fraudsters in more ways than one. Social engineers get their information from a variety of sources. In some cases they hack into intranets and gather information there, but social networks are also playing a growing role. The criminals can often obtain confidential information by means of so-called "vishing" calls to various parts of a company In a large hotel and casino chain a group of criminals identified one employee on LinkedIn and then contacted the IT help desk. Within 10 minutes they had elicited enough information to hack into the IT system. With skilfully crafted audio deepfakes, this is likely to become even easier in future, since employees can speak openly about the status of confidential projects or company secrets with their manager or supervisor, thus unwittingly helping in the scam. And in addition, internal accomplices are frequently involved both in social engineering and fraud. They may for instance collect voice material, document templates for invoices and emails as well as information about processes, control systems or contact persons and pass it on.

How can employees tell if something is a deepfake at all then?

Kragh: Unfortunately that is not nearly as easy as it used to be. Nevertheless there are a few indicators. For instance you should be on the alert for a rather unnatural pattern of emphasis, the speech intonation, or also how authentic movements or blinking appear. Poor audio or video quality or inexplicable background noises or alterations in lighting and skin tone are also important clues. Similarly, poor synchronization between lip movements and what is being said. You can also simply ask your opposite number to put a finger to their nose.

Alby: That is already quite a good approach, but I wouldn't entirely rely on it. I fully expect to see deepfakes in the next few months in which all those things no longer apply. That is why it makes sense for companies to come up internally with ideas about how they can put control mechanisms in place. Criminals don't rest on their laurels: they are working day and night to eliminate the remaining deficits, and the first thing they do is to make a note of such "tips how to tell a fake". That then becomes their input for the next stage of evolution. It is definitely going to be a constant game of cat-and-mouse.

So what concrete steps can companies take to protect themselves?

Kragh: As with any loophole, it is always a kind of arms race. First the fraudsters – and they are very creative – develop new scams and variants and companies tighten up their defences to counter them after a time. Companies are therefore mostly one step behind. Making employees aware of the danger in regular training sessions and seminars is of the utmost importance. Or running regular tests with simulated scam emails from your own IT security department. A commitment by senior management never to instruct remittances via video call or a password for certain business transactions can also be appropriate precautions. The important thing is that everyone keeps to the rules at the end of the day. And most important of all is openness: a good culture of error management and an open corporate culture are the most effective levers against criminal machinations. That is impressively illustrated by a fake president case which was recently foiled in which an astute check back by the employee (see the case studies on page 15) caused the entire construct to collapse like a house of cards.

Marie-Christine Kragh
Global Head of Fidelity
at Allianz Trade

Tom Alby
Chief Digital
Transformation Officer
at Allianz Trade

Alby: New technologies are changing processes and working environments and this is happening currently at breathtaking speed. This should be remembered if we want to at least keep more or less abreast of developments – which, to be honest, is going to be difficult. Covid 19 was a good example for abrupt and unanticipated process changes: suddenly the entire workforce was working from home instead of in the office – what changes does that mean for processes and security risks? The same is true of AI: these tools bring many advantages, but people have to learn how to use it correctly. For instance, it is definitely not a good idea to input internal company information to ChatGPT when writing an email to your boss just to save time, since the algorithm also uses this information to learn. That is why companies should define clear rules and binding guidelines about what is permissible and what is not. A number of security loopholes can already be closed through that. Regular stress tests, AI detection tools and multi-factor authentication are similarly options to at least minimize the risk. Looking ahead, fingerprinting, i.e. authenticating an email sender via their fingerprint could be one solution implementing a further layer of security. But the criminals will of course consider just these points and find ways of getting around them And: people will always be the weakest link.

Kragh: Especially since external perpetrators such as in social engineering are only one side of the coin: it is insiders, possibly working at the desk next to you, who still cause most losses. That is also an uncomfortable truth which will not go away.

> “It is definitely going to be a constant game of cat-and-mouse with the fraudsters. **Tom Alby**

Conspicuously invisible: When your friendly colleague suddenly pounces

Inside perpetrators, e.g. employees who harm their own company, are responsible for most, and the highest, losses in 2025. And that means: much as trust is an important element of corporate culture – there must be limits to it. With effective control systems and clear-cut processes, the opportunities for criminal acts can be minimized.

It is an unpalatable truth for companies: most losses continue to be caused by their own employees. Whether it the management secretary who financed her designer wardrobe with forged invoices for event services or the authorized officer of a security company who siphoned off a total of 26 million euros of company money to even heat the pathways at his villa – they mostly have a similar profile: they have been with the firm for at least 10 years, fit in so well that it cries out to be noticed, are well liked and implicitly trusted by their bosses.

According to Prof. Dr. Hendrik Schneider, white-collar criminals are often "latecomers to crime", i.e. people who only launch out into a criminal career in later life, - also because having a clean slate up to that point is a basic prerequisite for white-collar perpetrators. Someone straight from university would not have the competences to instruct money to be remitted for business transactions involving high sums. A manager with long years of service in the company, on the other hand, knows all the workings of the firm inside out, where the control deficiencies are, and has the requisite authority. "Then the temptation is great for some people to take advantage when a promising opportunity presents itself." Says Prof. Dr. Schneider.

In recent years external criminals have been catching up significantly and according to Allianz Trade loss statistics in 2024 have even overtaken for the first time. The perpetrators at the next desk were ahead in terms of the losses caused in 2025, though.

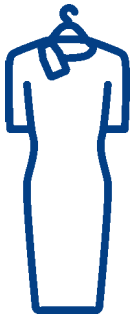
The insider criminals can also be expected to "upskill" thanks to AI tools. On top of that, their "efforts" often remain undetected for much longer, only coming to light after many years in some cases.

As regards motives and types of perpetrator, we are still dealing with a mixed bag: from the lorry driver with financial problems running a lucrative business on the side selling his employer's lavatory pans and continuous-flow water heaters, via the secretary who financed her 200 cats with company money to the accountant who systematically embezzled money onto inactivated accounts so that he could afford luxury furniture and sports cars (all true cases!), we find pretty much everything.

Employees with their insider knowledge are best placed to discover loopholes and – depending on their personal profile – to either report them, close them or exploit them. That is precisely why good control and compliance systems as well as whistleblower channels are so important: they minimize the opportunities for crime. The corporate and error tolerance culture of a company, as well as the "tone from the top" also play a vital role. Autocratic or strictly hierarchical cultures encourage people to "break out" and are frequently much more susceptible to white-collar crime. As so often: it's the balance that makes the difference.

Familiar voices and control-proof AI deepfakes

AI ensures a boost to efficiency – and also the upskilling of fraudsters. That is also apparent from the current example cases, which illustrate the full bandwidth of criminal energy. While striking the right tone in emails used to be a sophisticated and laborious art years ago, the AI today spews texts which appear quite authentic and perfectly forged invoices virtually by the second, imitates familiar voices - or the boss in a video conference. Its credibility, and thus the chances of a successful scam, increases with each evolutionary step, But insiders, too, are crafty – and stay undetected for much longer.



In a ball gown from my employer

In a company which specialized in renting out designer dresses and accessories designer gowns, matching shoes and various handbags and other accessories to the tune of 8,000 euros disappeared. It was only noticed that they were missing when a customer placed an order to hire a very extravagant ball gown and it could not be found despite an intensive search. The inventory which followed revealed that it wasn't the only dress which had disappeared without trace. Altogether, 13 dresses and 10 pairs of designer shoes had gone missing – all of them from two particular designer labels and in size 38 and shoe size 39. On the strength of this, the managers installed hidden surveillance cameras and this led to the perpetrator being caught.. The employee had a passion for luxury dresses - which however were way beyond her financial means. So she had topped up her wardrobe from her employer's stocks. Part of the bounty was found in her flat.

The shop in the shop scheme

An employee in a garden centre in Thüringen who was responsible for the online shop ran a "shop in the shop" scheme. He sold tools and garden equipment from the centre – but under his own name, at knock-down prices and without having legally acquired them beforehand. The shop flourished, since he knew all the processes inside out, knew when he would be alone and could take goods from the centre's warehouse unnoticed.

Since he despatched the goods directly from his office, he had no need to smuggle them out of the building first. His dual shop scheme worked for over a year – then came the shock: by chance, a colleague ordered a battery hedge trimmer which was offered at an incredibly low price and found out that his colleague was the seller. The loss came to a total of 180,000 euros.

The familiar voice and the recovered million

An employee of a mechanical engineering firm in south Germany was first of all contacted via IMessage by someone he assumed to be the CFO of the parent company. Then came an approach which is a classic in CEO fraud: it involved a top-secret company acquisition for which he needed the support of the implicitly trustworthy employee. They also mentioned briefly the CFO's post in the company intranet in which he had announced his return from his skiing holiday. A number of emails from a lawyer from an international firm who was supposedly entrusted with carrying through the acquisition, as well as several audio calls from the "CFO", whose voice sounded genuine, followed in the next few days. Over a period of 5 days the employee ordered payments to a total value of 1.9 million euros. The CFO was so impressed that he even promised the employee a high-paying job in the holding company. When it shortly transpired that it was not the CFO, but fraudsters who had ordered the payments, the company promptly commissioned a specialist to retrieve the trans-

ferred money – which was at least partly successful: it was possible to recover almost 1 million euros. Allianz Trade indemnified the rest.

In a similar case – initial contact via Whatsapp with the CEO's correct profile image and subsequent correspondence with a lawyer – the employee transferred two payments totalling 850,000 euros to accounts abroad, When a third tranche was ordered, he became suspicious however and the fraud was exposed. Thanks to swift action by the directly commissioned recovery specialist, at least the second payment of 400,000 euros was seized from the recipient account.

CEO avatars and the saving callback

An internationally active band of criminals managed to get away with some 8.7 million euros in a CEO fraud in the Netherlands in early 2025 by means of a deceptively genuine deepfake video. In this ingenious scam, they assumed the role of AI-generated avatars of the managing director and a lawyer representing the sole shareholder of the Dutch company. The video and audio quality was so good that both appearance and voice were entirely convincing: the employee who was entrusted with the payments in the video conference executed altogether 17 bank transactions.

As well as deepfake videos, falsified documents and minutes of meetings were also involved.

The financial transfers could be traced to accounts in Bulgaria, Slovakia and Austria. The loss incurred was about 8.7 million euros. Through close cooperation between banks and international authorities in Austria it proved possible to recover 1.5 million euros– the remainder had vanished.

A video deepfake case in Britain in 2024 had already caused a furore. After a video conference with the cloned boss, an employee transferred more than 20 million euros in 15 tranches – without ever checking back. The fact is that just this simple healthy suspicion would have made the whole house of cards collapse. During the subsequent investigation it turned out that the videos had in all probability been prepared beforehand and just played.

Another failed fake president scam in an international automotive concern, also in 2024, shows how this could have been prevented. The quick-witted manager asked a "golden question" to the supposed CEO who was requesting him to transfer several million euros for an allegedly confidential company acquisition:

„What was the name of that book you recommended to me the other day?" The fraudster was trapped and had of course no idea of the book – checkmate in one check-back.

Dazzled by big names – and a solar farm half vanished

A supplier of components for solar plants in North-Rhein Westfalia received an enquiry from a very well-known power company for their planned expansion of their solar generating capacity. After a quotation had been successfully submitted, the power utility then ordered a large quantity of components for solar plants, including solar panels, inverters and mounting systems. They notified that the parts were to be delivered to various warehouse addresses which supposedly belonged to the company.

The supplier – thrilled over the large orders – started to despatch the goods without suspecting anything. When the invoices fell due, none of the familiar contact persons could be reached any more and it transpired that the real company had nothing to do with the contract. The delivery addresses were only warehouses which had been rented for a short time and were long since abandoned. The fraudsters had quickly resold the goods and then disappeared without trace, leaving behind a loss of 2.5 million euros

The perfectly forged AI invoice

A wholesaler in Hessen received an invoice from a supplier he had known for years for goods worth almost 200,000 euros. Shortly before the due date, the wholesaler's accounts department received an email with the request to redirect the payment to a different bank account. An invoice attached to the email confirmed the new bank details. The wholesaler made the payment without checking back. After a while, however, a reminder arrived in the post. When it was checked, it turned out that unknown third parties had gained access to the supplier's IT, altered the original invoice and triggered the communication in the supplier's name. The forgery looked so genuine that it was not even realized in the routine checks, which actually took place. Attempts to recover the amount transferred were unsuccessful. The scammers had long since withdrawn the money.

Male, c. 45, top finance manager seeks … loopholes in the control systems

The biggest losses are inflicted by male perpetrators in their 40s to mid-50s, well-educated, holding high and senior management positions in finance departments, who have been with their companies for at least 10 years.

They don't turn criminal so often, but when they do, it is with no holds barred, causing huge losses: they know all the loopholes in the control systems and due to their long service with the company, colleagues and superiors trust them implicitly, so that they can often operate for a long time without arousing any suspicion.

And usually they are helped in this by being friendly and polite to everyone – in fact they blend in so well that they are the last person anyone would dream of suspecting.

The typical perpetrators

The criminals who defraud their own company come from practically all genders, ages and hierarchical levels. Male offenders still predominate – but Allianz Trade loss statistics reveal a wide range of differences in how often fraudsters strike and how high the losses are.

Young, no experience, criminal, seeks … quick money

Young, inexperienced employees who have only been in the company a short time, are poorly educated and at low hierarchical levels without management responsibility commit crimes far more frequently; in most cases, however, this involves much lower sums – also because they are found out much faster.

Such frequent offenders are on average between 35 and their mid-40s. The most frequent crimes are theft, embezzlement or misappropriation.

Source: Allianz Trade loss statistics, Studies White-collar crime from KPMG, PwC, BKA Monitoring Report Insider Crime

And this is how they get caught

Trust is good – checks are better: fraudsters are most often revealed by internal control systems, followed by whistleblowing. That is why these two components play a key role in prevention. Most fraud in companies is discovered by audits, other routine checks or when checking back on anomalies. But tip-offs from other employees often lead to internal criminals being caught. That is precisely why the Law on Protecting Whistleblowers is becoming increasingly important: companies have to set up appropriate internal channels to protect those who report anomalies. Sometimes things come to light by pure chance, and in rare cases fraudsters have such a guilty conscience after wrongdoing that they report themselves.

1. **1. internal control systems**
- **routine checks/ audits**
- **checks on anomalies**

2. **whistleblowing**
- **tips from other employees**
- **tips from outsiders**

3. **chance**

4. **self-disclosure due to a guilty conscience**

Source:
Allianz Trade loss statistics

The Law on Protecting Whistleblowers: What is it and what does it mean for companies?

The Law on Protecting Whistleblowers (Hinweisgeberschutzgesetz (HinSchG)) is the enactment into German law of the EU Whistleblower Protection Directive. This law, which came into effect in July 2023, is intended to protect whistle-blowers from all kinds of negative consequences. For most companies, public authorities and municipalities that means that they are obliged to set up an internal whistleblowing system. Tip-offs from employees are thus be encouraged by law and court practice.

According to a study by the Fachhochschule Graubünden (FHGR/formerly HTW Chur), only 55% of respondents had a notification officer in 2019. With the legal obligation and the new whistleblowing systems set up as a result, it is to be expected that significantly more anomalies will be reported and cases of wrongdoing by insiders detected.

Lawyer Prof. Dr. jur. Hendrik Schneider
Is a legal scholar and criminologist. In his research he has dealt extensively with different perpetrator profiles and their motivations.

INTERVIEW

"The first time is often a pacemaker into crime."

What different types of perpetrators are there, how do they differ and why do they actually become perpetrators? Prof. Dr. Hendrik Schneider reports on the differences and motivations of white-collar criminals - and what companies can do to protect themselves from white-collar criminals today, but especially in the future.

According to Allianz Trade loss statistics, the "typical perpetrators" who cause the most damage are highly educated men in their mid-40s, managers who have been with the company for at least 10 years; colleagues describe them as "conspicuously inconspicuous" up to now. Why?

White-collar criminals are "latecomers to crime", meaning late bloomers in their criminal career. There are several reasons for this. A graduate fresh from university, for example, would not have the authority to order transactions involving large sums of money. A manager with many years of service, on the other hand, knows how things work, where there are niches and control deficits, and has the necessary authority. Some people are tempted to take advantage of a favourable opportunity. This can be seen, for example, in the extreme increase in proceedings for subsidy fraud in the Corona crisis in 2020 by a staggering 2285% with losses of around EUR 95 million. However, no one in a position to apply for economic subsidies, for example, can get a clean police record. In other words, a clean slate is the basic prerequisite for white-collar offenders.

Why is it actually mainly men?

That's hard to say – one of the reasons is certainly that there are still more men in corresponding management positions.

When we talk about "typical perpetrators," age, position and company affiliation say little about the perpetrator's personality. Are there any characteristic traits?

On the one hand, we differentiate between opportunity seekers and opportunity seizers. As the name suggests, some proactively look for vulnerabilities and others react to an opportunity that arises. There are also personal risk factors. we differentiate between four types of perpetrators: the perpetrator with economic criminological stress syndrome, the crisis perpetrator, the dependant and the inconspicuous one.

What drives them?

The dependant is – as the name suggests - usually an accomplice and henchman of a dominant main perpetrator on whom he is economically or hierarchically dependent.

The perpetrator with economic criminological stress syndrome, on the other hand, lives an unrestrained life in the moment according to the motto "earning and burning money" and is part of a "work-related subculture". Often the crimes occur in a biographical upheaval phase that is associated with control deficits and lack of involvement, e.g. the job abroad, divorce, etc. He is an opportunity seeker who immediately seizes every opportunity that comes his way.

Does opportunity really make the thief?

Sometimes that actually is the only trigger. It's exactly the same with the "inconspicuous" person. This type of perpetrator actually has no or only very low personal risk factors. The temptation of the favourable opportunity was simply too great. If the crime comes to light, everyone around him is surprised because he was previously inconspicuous and conformed to the rules and would have fallen through the cracks in a risk screening.

Additional payments for electricity or heating costs, high inflation and rising interest rates are currently presenting many people with major problems. Do companies now have to fear crisis perpetrators and what makes them so?

In this respect, we are talking about economic pressure situations that are increasingly occurring under today's economic conditions. From the perpetrator's perspective, the crime may represent the only way out of the financial crisis. Because the act conflicts with his self-image, neutralization techniques help him to smooth out the inner turbulence, e.g. "I'm just borrowing the money"; "The insurance will compensate the loss anyway".

But not everyone becomes a criminal?

No. Crisis perpetrators are under massive pressure, but there are of course ways out that do not involve criminal offenses - in extreme cases, filing for bankruptcy. But not everyone is ready to take these steps or to adjust their living standards downwards during the crisis.

You mentioned neutralization strategies. how should we imagine such strategies?

White-collar criminals are not inherently immoral. Crisis perpetrators in particular often have high values and therefore have difficulty justifying criminal acts to themselves. "It's just this one time", "I'm just doing what everyone else is doing", "It doesn't affect anyone else personally, they can afford it" can be such justifications.

If perpetrators still see the need to rationalize something, this is actually a good sign that all is not yet lost. This means that there is still a value orientation and inner turbulence that raises the alarm. But it could also be the beginning of the end.

So then they become repeat offenders?

The first time is either actually just a one-off - or a pacemaker into crime. The first time, the inhibition threshold is often high. But there is success learning and a habituation effect. The more often one lies or cheats, the lower the discomfort. At some point, the alarm bells no longer ring and it then runs virtually by itself. As long as the facade and camouflage are intact, perpetrators often don't even notice how criminal they are because this gradual slipping means that it doesn't feel so criminal at all - that often doesn't come until the court case. This is called a "drift into entrenched criminality," and white-collar criminal careers can develop.

Incidentally, this is also the case in workplace-related subcultures. In these parallel worlds, people are among like-minded people and there is no objective corrective. When, over a beer in the evening, you review how slyly you acted today, completely new value spaces are created and you are in harmony with your environment. The group dynamic means that they don't need neutralization techniques. However, it also leads

to being pulled into the abyss even faster. Then, at some point, the rude awakening will come.

Speaking of a rude awakening: Aren't the perpetrators afraid of being discovered and losing their jobs?

In fact, the perpetrators – contrary to many assumptions – usually have a lot to lose. The risk of detection does play a role in their consideration of whether to succumb to the lure of the opportunity to commit the crime.

But there is often a big difference between the objective and the subjective risk of detection. Risks in the future that seem far away are often weighted less heavily.

If I, as the perpetrator, know that the deeds could be discovered during the next audit, it makes a difference for the subjective risk of discovery whether the next audit takes place in three weeks or in three years.

Keyword control systems - how can companies protect themselves?

Good control and compliance systems and clean processes are the be-all and end-all, because they minimize the opportunities for crime. At the same time, it is important to constantly think about the new risks that could arise in the future as a result of digitalization, increasing cyberattacks, new technologies, and artificial intelligence such as ChatGPT. Fraud schemes are likely to accelerate just as rapidly as technological progress. When a fake boss can spit out a "CEO style" email at the push of a button, professionalism and scalability speed into new realms.

Indeed, this is also a generational issue. That's why it's important to have young, technology-savvy employees on board who are aware of the risks involved. Incidentally, this applies to compliance as well as to supervisory boards.

You can also simply do a self-test and try it out. Send a chat GPT mail to your own organization. This will allow you to mercilessly identify your own weak points in processes and control mechanisms.

You can then readjust before financial damage occurs.

Awareness-raising and training measures are very effective for prevention. And since July 2023, certain companies have also had to implement anonymous reporting channels for irregularities under the Law on Protecting Whistleblowers.

What role does corporate culture play?

The corporate and error culture as well as the "tone from the top" play an important role. Autocratic or very hierarchical cultures favour "breaking out" and are often much more susceptible to white-collar crime. As is so often the case, It is a matter of finding the right balance.

In some companies, complementary dual leadership can work well, and in fact diverse teams are helpful for both corporate culture and corporate success. When different points of view, perspectives and value orientations come together, things are questioned and considered in a completely different way. This often leads to a much more differentiated approach and helps with important decisions and culture.

How can companies protect themselves from black sheep?

Fraud and embezzlement continue to rank among the top white collar crimes. The number of cases of white-collar crimes registered under fraud in police crime statistics[8] went up significantly by 116.7% year-on-year in 2024 – often involving insiders. In Allianz loss statistics, too, it is insiders who caused most and the major losses. There are more black sheep than many companies think, and they cause huge financial losses year for year.

Yet in many cases they are very hard to identify. They often blend in so well that it cries out to be noticed, are friendly, fit in well and are completely integrated. Many eminently desirable qualities of high achieving workers are the same ones which characterize fraudsters as well – such as determination to succeed, a high risk appetite, ambition and a focus on getting to the top.

That is why it is important for companies to find the right balance between trust and corporate culture on the one side and prevention and controls on the other.

Satisfied employees who feel comfortable, are respected and appreciated by their managers and their colleagues and are happy with the tasks they perform and their pay as well as their career prospects and further training opportunities identify with their company and are normally far more loyal than those who find themselves in a toxic working atmosphere. Harassment, frustration and revenge are often the motives which prompt insiders to commit crimes.

The corporate culture and culture of error tolerance as well as open and transparent forms of communication therefore have a vital role to play. When people who work together trust each other and articulate their grievances, weak points can be identified, loopholes closed and criminals identified much faster.

That said, control mechanisms, guidelines and regular routine checks are just as important for companies in order to protect themselves – because opportunity makes thieves.

Nevertheless: the human factor is flexible, and black sheep will always find ways and means. Many inside criminals have a high degree of criminal energy, they seize opportunities as soon as they are aware of them and can get around even the best control systems. For that reason companies should never become complacent about their control systems or allow themselves to be lulled into a false sense of security.

[8] *Source: German Federal Report on Economic Crime, 2024 (Bundeslagebild Wirtschaftskriminalität 2024, BKA)*

Trust & culture

An open, trust-based **corporate culture** with flat hierarchies

A good, constructive **culture of criticism of errors** and open communication

Clearly formulated **corporate guidelines and ethical values** which are also integrated into day-to-day work

Satisfaction surveys of staff; Implementation of measures to increase staff satisfaction levels

Support for employees in (personal or financial) difficulties through appropriate assistance or counselling programmes

Equal opportunities, diversity, fair career prospects with clearly defined, objective and transparent criteria

Talent management and **development;** further training in hard and soft skills; junior staff development

Satisfaction surveys of staff; Implementation of measures to increase staff satisfaction levels

Support for employees in (personal or financial) difficulties through appropriate assistance or counselling programmes

Precautions & controls

Putting **control and Compliance systems** in place; in particular the separation of functions (4 or more eyes principle)

Campaigns and training to raise awareness in staff for **internal guidelines** and critical situations and **how to detect anomalies**

Regular **routine checks,** internal audits, where needed checks by external third parties

Implementation of secure internal (and where appropriate, external) **whistle-blowing channels** (e.g. ombudspersons) and regular information to staff

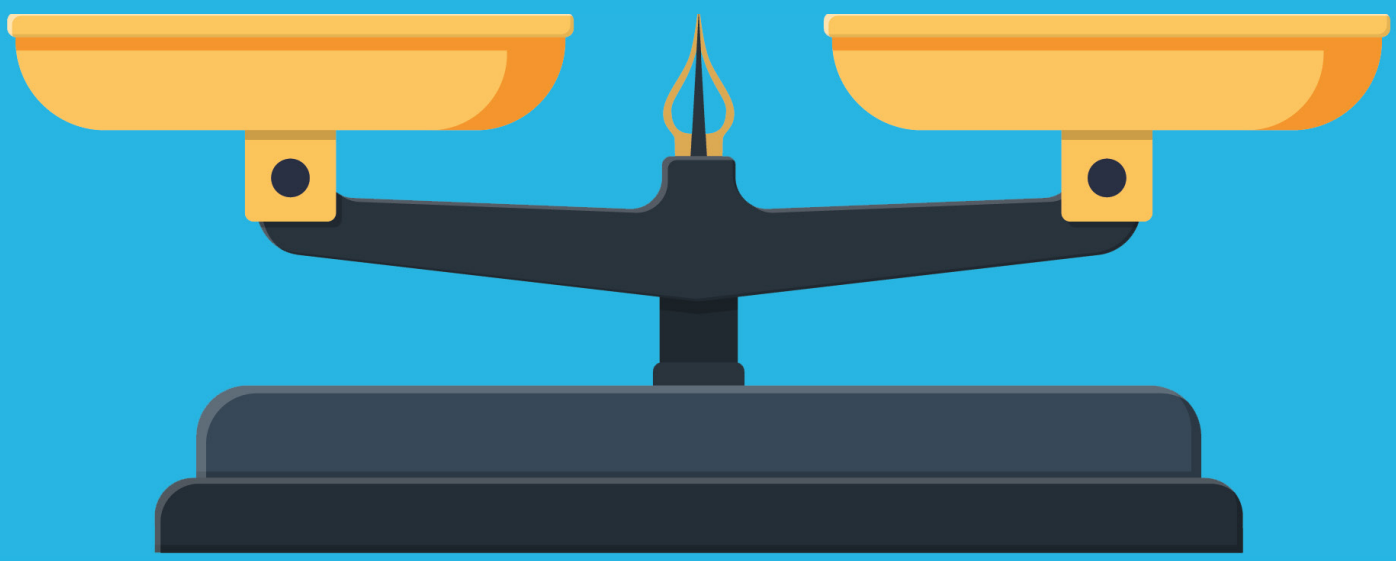
Checks on job applicants, e.g. compliance screening, police clearance certificate, Schufa report, plausibility or background checks, references

For especially security-sensitive positions where appropriate **determination of personal factors,** e.g. Hannoversche Corruption Perceptions

Prompt, transparent and objective **investigation where there is any suspicion**

Checks on job applicants, e.g. compliance screening, police clearance certificate, Schufa report, plausibility or background checks, references

For especially security-sensitive positions where appropriate **determination of personal factors, e.g.** Hannoversche Corruption Perceptions Index



Close the security loopholes

Despite all the precautions you may take, fraud and misappropriation cannot always be prevented. When an event of loss occurs, it is of the essence for a company to act swiftly and effectively and to systematically close the security loopholes. Companies should also check the most frequent risk factors, ideally at regular intervals.

1. Corporate structure & governance

- **a.** Are workflow and processes in the company clearly demarcated and accessible?
- **b.** Is there a reporting system about necessary and possible security precautions as well as for incidents and the effectiveness of controls?
- **c.** Are there defined escalation channels in the event of suspected social engineering?
- **d.** Is out-of-band confirmation mandatory and is it documented?
- **e.** Is there an open corporate culture with the active reporting of suspicious circumstances?

2. Payment transactions

- **a.** Is there a technically compelling dual control principle in payment transactions?
- **b.** Is it defined which payments need to be cleared?
- **c.** Are bank details only changed after an out-of-band check-back?
- **d.** Are new bank connections compared with historical data?
- **e.** Are BEC safeguards in place?
- **f.** Are there awareness programmes for social engineering and deepfakes?

3. Secure. emails

- **a.** Are email authentication protocols observed (SPF, DKIM, DMARC)?
- **b.** Do you use DMARC with Policy "reject" and Monitoring?
- **c.** Is there a process for detecting compromised accounts (identity protection)?
- **d.** Do you offer training courses about modern phishing scams (audio/video deepfakes)?

4. IT security

- **a.** Is there a security concept for the IT system?
- **b.** Are phishing-proof MFA (passkeys, hardware tokens) used?
- **c.** Is there a business continuity plan for compromised accounts?
- **d.** Are there regular checks to detect manipulation of email accounts?

5. Purchasing / Sales

- **a.** Are responsibilities clearly demarcated?
- **b.** Is there an independent check on inventory processes?
- **c.** Are reports made to management on returned goods and cancellations?
- **d.** Do you have a purchasing policy and a code of conduct?
- **e.** Is communication with suppliers checked for deepfake / BEC indicators?

6. Personnel / HR

- **a.** Are unusual job applications checked?
- **b.** Are in-depth checks carried out for key positions?
- **c.** Are all employees sworn to secrecy?
- **d.** Are there obligatory training courses on phishing, social engineering and AI scams?

7. Audit & controls

- **a.** Do you have an internal audit department?
- **b.** Are regular audits carried out in all departments?
- **c.** Are the effects of remote office working evaluated?
- **d.** Does the audit department check out-of-band findings?
- **e.** Is there an audit of indicators for account takeovers?
- **f.** Are BEC defence processes checked for effectiveness?

8. Modern attack scenarios

- **a.** Are there rules for payment orders under time pressure (fake president /CEO fraud 2.0)?
- **b.** Is payment release via video/phone call only done after checking back?
- **c.** Is there a policy for detecting deepfakes?
- **d.** Are red flags for unusual communication patterns detected?

Euler Hermes Deutschland
Niederlassung der Euler Hermes SA
22746 Hamburg
Tel. +49 (0) 40 / 88 34 - 0
info.de@allianz-trade.com
www.allianz-trade.de

05 4000DE-EN 0426