www.pwc.cz/crimesurvey

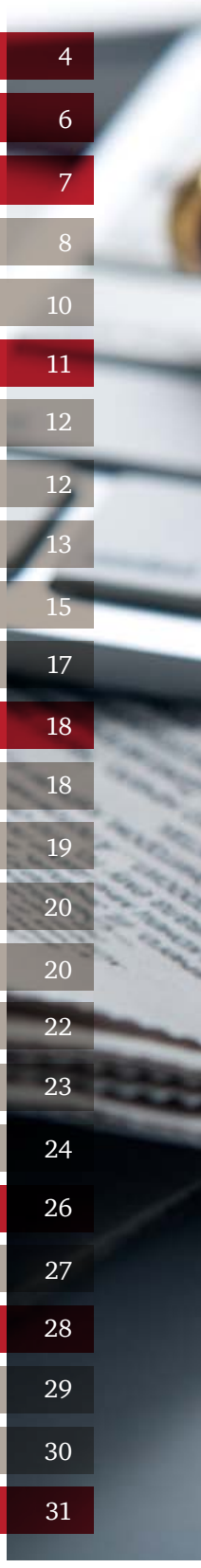
Global Economic Crime and Fraud Survey 2018

Czech Republic

Pulling fraud out of the shadows

pwc

Content



Preface

Pavel Jankech
Director, Forensic Technology Solution

Kateřina Halásek Dosedělová
Senior Manager, Forensic Services

We are pleased to present to you the results of the **2018 PwC Global Economic Crime and Fraud Survey**, which continues to be the largest study of its kind available worldwide. To get the most updated insight into the current state of economic crime, its perception, impacts and the awareness organisations have about economic crime, we collected responses from 7,228 organisations from 123 countries, including 73 leading companies within the Czech Republic.

Beyond offering valuable data on the evolution and current state of fraud this year's Economic Crime and Fraud Survey sheds much-needed light on some of the most important strategic challenges confronting every organisation – from compliance, culture and crisis response to new perspectives on accountability, technology and cybercrime.

The time is right for organisations to adopt a new, more holistic view of fraud. One that recognises the true shape of the threat – not a mere nuisance, not a "cost of doing business", but a shadow industry. Since fraud hides in the shadows. We should not ask: Are you the victim of fraud? The important question is: Are you aware of how it is touching your organisation? Are you fighting it blindfolded, or with eyes wide open?

Fraudsters are more strategic in their goals and sophisticated in their methods.

Strategies used to detect fraud a few years ago are therefore becoming outdated and not as effective in combatting economic crime. We will explore in this report, how to utilise the potential of available technologies to fight fraud effectively, since even though the global and CEE trends indicate increased use of technology in fraud detection. This year's results show a somewhat reduced use of technology by the Czech respondents.

We invite all entrepreneurs, compliance officers, fraud managers and others engaged in corporate governance, compliance or fraud risk management to read through the report and draw conclusions relevant to their business. This local report supplementing the 2018 Global Economic Crime and Fraud Survey report is available to help you in your fight against economic crime. We believe that the results of our Survey will allow you to better understand the significant impact that economic crime can have on your business, assess the risks of fraud that you may face, and find ways to mitigate those risks.

Last but not least, we would like to thank the Survey participants from the Czech Republic who were kind enough to share their observations of fraud and provide their insights. The respondents share our belief that economic crime is too costly to be ignored.

123
countries

Surveyed in
18
different languages

7,228
completed surveys globally

22
industries

73
Czech companies

Highlights

Current fraud environment in the Czech Republic

- In PwC's 2018 Global Economic Crime and Fraud Survey ("Survey"), only 33% of Czech respondents mentioned that they were victims of economic crime. In comparison with our previous Surveys, it appears as if incidents of fraud at the Czech respondents were decreasing.
- This is contradicting the CEE and global results showing that incidents of fraud reported by the respondents have risen from 33% and 36% 2016 to 47% and 49% in 2018, respectively.
- Similar to the results from our previous Survey, asset misappropriation represents 50% of all reported fraud cases. Followed by consumer fraud (38%), procurement fraud (29%) and cybercime (25%).

Cybercrime

- While companies use the most up-to-date technology in their daily business, and thereby opening themselves to increasing risk of external attacks, cybercrime incidents reported by Czech respondents dropped sharply from 36% in 2016 to 25% in 2018. This is quite a contrast when compared to the CEE (30%) and global level (31%) in 2018.
- The most frequent technique of cyber-attacks reported by the Czech respondents is phishing (41%). It is significantly higher than the CEE (28%) and global level (33%). The results further indicate that none of the industries is immune to phishing attacks.

Role of technology in fraud detection

- As new technologies are more common in our everyday life, companies can take advantage of various modern automated anti-fraud solutions. However, not only have companies been utilising modern technologies, but fraudsters also have not been falling behind and exploiting new technologies to expand their possibilities for fraudulent attacks as well. As criminals are perpetrating increasingly complex fraudulent schemes, organisations should catch up to new trends as fast as possible to stop fraudsters from gaining the upper hand.
- In this respect, another trend out of our Survey might come as a surprise. Czech companies have been using less modern technologies to combat fraud than CEE and global companies. On average, only 30% of Czech respondents use modern technologies to combat fraud compared to 37% in the CEE region.
- An obvious question needs to be asked: "Is there any causality between the limited use of the anti-fraud technology solutions by Czech respondents and the reported decreasing number of fraud cases, a number which is significantly below the CEE level?"

Training and corporate culture still play a significant role

- When combating fraud, the use of up-to-date technology is highly recommended. However technology alone is not enough. No matter how good your anti-fraud tools are at successfully counterattacking fraud, your company should invest in its employees, provide them with appropriate training and focus on creating and maintaining a corporate culture devoted to combating both internal and external fraud.
- One of the key pre-requisites of a successful fraud-risk management is the proper assessment of fraud risk, because as without knowing which risks your business is facing, it is hard, if not impossible, to effectively minimise them. The other key components are ethics and compliance programmes. It is, therefore, very good news that 93% of Czech organisations performed a fraud risk assessment and 92% implemented their ethics and compliance programmes.

1 *Coresponds with the Eastern Europe as reffered to in the PwC's 2018 Global Economic Crime and Fraud Survey*

I. Economic Crime in the Czech Republic

Even though the occurrence of economic crime slightly decreased since our last Survey, every third respondent was affected by fraud

Contrary to global and CEE trends, Czech respondents have not experienced an increase in the occurrence of economic crime – instead, the reported incidence has decreased slightly compared to our previous Survey results. Only one-third of our Czech respondents stated they have experienced economic crime in the past 24 months. This is something that is not in line with either CEE or global data that indicate economic crime has risen from 33% and 36% in 2016 to 47% and 49% in 2018, respectively.

Do these results indicate that Czech companies are less prone to risk of fraud? Probably not.

When analysing the types of fraud identified and the ways in which these cases were identified, it becomes apparent that Czech companies rely heavily on internal or external tip-offs, in addition to general internal controls (refer to section III.).

This is reflected in the types of fraud identified, most commonly asset misappropriation and consumer fraud, which are likely to be detected by less sophisticated precautions. This suggests that Czech companies are less likely to detect sophisticated fraud schemes than their counterparts in other countries.

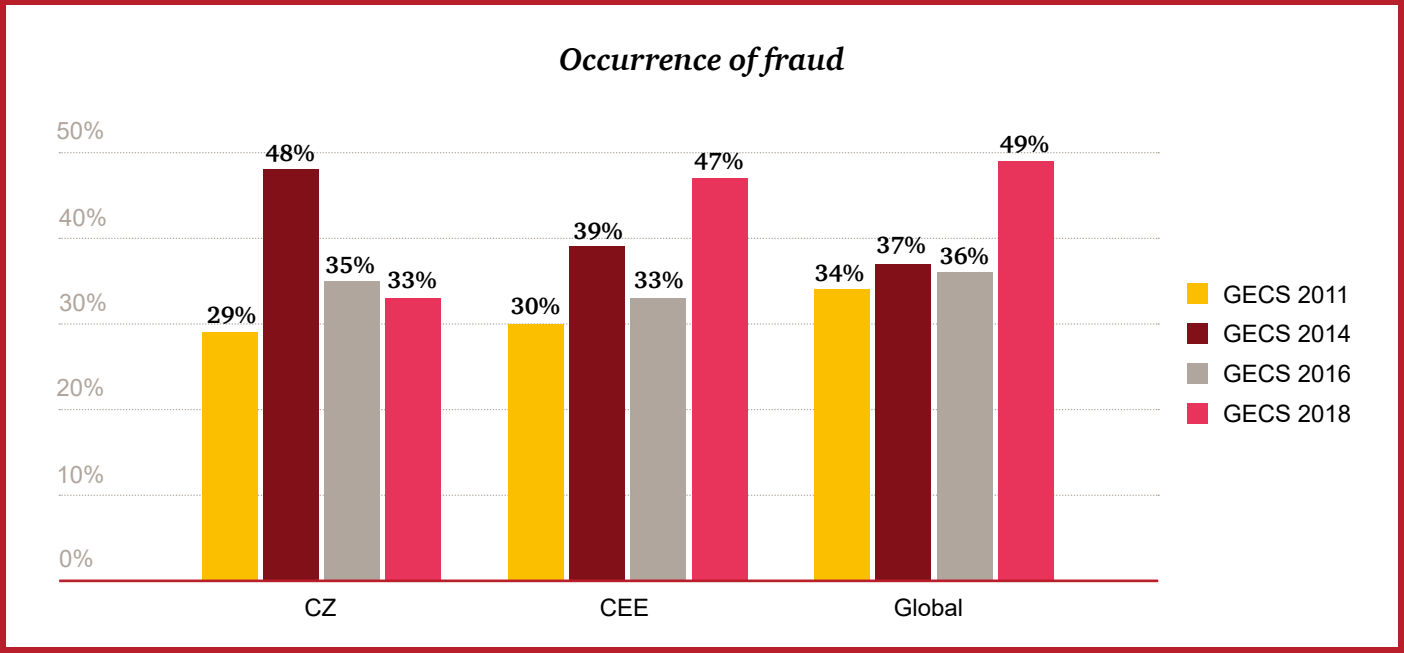
The major gap between Czech companies and their CEE and global counterparts in terms of the number of reported fraud incidents can be caused by the fact that Czech companies are not aware of some fraud cases. What would be the root cause of this lower level of awareness in Czech companies?

The so-called blind spots might be one explanation. They might occur when the corporate fraud risk management is not centralised and different departments are responsible for different types of fraud. On one hand, the responsibilities can overlap, but on the other hand, this decentralized approach can create situations where everybody thinks some other department is already dealing with this type of fraud and thus assume they do not have to address it. However reality can be far more different resulting in fraudsters having the chance to easily penetrate a company's anti-fraud defence and so stay undetected.

As economic crime evolves, so has our study.

Among some enhancements we have made this year are:

- We have added questions on the specific types of anti-fraud technology companies currently use
- We have included benchmarks on both the costs of fraud and the amounts companies spent on fighting it
- We have added new types of fraud, whose prominence has grown



What types of fraud should you watch for?

Asset misappropriation remains the most common type of fraud reported not only in the Czech Republic, but also at the global and CEE level. Over the last two years, it represented 50% of the fraud reported per our Survey.

50%
Asset misappropriation

38%
Consumer fraud

29%
Procurement fraud

25%
Cybercrime

Asset misappropriation

Asset misappropriation schemes include both the *theft* of company assets, such as cash or inventory, and the *misuse* of company assets.

Common asset misappropriation includes managers making payments based on false invoices, employees claiming fictitious business expenses or payroll accountants creating ghost employees.

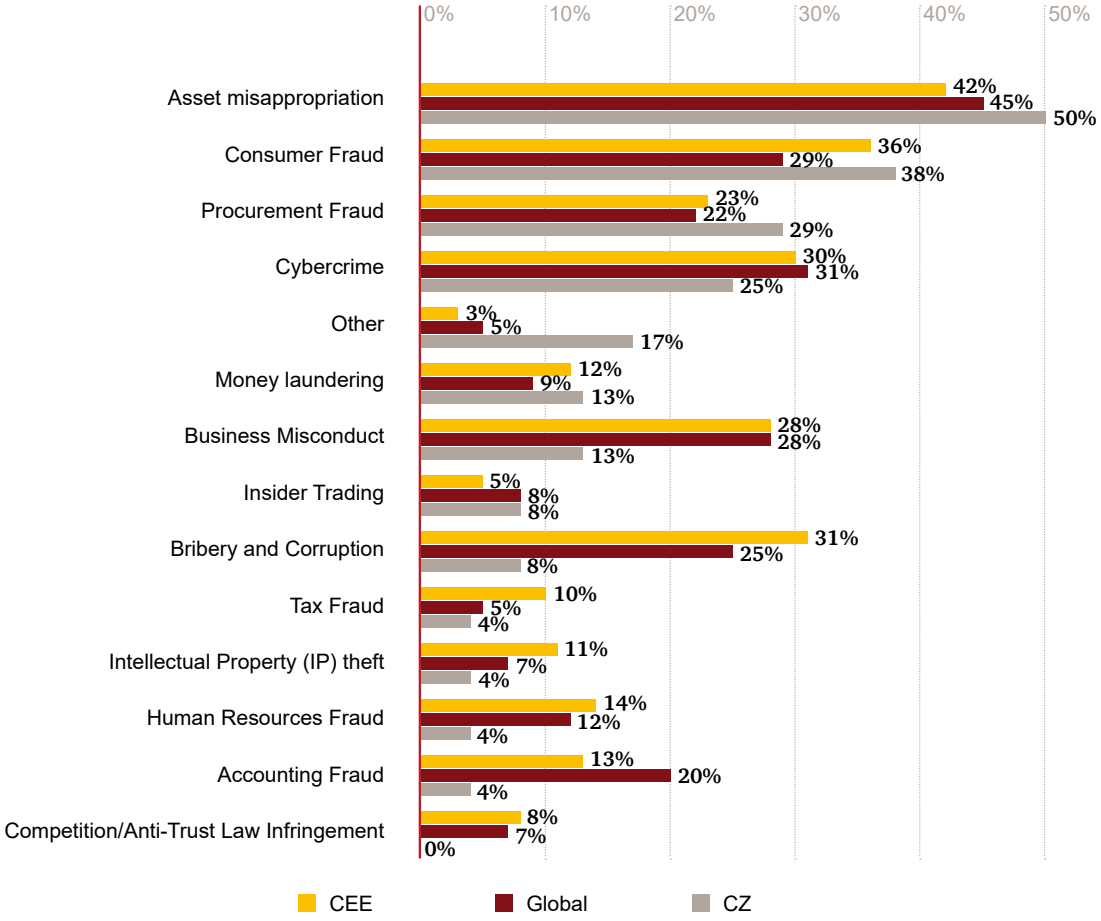
Asset misappropriation has been the leading type of fraud in this Survey for a number of years. Its high rate of detection is expected considering asset misappropriation is one of the easiest fraud types to uncover. This also corresponds with the CEE (42%) and global (45%) results.

Fraud committed by the consumer is a type of fraud whose prominence has grown so much in the past years that we have measured it as a separate threat for the first time. In the Czech Republic, it was reported as the second most common fraud faced by 38% of our respondents. This is in line with the CEE results (36%) but is significantly higher than at the global level (29%).

Procurement fraud took third place being reported by 29% of respondents. Similar to asset misappropriation and consumer fraud, procurement fraud occurs more often in the Czech Republic than at the global (22%) or CEE (23%) level.

Contrary to the above, **cybercrime** is reported significantly less frequently in the Czech Republic (25%) in comparison with the CEE (30%) and global (31%) results.

Types of economic crime



Similar to cybercrime, Czech companies seem to have experienced less misconduct, bribery and corruption or HR frauds compared to businesses in the CEE region or globally.

As previously mentioned, the fact that Czech companies reported fewer fraud cases detected over the last two years does not necessarily mean that fewer frauds actually occurred in Czech firms. The fraud cases might have been committed in such a way that existing detection mechanisms in the organisations were not able to identify them.

This conclusion is in line with the latest Transparency International Corruption perception index for the Czech Republic, which states that "*corruption has not disappeared, but is performed in a more sophisticated and delicate way*."[2]

[2] Perception index indicates what is perceived levels of corruption of the country, as determinated by expert assessments and opinion surveys.

What is the cost of fraud?

Even though this year's Survey results indicate that the fraud in the Czech Republic is in general less costly than in other territories, there are still **42% of Czech respondents** that experienced a loss of more than **USD 50,000** from the most disruptive economic crime incident.

Financial loss is an obvious and the most prominent effect of economic crime. However, fraud also causes damages that cannot be measured in financial terms, and can have an even bigger negative impact on an organisation than the loss of funds.

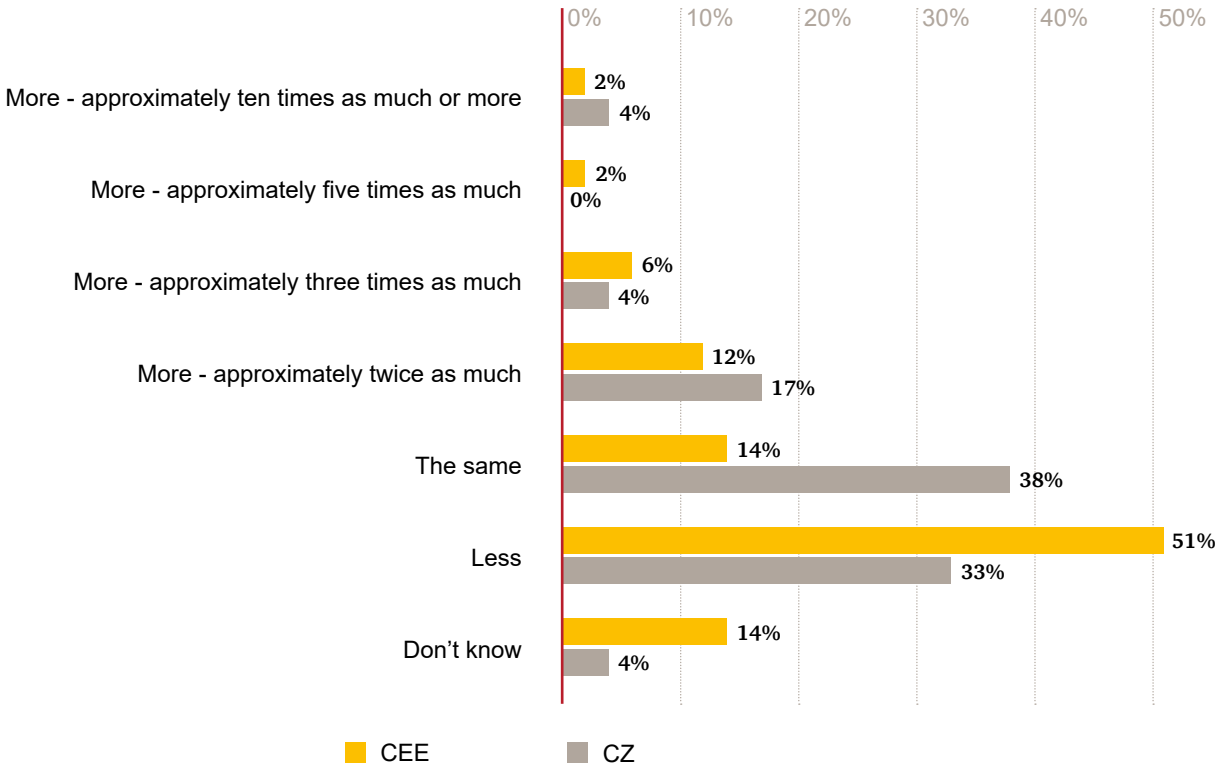
According to the Czech respondents, the disruption of employee morale is the most negative consequence of a fraud incident. Low employee morale can be very destructive to business operations. It can even be a root cause of more fraud or misbehaviour in the future as employees could adopt an "everybody does it" attitude. It is therefore critical to establish a strong "tone from the top and middle" to ensure that attention is paid to all suspicions and malpractices, a consistent approach is taken to investigations and no beneficial treatment is given to certain employees or employee groups such as management.

A negative reputation of the company and damage to the strength of the brand were mentioned as the second most detrimental impact of an economic crime. The reason appears to be obvious: the consequences of weak public trust can range from decreased creditworthiness resulting in a lack of external financing options and damaged business relations to refused memberships in trade organisations.

In order to minimise the detrimental effects, it is necessary to ensure that allegations are properly investigated. Such an investigation might be quite costly. More than one-third of the respondents stated that the amount they spent on the investigation of their most disruptive crime case experienced in the last 24 months was equal to the amount directly lost through this crime.

Moreover, 25% of respondents **spent even more on their investigation than double of** the amount directly lost. In the case of 4% of respondents, the amount spent was even more than 10 times higher than the direct financial losses of an economic crime incident.

How much did the investigation of the most disruptive fraud case cost in comparison with the direct losses of such a case?



II. Cybercrime

Data and technology are considered the two critical aspects of the current business, regardless of the industry. Technology-enabled business processes are no longer a privilege; they are a necessity.

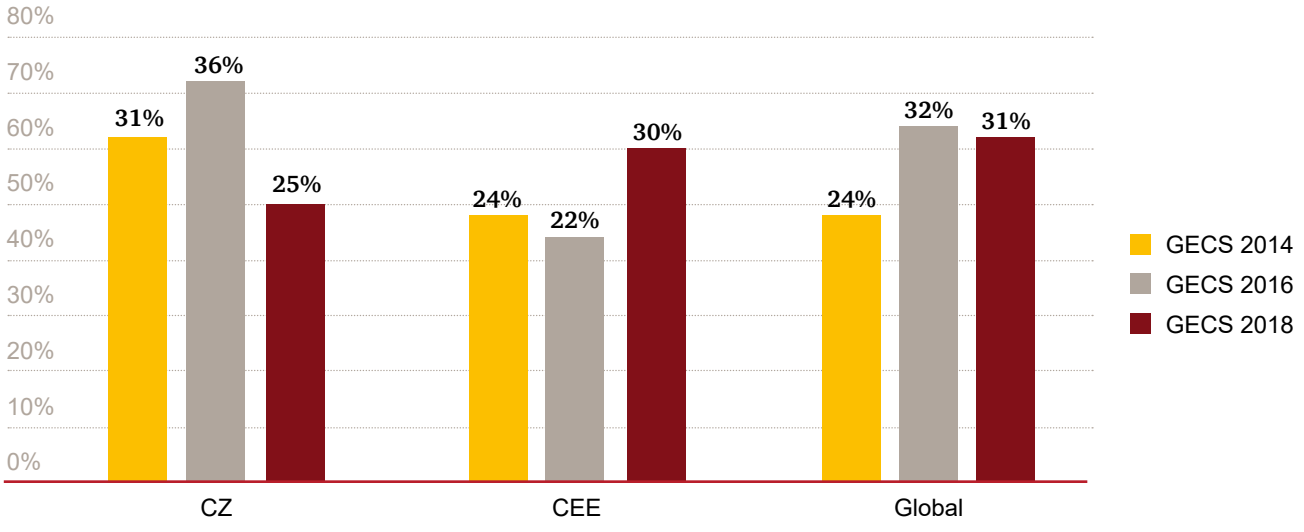
On one hand, in order to stay competitive, organisations need to keep pace with technological development applied in their industry. Should organisations have ambitions to become the industry leader, they need to be even more progressive, being early adopters of new technological innovations and deeply exploring and utilising internal and public data sources. For instance, the integration of artificial intelligence, technology capable of intelligent behaviour, is on the rise especially in the healthcare or financial sectors. In retail, big data can give companies valuable insight into who their customers are, what they want and how they react to different marketing strategies.

On the other hand, the reliance on technology and new trends like connecting physical devices to the network, digitalising all business and client related data, creating new virtual platforms and communication channels that are client friendly, open organisations to significant risk of cybercrime. As technology becomes more advanced, fraud schemes are also becoming more complex. Sensitive data stored, such as details of credit card numbers or spending and behaviour habits and information that people volunteer to share with the organisation through social media can be easily abused when it gets into the wrong hands.

Some hackers steal data, others gain access to system resources and nowadays a few do it just for the fun of it. They use different methods to exploit networks – malware, ransomware or eavesdropping. Lots of them easily escape your attention: a friendly attachment causes havoc in your computer; email from your bank asking for confirmation of personal data now comes to light as a hacker's phishing attack; packet sniffers grab your network data in transit; a seemingly innocent link launches a Trojan horse spyware; key loggers track your typing; and the special plugin you have just installed turns out to be a malicious rootkit with access to all your folders.

At the CEE level, cybercrime has steadily been increasing since the 2011 Survey. Surprisingly, reported cybercrime incidents in the **Czech Republic dropped to 25% in 2018 from 36% in 2016 and 31% in 2014.**

Cybercrime development



Phishing as the most common cyber-attack technique

Phishing has become one of the most common ways attackers try to obtain information and use it for identity theft. 41% of Czech respondents report to have been targeted by a phishing attack in the last two years.

This is significantly above the CEE (28%) and global level (33%), which may suggest that either the Czech Republic is an easy target for phishing fraudsters or Czech companies are better prepared and can more easily detect it.

Hackers have become more sophisticated and advanced. Individuals as well as companies are therefore facing attacks, which make it often difficult to distinguish between a normal business communication and a dishonest email. Phishing nowadays covers a lot more sophisticated attacks than those easily spotted, such as the infamous 'Nigerian Prince Email Scam'. In the last couple of years, fraudsters have pretended to be CEO's requesting to wire funds, financial authorities demanding consumers repay debt on taxes, banks asking for an update of personal data or post offices encouraging recipients to track their package on a false link.

In other cases, attackers managed to hack into the victim's mailbox, borrow a subject line from previous correspondence and send very plausible emails to the victim's contacts requesting sensitive details such as access to bank accounts or requesting financial funds to be sent to the fraudster's account.

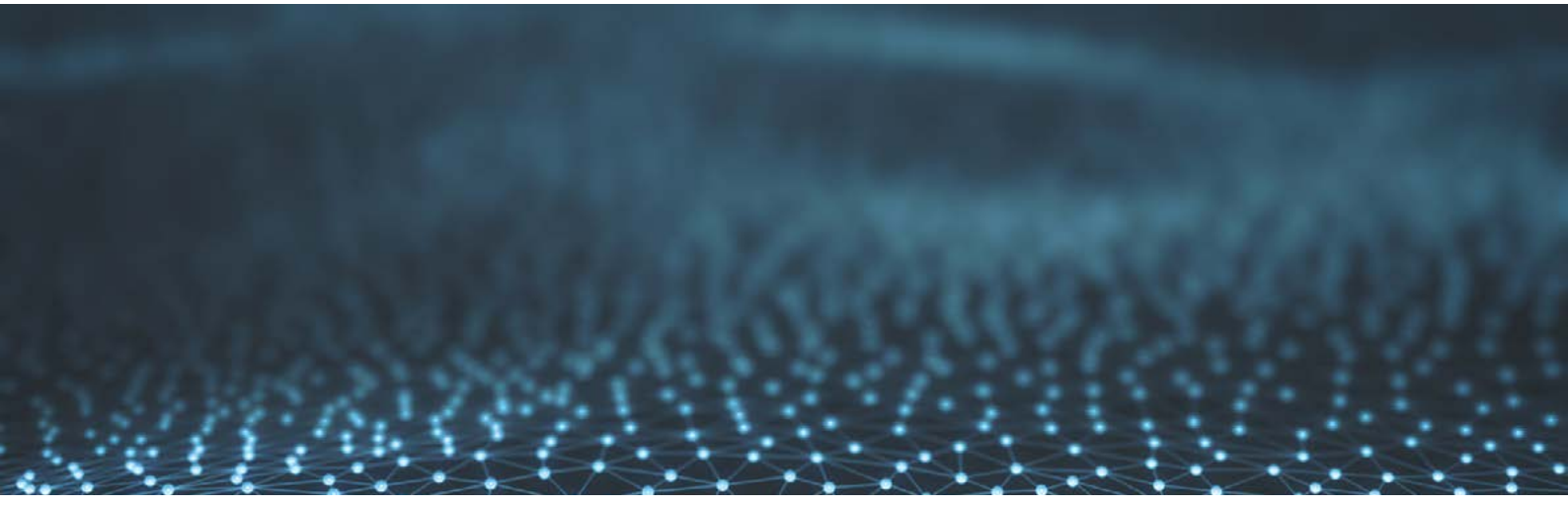
Malware – are you ready or 'wanna cry' about the many different ways attackers can get to your computer?

Malware was mentioned by 37% of surveyed companies as the second most common cyber-attack that Czech companies have been facing in the last two years. This is in line with the global (36%) and CEE trend (38%), which shows that malware is a cross-border threat.

What is malware? Malware ('or malicious software') is a broad term that refers to different types of malicious programmes performing undesirable operations in your computer.

In general, no industry is immune to cyber-attack; however, our Survey shows that the most affected by phishing and malware are manufacturing (13% and 22% respectively) and financial services (13% and 19% respectively). The reason might be obvious, as attackers use phishing and malware to gain access to the sensitive information both industries deal with. Such as clients' databases, account lists or advanced technological innovations.

Apart from the recent ransomware WannaCry, which was one of the biggest tests for security programmes across borders, some malware attacks are less prominent, but specifically targeted. Technet.cz, a Czech technology news portal, reported in April 2017 a recent ransomware attack aimed at the Czech Republic, which tricked users by using a fraudulent email in perfect Czech language, including an attachment that when opened would encrypt the users' files and demand a ransom.



Cyber Security Programme - better safe than sorry

The digital age brought a rapid change to the way businesses operate. Securing critical data, transactions and operations means working beyond the walls of your enterprise. Companies are trying to increase efficiency by many means, for example, by employing cloud computing. However, this is putting more pressure on companies when it comes to data protection and ownership.

The dependence on digital systems has paved the way for new forms of cyber security risks. The threats are numerous and, by the time you have strengthened your defences, you are probably already under attack. Combating cybercrime and data breaches can thus be a game of cat and mouse.

Ensuring an adequate, up-to-date and strong cyber security programme is now more important than ever before.

Your programme should provide continual insights and intelligence on the threats your business faces, protect what matters the most and allow for a quick and effective response. To ensure this, technology and computers alone will not be sufficient. You will need to analyse your critical business processes, ensure that internal policies are comprehensive and respected and that personnel are trained and continuously informed. As your employees are the ones who will be receiving the phishing or malware emails, their awareness of the risks and their scepticism when opening email attachments, clicking on links and downloading software is the critical factor for your company to avoid becoming a victim of cybercrime.

In PwC, we believe that a successful security model has the following characteristics:

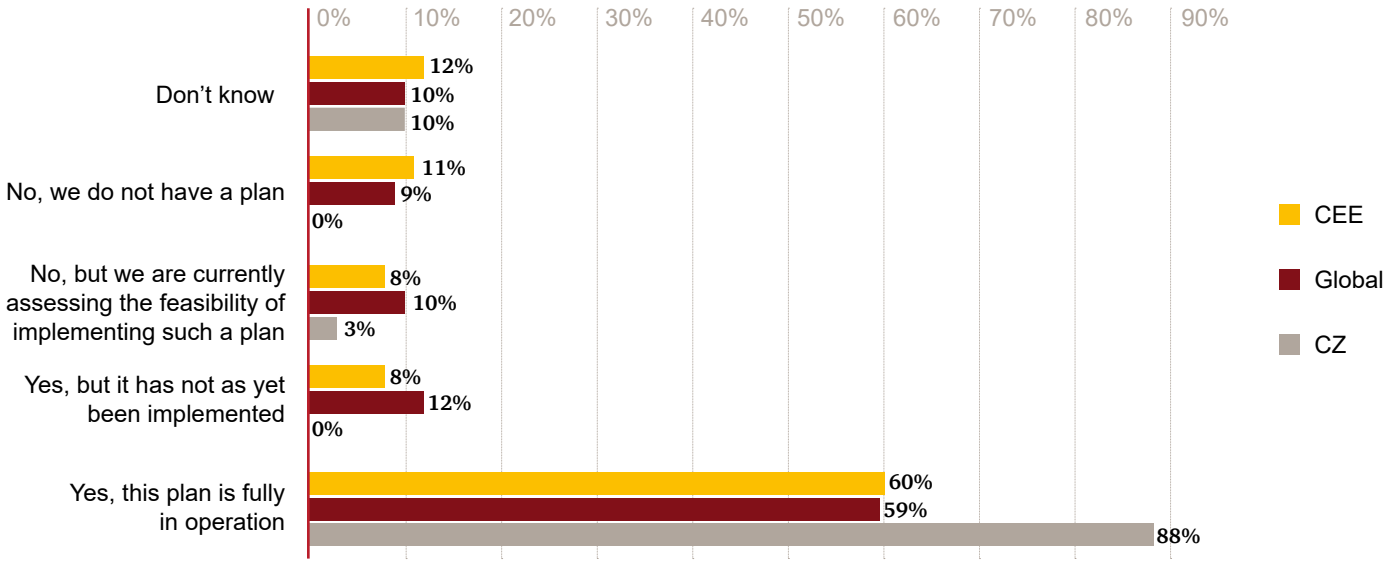
Continually monitor your risk profile and understand what matters to the success of your business.

Understand in real time the new threats within the digital landscape. You should be fully aware of the risks you are exposing the organisation to as you execute your strategic plan.

Recognised boundaries have shifted: your business landscape has changed and so have the associated technology-related risks. Be aware that threats can come from within your organisation as well as from outside it.

Do not forget to invest not only in the technology, but also in your employees.

Implementation of Cyber Security Programme



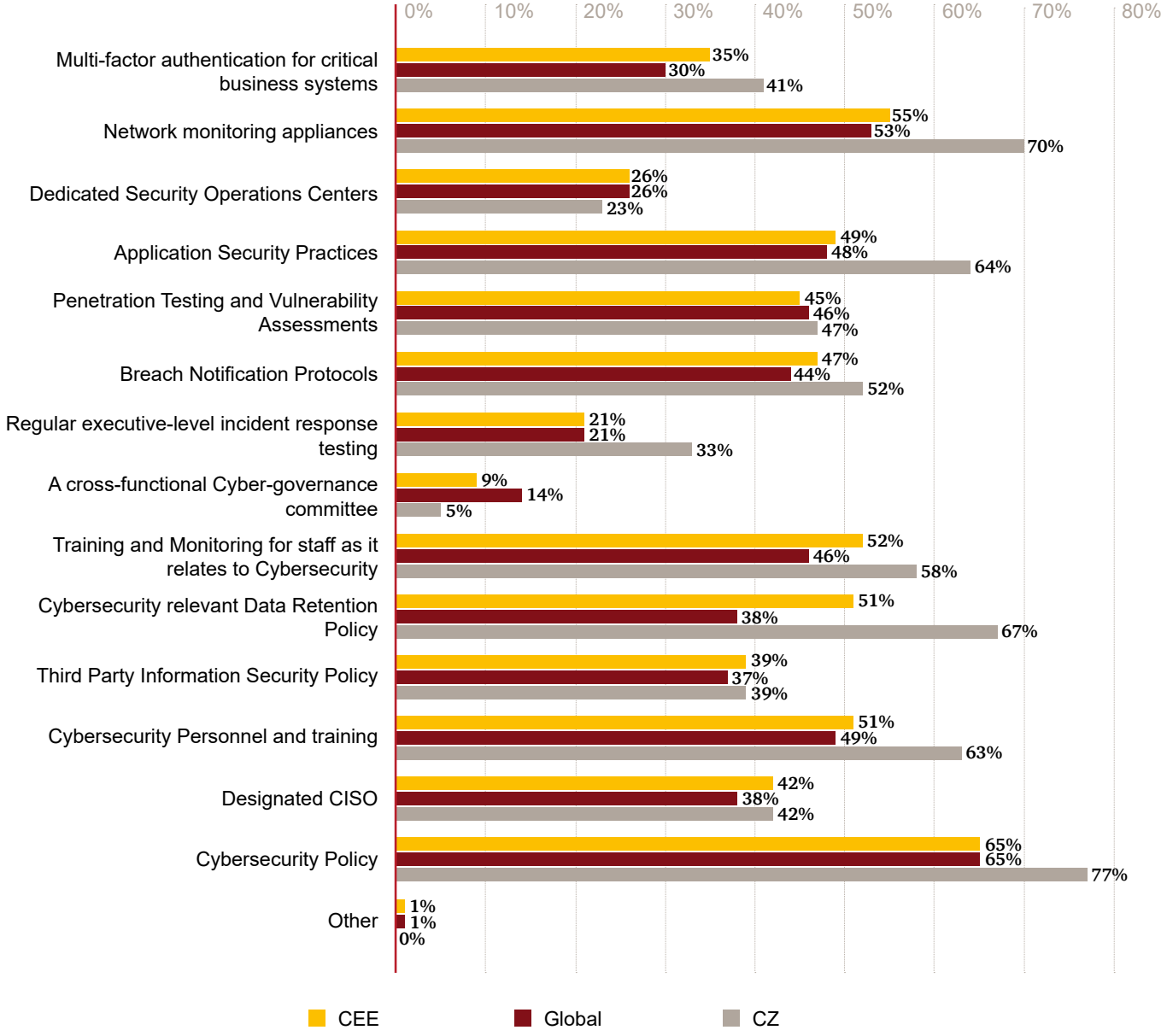
What is the reality in the Czech Republic? 88% of Czech respondents claim their organisation has implemented a Cyber Security Programme to deal with cyber-attacks. Global results, on the other hand, suggest that only 59% of organisations globally have a Cyber Security Programme in operation.

While the 88% alone says nothing about the efficiency of the Cyber Security Programme implemented by these respondents, it is promising to see that Czech companies are well aware of the cybercrime risk and the necessity to take actions to guard the business against its negative consequences.

Compared to the CEE and global results, Czech companies appear to have one of the most developed security systems. In particular, they have implemented data retention policies, network monitoring appliances and application security practises. However, Czech companies lag behind their CEE counterparts in two areas: in the set-up of dedicated security operation centres and establishment of a cross-functional cyber-governance committee.

Indeed, creating a specialised centre requires considerable time and money as well as ongoing monitoring in order to achieve high effectiveness. Many organisations simply do not want to make such an investment until the "business case" is there. A cyber-governance committee, on the other hand, is usually composed of senior executive business managers and reports to the board. Generally, a cyber-governance committee is effective in increasing the overall governance of security risks and facilitate the alignment of corporate objectives with security requirements.

Which of the following are elements of your Cyber Security Programme?



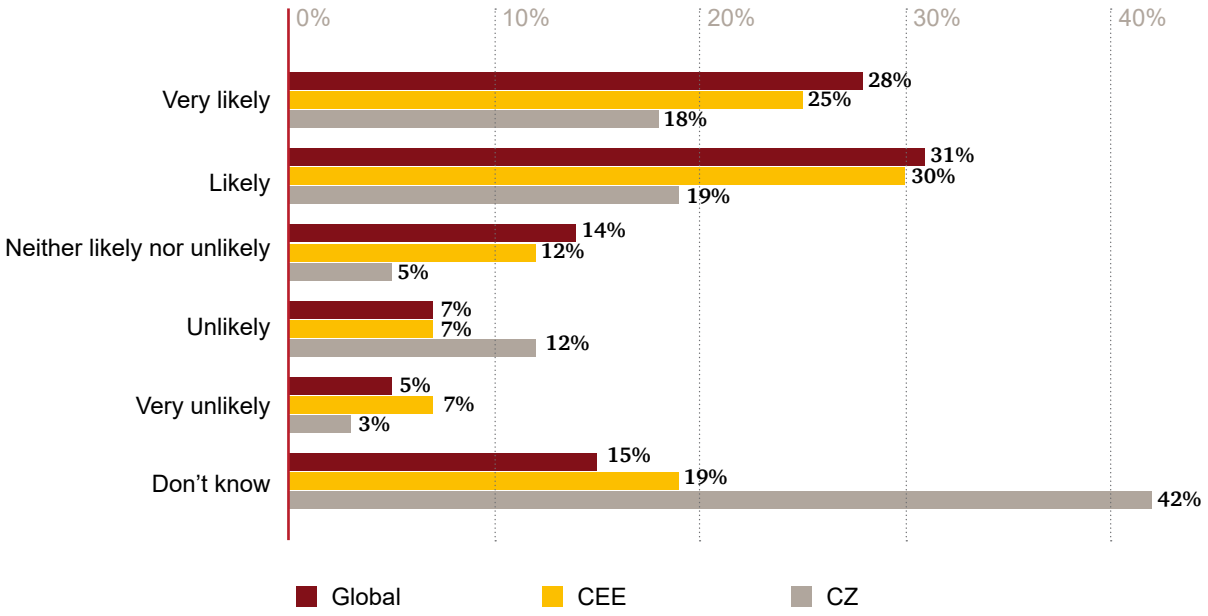
Are companies willing to report cyber-attacks to government or law enforcement agencies?

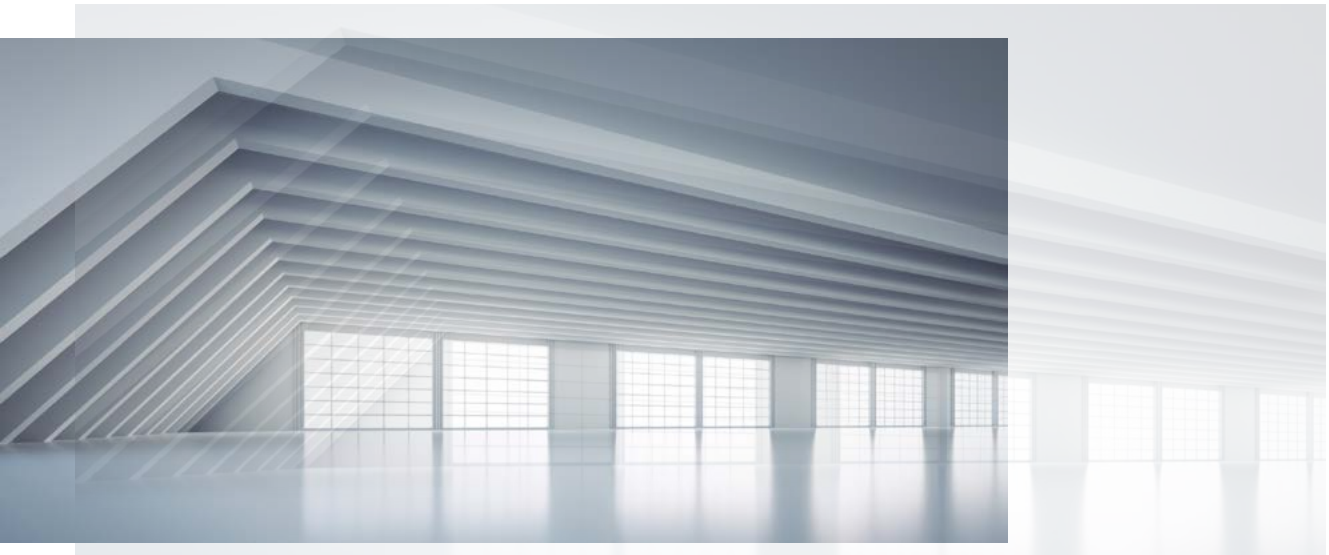
Imagine that your client's database or the personal details of your employees were stolen. Would you report such an incident to the respective regulatory body, such as the Office for Personal Data Protection?

When certain conditions are met, companies need to notify regulatory bodies or other government agencies about such events. If the company fails to notify a government agency and the fact that the data was stolen comes to light later, this can have a serious negative impact on the company, ranging from a fine from a regulatory body to lawsuits filed by clients.

This year's results indicate that Czech companies do not have trust in government or law enforcement agencies with respect to reporting cyber-attacks. Only 37% of respondents would very likely or likely share information with government/law enforcement agencies, whereas at the global level it would be more than a half.

How likely will companies share information about cyber-attacks with government agencies?





Czech respondents stated particularly the following three reasons for not reporting cyber-attack to governmental agencies: risk of uncontrolled public disclosure (64%), lack of trust that the enforcement agencies have the required expertise (50%) and legal privilege not to share information (50%).

Only 37% of Czech companies stated they would report a cyber-attack or suspicion of one to a government or law enforcement agency.

What types of cyber-attacks should be reported and why?
"Cyber-attacks which will lead to leakage of personal data or attacks aimed at the critical infrastructure of the state per Act 181/2014Coll."

How do you explain it?
"Attacks, which are not aimed at the above-mentioned assets, do not have to be reported. Companies usually tend to keep these events secret in order to prevent harm to their reputation."

Is there something the government should do to change this?
"I do not think so. Companies should deal with their cyber security for their own self-prevention, not because of the regulations."

Michal Čábela,
Head of Cyber Security team, Risk Assurance

What is the key to successful investigation of data leakage?

"It is essential to have a proper response plan in advance. Very often, organisations are thrown into panic, making quick decisions, leading to loss of important evidence. Companies fail to look beneath the surface, believing that a simple internal security review will fix the issue. Often, the actual root causes and the full extent of the breach remain undetected. Knowing what to do first, who to contact and how to communicate are the key factors for successful data leak investigation."

Pavel Jankech,
Director at Forensic Technology Solutions in Czech Republic

Interview

Michal Čábela

Head of Cyber Security team, Risk Assurance, PwC

Q **What are the main risks in the area of cyber-crime that Czech clients mainly face nowadays?**

A If you would compare the number of cyber-attacks on an employee from the Czech Republic with the number of cyber-attacks on an employee from Western Europe, then from such a comparison the Czech Republic would appear to be the safer country. However, this would result from the fact that in the Czech Republic there is a lower concentration of big companies that are the frequent target of cyber criminals.

In the last 12 months, we encountered several trends in the area of cybercrime. One of these trends arose from the growing price of Bitcoin and other cryptocurrencies, which lead to an increase in unauthorised mining of these currencies from hacked computers.

Another trend is the increased number of ransomware attacks (blackmailing malware cyberattacks). This type of attack encrypts computer discs and criminals blackmail victims in order to obtain financial funds or cryptocurrencies (usually Bitcoin). In my opinion, this trend will continue in the future.

Q **What do you currently consider as the most dangerous type of cyber-attack(s)?**

A It depends on the point of view. For the individual, the most dangerous is ransomware, which can delete all the digital memories of the individual. For the company, ransomware might represent a lower threat, but only under the condition that the company has advanced tools for detection and regular data back-ups.

For some companies, the most dangerous is a DDOS (distributed denial of service) type of attack, which might in critical moments disable access to key information (for example the result of an election). It always depends on the type of the company. Sophisticated cyber-attacks on chemical companies or infrastructure might even endanger the health and lives of people. This type of attack is usually planned for a longer time and the aim is to harm critical infrastructure of these companies such as industrial control production systems.

Unfortunately, what we observed in practise is that the key systems of the companies are usually not well protected and thus it is not so difficult for hackers to attack them.

Q **Our survey noted a lower occurrence of cybercrime in the Czech Republic compared to previous years. From your experience, has cybercrime really decreased? If not, how do you explain it?**

A The question should be, has the level of cybercrime in the Czech Republic really decreased or has the level of cybercrime sophistication increased in such a way that only the number of detected cyber-attacks has decreased. Nevertheless, it is important to say that level of security of the Czech companies is continually increasing. The remaining question is, does the increase in the level of security correlate with the increase of the sophistication and number of cyber-attacks.

Q **Czech companies reported phishing attacks considerably more than other CEE countries. Why are the Czech companies an easy target?**

A Czech environment still lacks sufficient education. Employees are always the weakest part of cyber-security and that is why phishing attacks are still very successful. From my experience, the average success rate of the phishing campaign is 30% of employees. Therefore, in the company that has 1,000 employees, 300 of the employees will click on an infected email and just one click of the one employee is enough to spread the infection.

I would encourage companies to invest in cybercrime education for employees, although not at the expense of the technical security. You can have several alarms installed in your car, but if you leave the keys in the door then someone will steal it.

III. Managing fraud in the Czech Republic

Maintaining in-depth knowledge of fraud taxonomy and how fraud risk can be minimised if not eliminated should be essential for every business.

Prevention of fraud

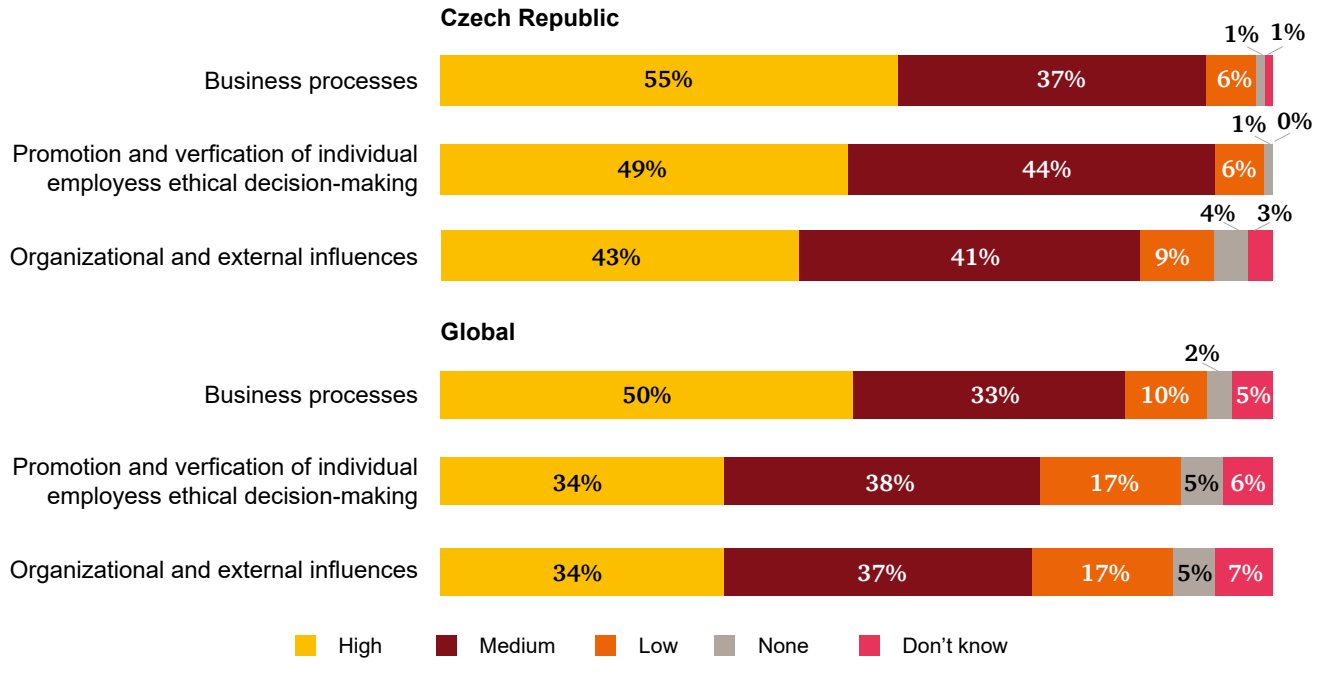
Preventing fraud is usually the preferred option. In the long term run the related costs are lower that the costs for investigation, remediation and recovery and other negative implications relating to fraud that already happened.

A good prevention programme should be built on several pillars, including but not limited to tone from the top and middle, culture of fraud awareness, robust internal control procedures, safe whistleblowing system and continuous education of employees about the importance of fraud prevention.

The foundation for fraud prevention should be a robust and regularly performed fraud risk assessment that identifies the key risks faced by an organisation. According to the results of our Survey, 93% of respondents' organisations performed a fraud risk assessment in the period of the last 24 months and they focused mainly on the following three areas: general fraud risk assessment, cyber-attack vulnerability, and anti-bribery and corruption.

We consider it surprising that 7% of Czech respondents still do not perform any risk assessment at all. Nevertheless, this corresponds with the global average of 10% of companies not performing any risk assessment.

What level of effort do organisations apply in the following categories in order to combat fraud internally?



How are incidents of fraud initially detected?

While it is not possible or economically feasible to implement measures to prevent all fraud risks, attention should be paid to an effective system of detection mechanisms.

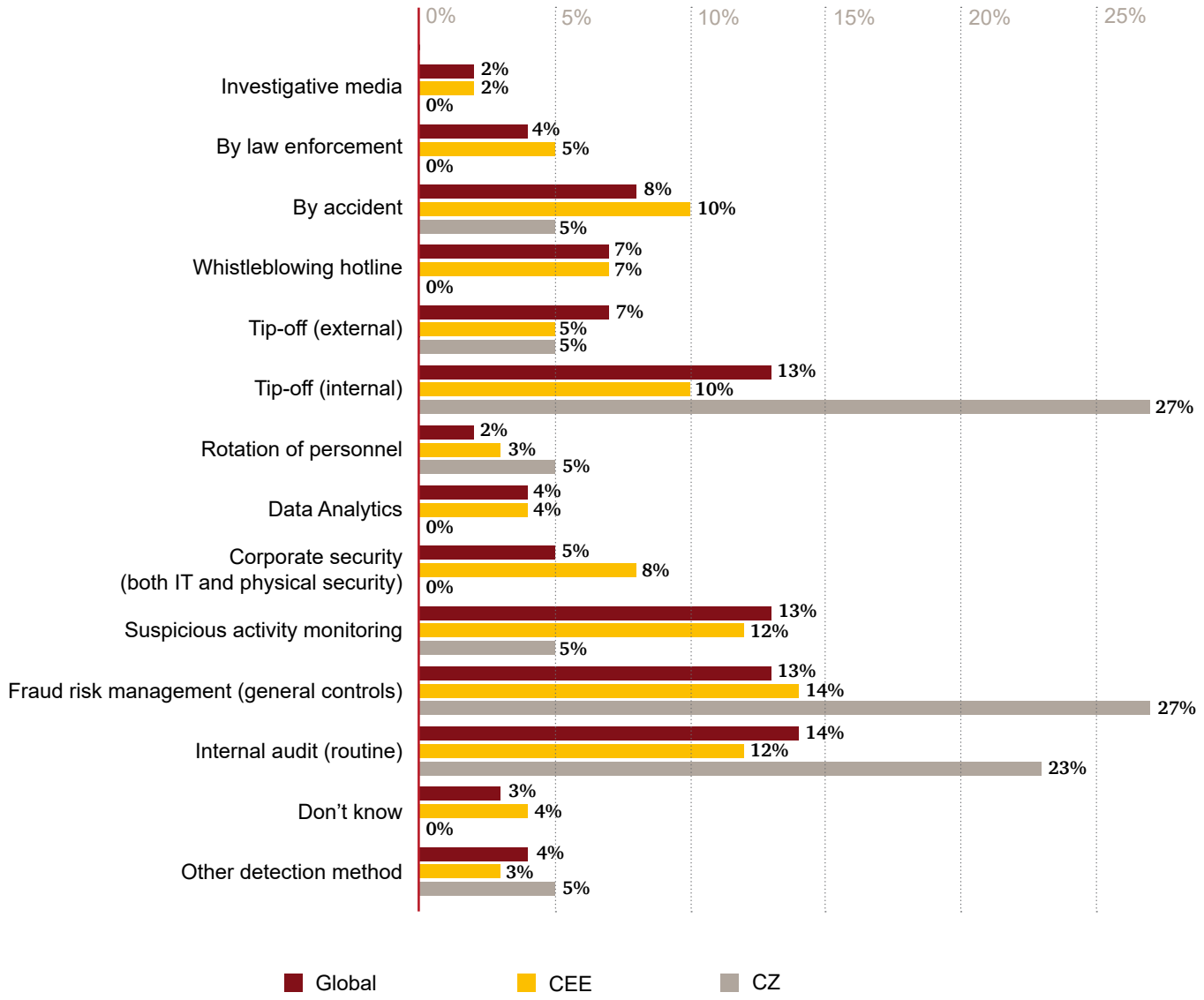
Fraud detection techniques used in companies globally include in particular regular transaction monitoring, fraud risk management controls and internal audits, both regular as well as spot audits.

50% of most disruptive frauds or economic crimes in the Czech companies were detected either through general controls of fraud risk management or internal audit routines. It is very promising and encouraging for internal control functions such as compliance, internal audit or fraud risk teams to see that a well-established corporate culture can pay off.

Nevertheless, a tip-off still plays an important role in fraud detection, with more than one quarter of fraud cases being detected via internal tip-offs compared to 5% via external tip-off.

The Survey also shows that other methods such as a whistle-blowing hotline or data analytics are, in comparison with global results, not as utilised in the Czech environment.

How were incidents of fraud initially detected?



Role of whistleblowing in fraud detection

While **Czech companies reported that none of the fraud cases** were detected **by a whistleblowing** mechanism, 7% of both CEE and global companies were notified about fraud happening in their companies via a whistleblower hotline.

There might be various reasons for this, including but not limited to historical connotations or negative consequences for whistleblowers in past years or non-existing anonymous reporting mechanisms. Even though general legislation protecting the whistleblowers is in place in the Czech Republic, there are examples where the whistleblowers were dismissed from their positions due to other reasons sometime after blowing the whistle.

According to Transparency International, whistleblowers play a crucial role in the detection of corruption, fraud and mismanagement. On the other hand, little legal protection of whistleblowers, insufficient investigation of their claims and ineffective mechanisms for internal reporting can discourage people from speaking out. [3]

Czech companies use less technologies to detect fraud than their CEE counterparts

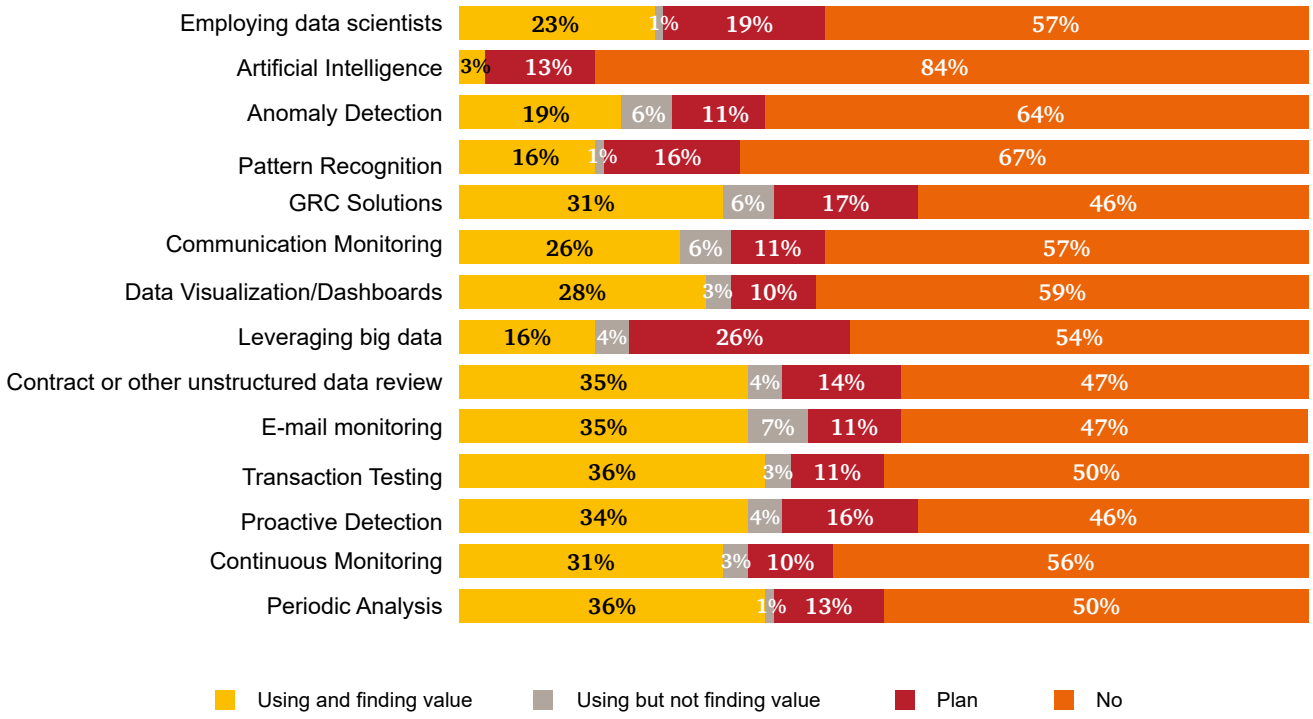
Fraudsters are becoming more sophisticated and strategies used to detect fraud a few years ago are becoming outdated. Without fully utilising the potential of available technologies, companies will struggle to fight fraud effectively.

It seems that organisations in the Czech Republic are rather reluctant to or sceptical about using modern technologies as an instrument to combat fraud and economic crime. Approximately **30% of Czech respondents use the majority of the below-listed technologies** and another 14% of respondents plan to implement them – compared to 37% and 18% at the CEE level and to 36% and 22% at global level.

It is worth pointing out that we observed an inconsistency in the Czech respondents claim to use a wide variety of technology and data analytics solutions in order to detect fraud (see chart below). However, there is no evidence that these solutions have actually resulted in the detection of any cases (see chart "How were incidents of fraud initially detected").

In our opinion, there are at least two potential explanations for this discrepancy: either the different terminology used in the two questions has led to misclassification of detection methods by respondents or the systems implemented by Czech companies are not fully effective in detecting fraud.

Use of technologies in combating fraud in the Czech Republic



[3] www.transparency.org/topic/detail/whistleblowing

Proactive detection methods (currently used by approximately 40% of our respondents) are widely used especially in the financial sector, where they allow reviews of hundreds of thousands of transactions, spot irregularities and send automated alerts. Another sector that benefits from the proactive detection methods is the telecommunication industry. This gives the benefit of screening almost all if not the entire population of transactions and leaves more time for the actual investigation, which can lead to better understanding of the biggest threats businesses face.

Another technology commonly used by the surveyed companies are reviews of unstructured data. In other words, data that cannot be analysed in a traditional row-column database – such as contracts or e-mail messages - 39% of companies in the Czech Republic are already using review of contracts or other unstructured documents. Regular contract reviews are one of the procedures used to prevent procurement fraud, alongside the rules on the conflict of interests, separation of duties or due diligence of suppliers.

Artificial intelligence, pattern recognition and big data are used relatively scarcely (3%, 17% and 20% respectively) in the Czech Republic, although more companies plan to implement them in the future.

How can artificial-intelligence-based solutions help to combat fraud? One of the examples can be a tool that will simulate the work of an internal auditor – examine every uploaded transaction, every user, every amount and every account to find unusual transactions or transactional patterns in the general ledger. A simpler solution can be a model of pattern recognition programmed to look for repeated withdrawals or transfers. Such a model can spot cases where the amounts do not perfectly match or that do not reach the 'materiality' level to catch the attention of an internal auditor.

In comparison, **13% of companies in CEE have embraced artificial-intelligence-based solutions** to combat fraud, 29% are using pattern recognition and 30% are leveraging big data.

What is the reason behind the considerable difference between the Czech Republic and other CEE countries? Is it a lower level of knowledge about up-to-date techniques or limited financial resources that companies are not willing to invest until they have a "business case"? What would encourage companies to fully utilise the potential of new technologies?

Interview

Martin Diviš

Partner, Tax Services, PwC

One of the fraudulent issues that was not specifically asked in our Survey, but many companies face it, is a VAT fraud. Victims can be honest taxpayers, used as buffers, who are unaware of the fact that their counterparties are fraudsters. Since tax authorities have been increasing their efforts in effective tax audits, companies should understand that a proactive attitude is the solution to avoid the potential negative implications of being unknowingly involved in a VAT fraud scheme.

Q **How big is the risk of the VAT fraud in the Czech Republic (and which industries are the most affected)?**

A Companies actually do underestimate a significant risk of being dragged into VAT fraud scheme. We have seen many cases in which the companies were rejected the input VAT or were asked to provide guarantee for VAT unpaid by its supplier. Czech tax authorities have implemented list of unreliable VAT payers, currently containing more than 10 thousand VAT payers. If any company is trading with these "black-listed" third parties, it needs to be very careful, since it becomes jointly VAT liable.

Q **How do the authorities react and what are the consequences for the company involved in VAT fraud?**

A Tax authorities apply rather formalistic and strict approach. As all VAT payers need to submit control statements with the tax authorities (alternative to SAF-T reporting), tax authorities are supplied with very detailed information about major transactions. They do cross-check analysis of these reports and in addition use also other methods. In case they take view that the company could be part of the VAT fraud (either directly or even indirectly involved), they take quite radical steps to secure VAT. VAT payers can be held jointly liable in case they knew or should have known that the company's supplier will not pay an output VAT. Or the tax authorities may reject input VAT recovery. There are also number of cases in which the tax authorities took measures that practically lead to closing of the company's business. All VAT payers need therefore to very thoroughly check who their suppliers are. It is not sufficient to say that the company has good experience with the particular supplier."

Q **Q: How can companies effectively detect it?**

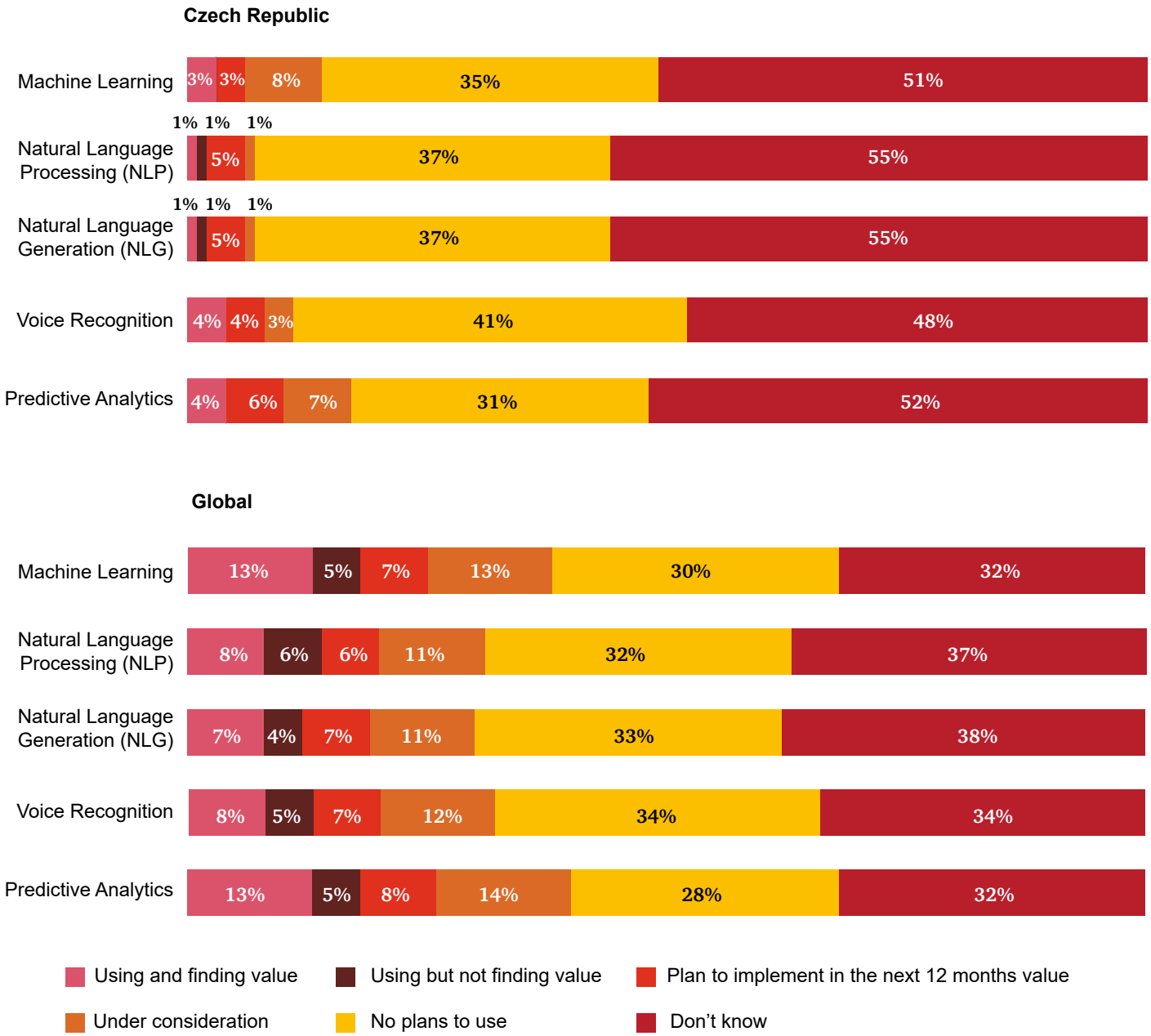
A There is actually not too many economically reachable measures that the companies can take in order to detect risk of potential VAT fraud. They should, however, make sure they do not become part of it. It is necessary to check all active suppliers on regular basis to evaluate the potential risk. Since manual check of all available sources is time consuming, an automated solution that checks number of different sources and provides risk scoring of suppliers is highly recommended. Further they should also check whether they do not purchase goods for unjustifiably low price than is usually on the market. The results of such checks should be properly documented so they can be used as a prove of performed controls in case of future tax audits.

Are you using the full potential of artificial intelligence and advanced analytics?

As mentioned earlier, particularly in the use of artificial intelligence or advanced analytics, Czech companies are falling behind their CEE counterparts. For example, according to our Survey, only 3% of Czech respondents use machine learning, compared to 17% across CEE and 18% globally.

The situation is also similar with other technologies such as voice recognition, predictive analytics, natural language processing and natural language generation.

To what degree is your organisation leveraging Artificial Intelligence or Advanced Analytics to combat/monitor for fraud and other economic crimes?



Interview

Pavel Jankech

Director, Forensic Technology Solutions, PwC

Q **What do you consider the biggest change in technologies used for combating fraud over past couple of years?**

A The technology is advancing at a quick pace. With a massive increase in computational power, Artificial Intelligence is getting into many different areas of human life. Machines now can recognise objects or translate speech in real time. Technology is really getting smart. Not surprisingly, there are also interesting advances in the area of detection and prevention of fraud. Automatic scanning of license plates on cars or facial recognition in airports and train stations to search for potential criminals and missing persons, does not surprise anyone nowadays. There is even a technology trying to predict if an individual will commit a crime before it happens. This technology uses facial recognition and movement analysis to find and track individuals. The system will detect if there are any suspicious changes in behaviour or unusual movements. For example, if an individual seems to be walking back and forth in a certain area repeatedly, then that is an indicator that the individual might be a pickpocket or casing the area for a future crime. I am sure those examples sound really interesting and exciting; however, those examples are not very relevant to the corporate sector in our region. Nevertheless, even there, technology advances and new types of analytical solutions arise.

Q **What is your opinion on use of Artificial Intelligence (AI) and Advanced Analytics in monitoring fraud?**

A Let me first define what I understand the term AI to mean. In simple terms, it is an activity where a computer is doing activities that are thought to require human intelligence in order to be performed. Examples may be understanding language and responding, recognising faces or subjects in photos, driving a car, or guessing what movie we may like to watch based on our previous experiences. In fraud detection, AI can help identify unusual patterns or outlying transactions that may be fraudulent.

AI is not a programme that searches automatically for red flags based on pre-defined rules, or that compares transactions to fixed scenarios, even though such products are marketed as Artificial Intelligence.

AI will ultimately be the future of fraud prevention and fraud detection systems in every company. Now, however, artificial intelligence struggles with a profound limitation: it needs a lot of data to learn about the world. Therefore, for AI to be successful, it requires a domain where we can acquire a lot of data. Big technology firms like Google and Facebook have access to mountains of data, making it much easier to create useful tools. When it comes to fraud, AI is thus far mostly used in the banking sector or in retail with large numbers of transactions.

Q **In what ways can machine learning be used in detecting or preventing frauds?**

A A human reviewer or investigator can review only a limited number of inputs at a time and make a decision. Current products on the market help by pre-filtering the inputs or red-flagging events. However, when there is enough data available for further review that is when machine learning is relevant. It can analyse thousands of different inputs and scenarios and look at probabilities of fraud. True AI is not limited by fixed rules, thresholds and scenarios. It learns from what a human reviewer confirms as suspicious or fraudulent, and tries to identify other such events, even creating its own scenarios or modifying thresholds to adapt to a changing environment. So not only will it save time by going quickly through a lot of data, but also highlight new types of fraud, new trends and new unusual behaviour to a human investigator.

Q **What is the most effective way for companies to prevent and detect crime when talking about technologies?**

A A key challenge with fraud detection is the dynamic nature of fraud. Fraudsters adopt and try to beat detection and prevention mechanisms by developing new methods and strategies. Therefore, adaptive analytical models and detection and prevention systems are required in order to detect and resolve fraud as soon as possible. Detecting fraud as early as possible is crucial.

Q **Our Survey shows that, in comparison with CEE, Czech companies are quite reluctant to use technologies as an instrument to prevent or fight fraud. From your experience, would you agree with this and what might be the reason for this?**

A Many companies still do not use analytical fraud detection techniques. Most still rely on an expert-based approach, building on the experience, intuition and business knowledge of the fraud analyst. Such an expert-based approach typically involves a manual investigation of a suspicious case, which may have been signalled for instance by a customer complaining of being charged for transactions he did not do.

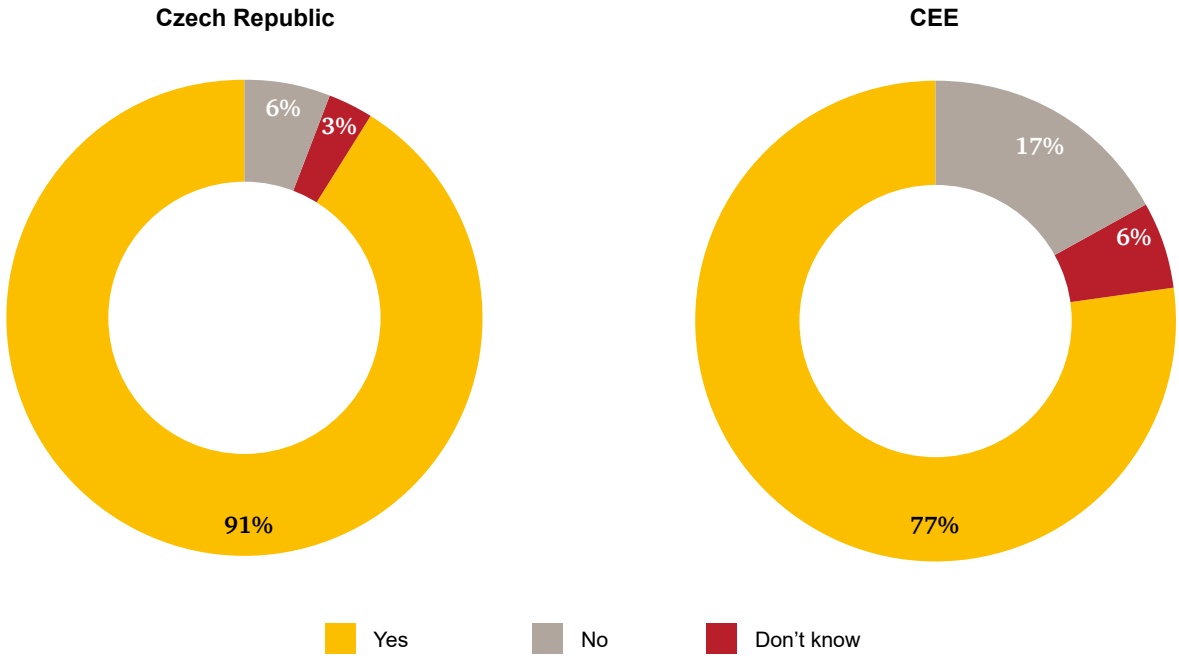
Even though true AI, in its current state of technology and at current costs, is not the best fit for everyone, I believe that adding an automation layer to fraud detection and prevention can save an investigator time and the company money. Products that highlight suspicious events, vendors or transactions are already common in western parts of Europe and are now quickly spreading to CEE, with all its language, legal and cultural specifics. Such tools (various “health checks” or “fraud tools”) are now mature and affordable enough even for our mid-sized companies.

I agree that Czech companies are relatively slow at adopting such tools, though I do not know the reason. I believe we can expect broader expansion of their usage in the coming years.

IV. Ethics & Compliance

It is very positive to see an increasing number of Czech organisations that realise the importance of ethics and compliance programmes. While in 2016, 86% of respondents had a formalised compliance programme, nowadays 91% of Czech companies reported that they have implemented formal ethics and compliance programmes.

Have you implemented formal ethics and compliance programmes?



This is significantly above the CEE and Global (77% both in CEE as well as globally).

Who is primarily responsible for the ethics and compliance programme? In the Czech Republic, they are under the responsibility of a chief compliance officer (34%) or chief executive officer (25%). The same also applies to their counterparts in CEE and globally, where the person primarily responsible for an ethics and compliance programme is the chief compliance officer (33% in CEE and 30% globally) or chief executive officer (20% in CEE and 17% globally).

The key to success is that compliance and business ethics programmes are not only on paper, but they are an integral part of the day-to-day business operations and compliance with the programme being monitored. It is therefore very positive that 89% of Czech companies review their compliance programmes as part of internal audit assignments and 54% established regular management reporting.

Why bother with procedures and policies?

Strong anti-fraud policies should be incorporated into the corporate code of conduct, as it will set the right tone from the top and the middle, showing that company will not tolerate any instances of fraud or other misconduct. An anti-fraud policy is strong if it is lived and breathed throughout the organisation: if each and every suspicion or allegation is properly reviewed, investigated and disciplinary procedures, if applicable, are taken independent to suspect's identity. Such a policy and corporate behaviour can deter those who are tempted by an opportunity to commit a crime and, it will provide guidance to the employees on how to properly handle the situation when fraud actually occurs.

A strong anti-fraud policy defines which kind of behaviour is not acceptable in the company and it also specifies who in the company should be notified about suspicion events, who is responsible for the investigation and to whom and when the results are reported. They also serve as good fraud prevention tools as they usually contain processes and specify controls that will help to prevent the fraud cases.

It is pleasant to see that most of the Czech surveyed companies appear to have specific policies in place on dealing with general fraud and bribery & corruption (63% and 61%, respectively). Overall, in comparison to CEE, Czech companies are more likely to have specific anti-fraud policies embedded in their ethics and compliance systems than are their regional counterparts.

According to the Czech respondents, on average:

90%

have in place specific policies or tailored controls against general fraud and bribery & corruption

80%

have policies or controls regarding industry specific regulatory compliance

70%

have policies or controls regarding anti-competitive/anti-trust and cyber behaviour

50%

have policies or controls regarding sanctions and export controls and AML

V. Will the future be bright?

Most organisations nowadays are well aware that one of the key fraud prevention tools is the screening of their third parties such as suppliers, subcontractors, or clients, as it is necessary to assess the risk resulting from co-operation with them.

Such risk can include but is not limited to financial loss resulting from cooperation with a fraudulent third party, reputation risk, risk of being connected to a corruption scheme or VAT carrousel fraud.

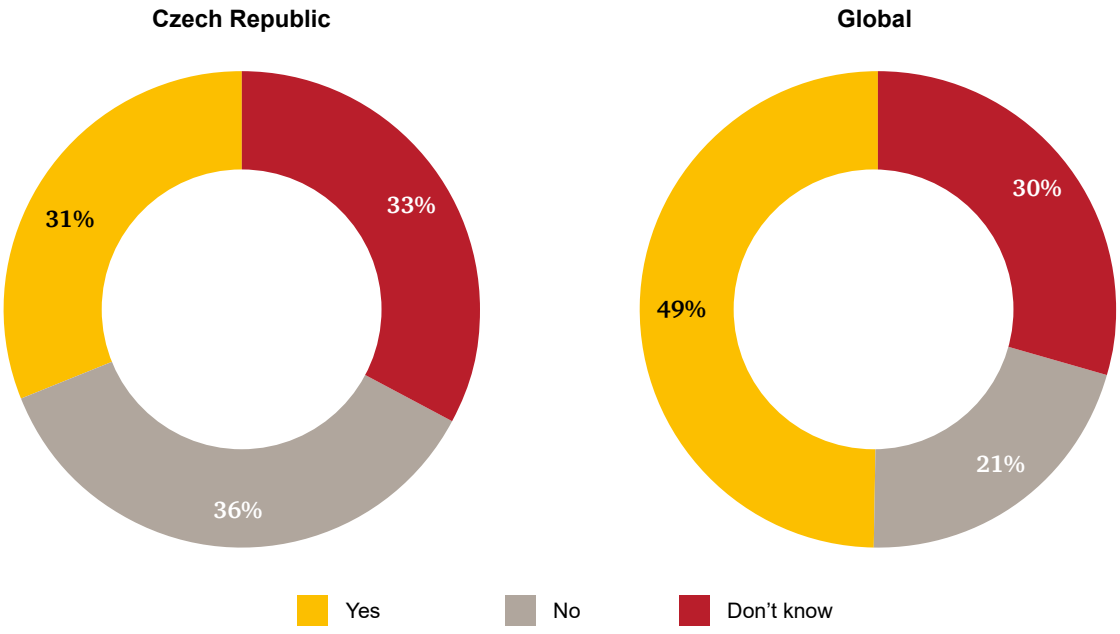
However, the key limitation that organisations face is the lack of independent information about ultimate beneficiary owners so they do not have to rely on information self-reported by those third parties that are subject to the screening.

Therefore, one of the questions we asked in our Survey is "Would the implementation of the Global Beneficial Ownership standards be beneficial to your organisation in combating economic crime?"

Czech respondents appear to be quite sceptical with respect to the implementation of Global Beneficial Ownership standards in comparison with the global respondents.

Only 31% of Czech companies believe implementation of the standards would be beneficial in combatting economic fraud. While global results show that 50% of respondents believe the implementation of such standards would be beneficial for their organisations.

In your business/industry, would the implementation of Global Beneficial Ownership standards be beneficial to your organization in combatting economic crime?



With the above in mind, it is noteworthy that, as of 1 January 2017, the Czech Republic encountered a novelisation of the Anti-money laundering Act which amongst other things established the "Register of the beneficial owners of legal entities and trust funds located in the Czech Republic", which will be held by respective register courts. Even though only information about the identity of the beneficial owner will be publicly available, the full information set will be accessible, under certain circumstances, to state authorities, courts, prosecutor's offices, tax administrators, entities who are subject to Anti-money laundering law and other relevant institutions, who will be able to prove their rightful entitlement.

You can find more about this topic in the interview with Petr Kincl from PwC Legal.

Interview

Petr Kincl

Managing Associate, PwC Legal

Q **The Czech AML Act was novelised with respect to the ultimate beneficial owners effective since 1 January 2017. What are the key changes in this area for the obliged companies?**

A The amendment extends the definition of obliged entities. In addition, the limit on cash payments to determine the liable person was reduced from € 15,000 to € 10,000.

Newly introduced was the duty of the obliged entities to identify and assess the risks of money laundering and terrorist financing. However, the main change is the establishment of the Register of Beneficial Owners.

Q **What is the purpose of the Register of Beneficial Owners and which companies will have to file information with this register?**

A The Register will collect information about the beneficial owners of all legal entities and trusts. The public bodies and the obliged entities will thus have a tool how to check who the beneficial owner is and confirm information provided by their clients.

All business companies, cooperatives and other legal entities that are registered in the Public Registers and trusts will be obliged to identify and register their beneficial owners.

Q **What type of information will have to be disclosed and what is the deadline for placing information into the Register of Beneficial Owners?**

A Basic identification information, i.e. name, surname, residency address, date of birth (and the birth number in case of Czech citizens) and nationality, and information on the share of voting rights or share of proceeds to be distributed from the entity. Deadline for placing relevant information is 31 December 2018.

Q **What are the potential consequences for companies if they fail to disclose the required information by the deadline?**

A There is no specific sanction stipulated by law. However, an entity failing to disclose its beneficial owner(s) will expose itself to the risk of suspicion in the context of AML. Further, it will be limited when participating in public procurement tenders and / or during bankruptcy proceedings as a creditor.

Q **Will the Register of Beneficial Owners be publicly available?**

A No, however public bodies and the private obliged entities will be able to access the relevant information.

Q **In your opinion, will the establishment of the Register of Beneficial owners help in combatting economic crime in the Czech Republic?**

A I do not believe it will have any substantial effect. There will still be ways to hide the real beneficial owners.

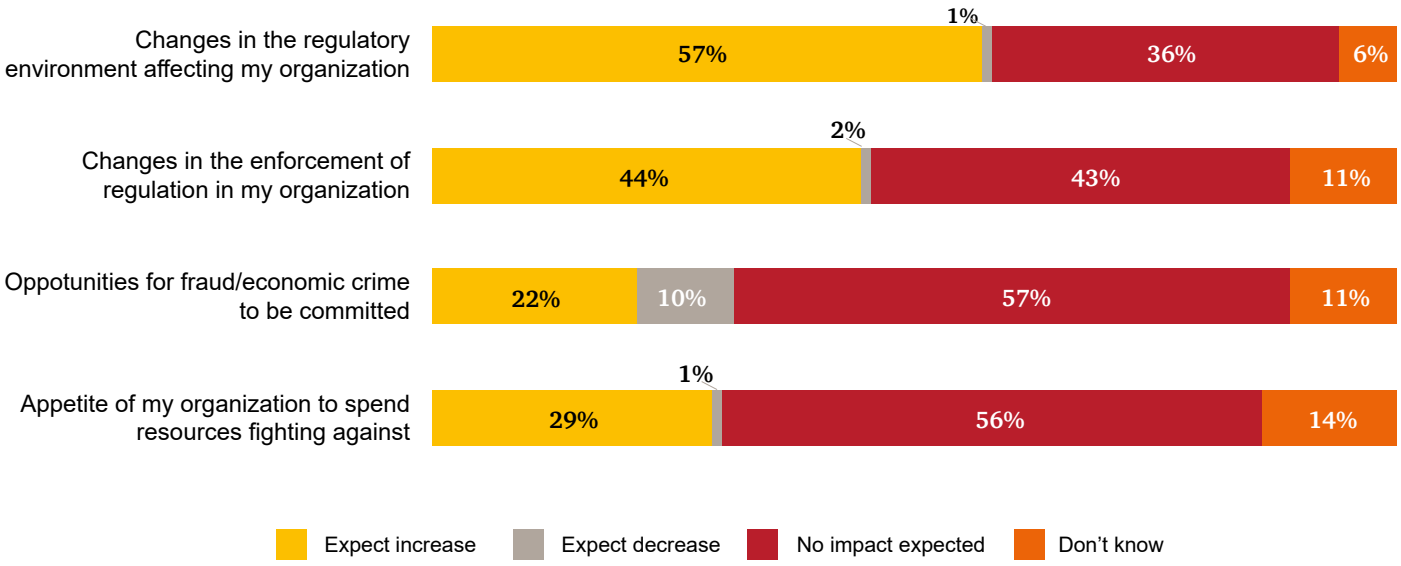
What are your expectations?

Similar as in previous Surveys, we asked respondents about their expectations for the next 24 months. It is interesting to see that the Czech companies believe cybercrime and asset misappropriation would be the most disruptive economic crimes in terms of the impact on their organisations in the next 24 months.

What are the expectations of Czech companies in relation to the changes in the geopolitical environment in the next 24 months?

- 57% expect an increase in the regulatory environment;
- 44% expect an increase in the enforcement of regulation in their organisation; and
- only 21% expect an increase in opportunities to commit fraud due to the impact of the changes in the geopolitical environment and 10% expect these opportunities to decrease.

How will recent changes in the geopolitical environment impact your organisation in the following ways over the next 24 months?



Contacts

In case you would like to discuss anything from the Survey or you have any questions for us, we are fully at your disposal.

Sirshar Qureshi
Partner, CEE Forensic Leader
sirshar.qureshi@pwc.com

Liviu Chirita
Director, Financial Crime
liviu.chirita@pwc.com

Pavel Jankech
Director, Forensic Technology Solution
pavel.jankech@pwc.com

Kateřina Halásek Dosedělová
Senior Manager, Forensic Services
katerina.halasek-dosedelova@pwc.com

Prague
Hvězdova 1734/2c, 140 00 Praha 4
Tel.: +420 251 151 111 Fax: + 420 251 156 111

Brno
nám. Svobody 20, 602 00 Brno
Tel.: +420 542 520 111 Fax: +420 542 214 796

Ostrava
Zámecká 20, 702 00 Ostrava
Tel.: +420 595 137 111 Fax: +420 595 137 611