Global Economic Survey 2016

Czech Republic

www.pwc.com/cz

35%
companies experienced one or more incidents of economic crime

36%
of incidents were cybercrime

pwc

Table of Contents

The 2016 Global Economic Crime Survey was carried out by PwC. It is the largest survey of its kind with 6,337 survey participants from 115 countries, including 79 companies in the Czech Republic.

The survey is intended not only to describe the current state of economic crime but also to identify trends and perception of future risks.

Preface

We are pleased to present to you the results of 2016 PwC Global Economic Crime 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 6,337 organisations from 115 countries, including 79 leading companies within the Czech Republic.

This year's survey again draws attention to cybercrime, which was considered a completely new form of economic crime a couple of years ago; however, it has recently become a primary topic of any fraud-related discussion. No company is immune – cybercrime affects organisations irrespective of industry and geography. Apart from cybercrime, the survey turns the spotlight on the ethic and compliance area. In light of the continuously growing globalisation of the business environment and increasing enforcement, compliance has become a prominent topic.

This report also explores the theme of opportunity – not only those opportunities that enable economic crimes to be perpetrated, but, more importantly, the opportunities available to organisations to proactively counter economic crime while balancing their legal responsibilities.

We invite all entrepreneurs and managers to read through the report and to draw conclusions relevant to their undertaking. A global report and local variants for different countries are available to help companies doing business globally. We believe that the results of our analysis will allow companies to better understand the significant impact that economic crime can have on their business, assess the risks of fraud that they may face, and find ways to mitigate those risks.

Last but not least, we would like to thank the survey participants who were kind enough to share their observations of fraud and provide their insights. We are especially grateful to the responding entities from the Czech Republic. All the respondents share our belief that economic crime is too costly to be ignored.

Sirshar Qureshi,
Partner responsible for Forensic Services in CEE, PwC

The highlights

The current fraud environment in the Czech Republic

Economic crime continues to be a serious issue affecting organisations worldwide, across Central and Eastern Europe ("CEE") and in the Czech Republic. In the past 24 months 35% of companies in the Czech Republic experienced one or more incidents of economic crime, which is comparable to the average for CEE (33%) and globally (36%).

Compared to the previous surveys, the occurrence of overall reported economic crime has dropped by 13 percentage points, however we should not be optimistic when drawing conclusions. In the context of the evolving risk landscape, organisations might face sophisticated fraud schemes, which remained undetected for several years. These latent and long running fraud cases represent more dangerous and costly threats for companies than one-off incidents.

Traditionally, the most common type of economic crime in the Czech Republic is asset misappropriation (61%). Asset misappropriation has been traditionally seen as the easiest to detect compared to other types of economic crime, thus its prevalence from year to year is generally predictable.

Apart from asset misappropriation, the top four types of economic crime reported by our survey participants include cybercrime (36%), procurement fraud (25%), bribery and corruption (21%) and accounting fraud (21%).

Most of the fraud in the Czech Republic is detected by various means of corporate control (in total 68%). However still almost one in five fraud cases is detected beyond the influence of management, out of which the most typical way is simply detection by accident (14%).

According to the 2016 survey, the share of external perpetrators (54%) on committed fraud is slightly higher when compared to internal perpetrators.

In the past 24 months 35% of companies in the Czech Republic experienced one or more incidents of economic crime

Cybercrime

More than one third of the respondents in the Czech Republic, that suffered an economic crime, reported that they have experienced cybercrime. This is slightly above the CEE results and global average. If there should have been one take away from this survey, it should be the change in perception of cybercrime – cybercrime is no longer just an IT problem, rather, it should be considered a fundamental business problem.

According to our previous surveys, the trend in the occurrence of cybercrime is increasing. The reported occurrence has increased from 13% as reported by the survey participants that suffered economic crime in 2011 to 36% reported in 2016. This is no surprise in the changing business ecosystem when the vast majority of documents, communication and transactions has gone digital.

According to the survey participants from the Czech Republic cybercrime is considered to be the biggest threat and its occurrence in the next 24 months is likely or so say more than one third of the respondents. Moreover, 57% of surveyed organisations think that the risk of cybercrime has increased.

Due to rapid technological change, the traditional perspective on cybercrime has become much wider. Currently, cyber risk encompasses more than just computers. The appliances at risk of cybercrime range from mobile devices, gadgets interconnected in cloud, cars to household devices.

Cybercrime appears to be costly in financial terms. Globally, one fourth of the surveyed organisations has lost CZK 1,200,000 or more through cybercrime in the last two years.

36% of the respondents in the Czech Republic that suffered an economic crime reported that they have experienced cybercrime.

Ethics and Compliance

According to our survey, corruption and bribery rank as the fourth most common types of economic crime in the Czech Republic.

Positive message is that more than 86% of the survey participants have a formal business ethics and compliance programme which is slightly above the CEE and global average (identically 82%).

80% of the organisations surveyed responded that the Code of Conduct in their organisation covers key risks / policy areas and sets out the organisational values. According to 79% of respondents, their organisational values are clearly stated and understood and 55% of organisations provide regular training on the Code of Conduct and supporting policies.

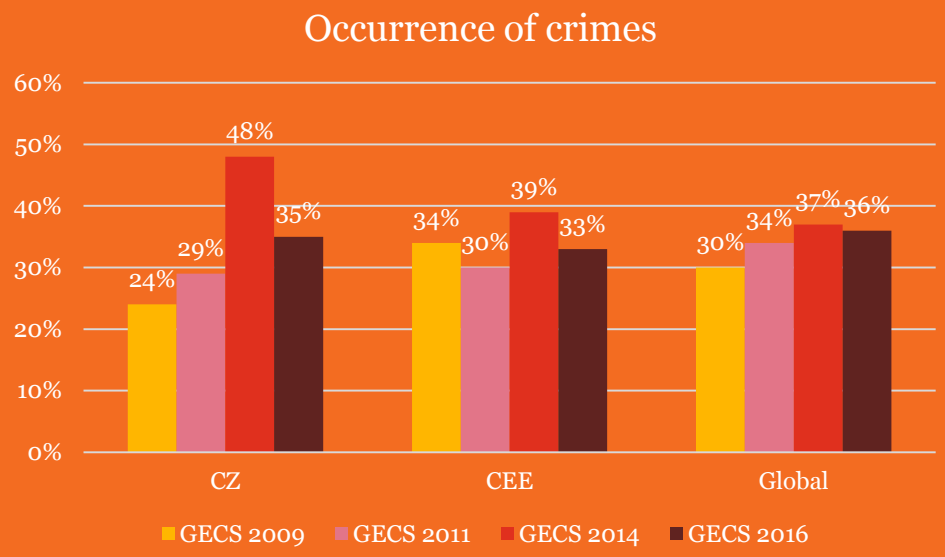
These relatively high reported numbers suggest that Czech companies have adequate Codes of Conducts. Having an understanding of the employees and firm-wide communication are important features contributing to an effective compliance function. In addition, regular trainings are advised for all participants.

Approximately 6% of organisations were asked to pay a bribe in the past 24 months.

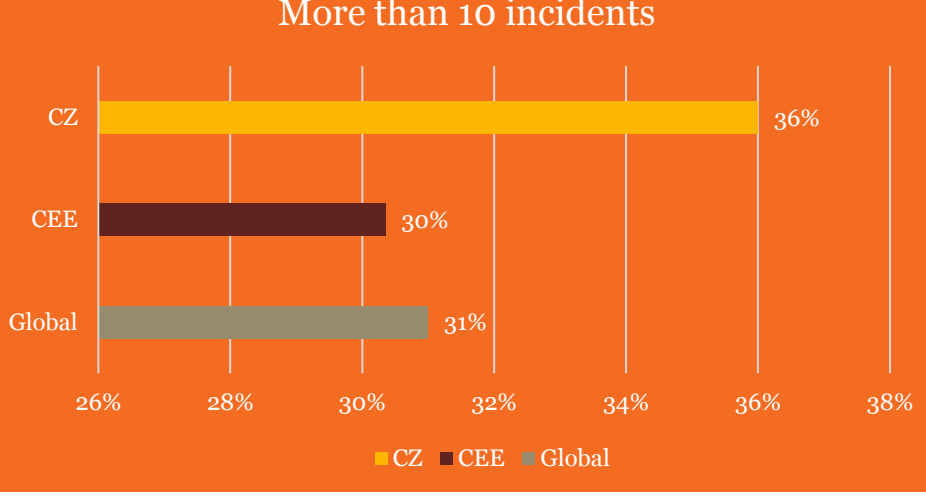
Economic Crime in the Czech Republic

Economic crime is an obstinate threat
How many organisations experienced fraud in the last 24 months?

Economic crime continues to be a major concern for organisations of all sizes, industries and different ownership structures. In the Czech Republic, more than one third (35%) of respondents has experienced economic crime in the past 24 months. When compared to the relevant region, CEE, which indicates 33%, the occurrence of economic crime in the Czech Republic is slightly higher. The positive outcome of this result is that it demonstrates a decrease compared to the results of the previous survey from 2014 but it still shows a growing trend considering the results since 2009.



36% of organisations, who suffered economic crime, were subject to more than ten incidents. This result is above the regional and global average (30% and 31%, respectively) which shows that when economic crime occurs in Czech organisations it tends to occur more often or repeatedly.



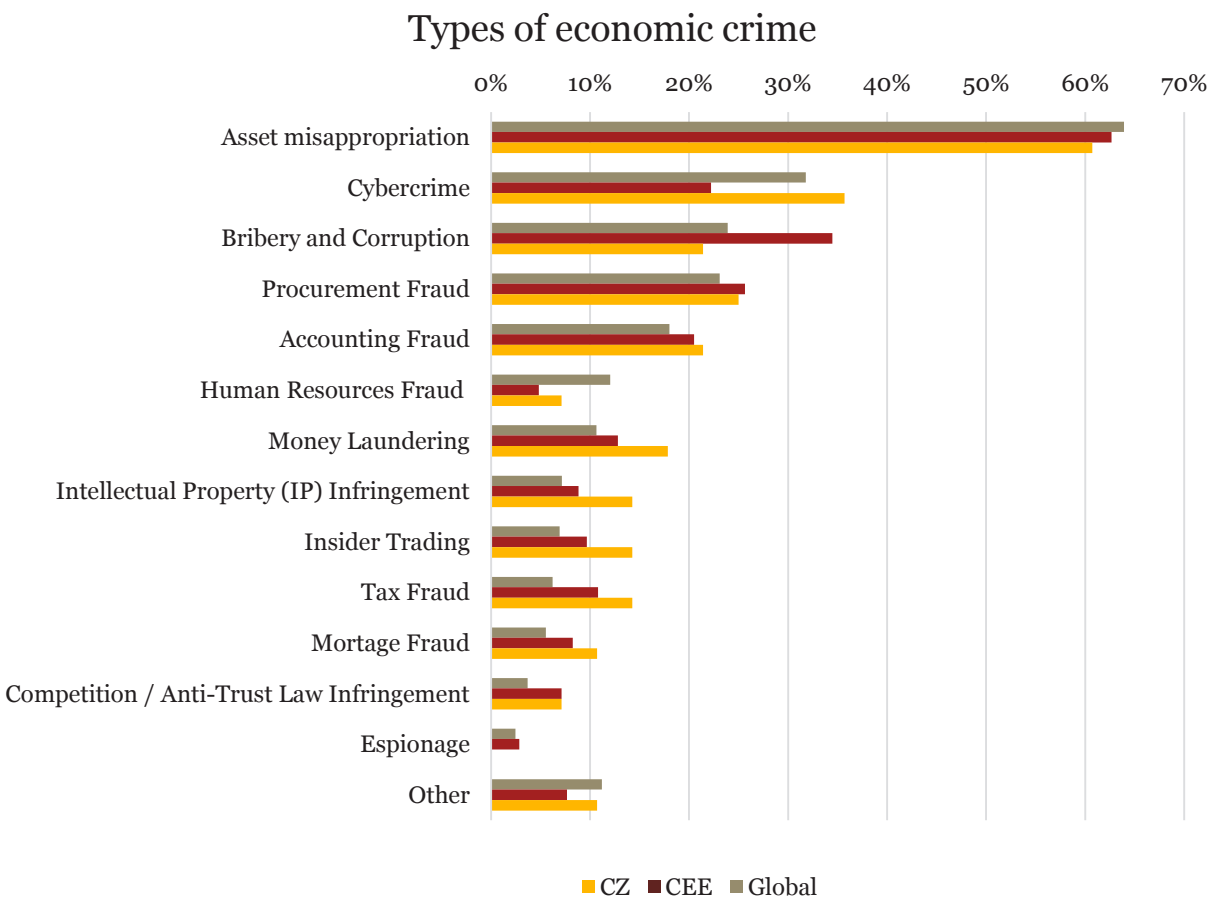
What types of economic crime are companies facing?

Most types of economic crime have decreased compared to the results from previous surveys (except for cybercrime and accounting fraud).
Among the most common types of economic crime are asset misappropriation (being the first with 61% of organisations who have suffered the economic crime), then the still growing cybercrime (36%), procurement fraud (25%), bribery and corruption and accounting fraud (both types 21%).

61%

Asset misappropriation has been first place in our survey for a number of years. This fact is generally predictable, because asset misappropriation is regarded as the easiest of frauds to detect.

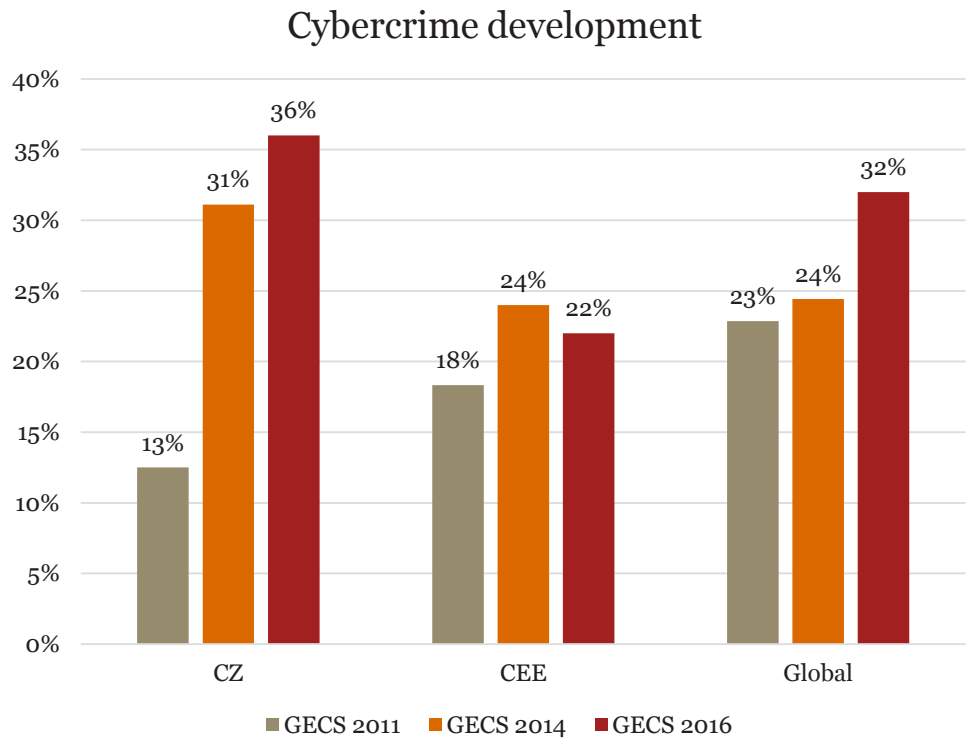
Asset misappropriation has been in first place in our survey for a number of years. This fact is generally predictable, because asset misappropriation is regarded as the easiest of frauds to detect.



Generally speaking, the Czech results are more or less in line with the distribution of economic crime in the CEE region and globally. Czech surveyed companies reported a higher occurrence of cybercrime than those in CEE and globally. In contrast, bribery and corruption appear to be more significant issues on the CEE level than in the Czech Republic.

Cybercrime

Cybercrime has been showing an increasing trend since it was included in our survey in 2011. It has risen globally so as regionally, but, in the Czech Republic it has risen even above regional and global level (36% in the Czech Republic compared to 22% in CEE and 32% globally). Cybercrime is also perceived as the biggest threat in terms of economic crime among the respondents in the Czech Republic.

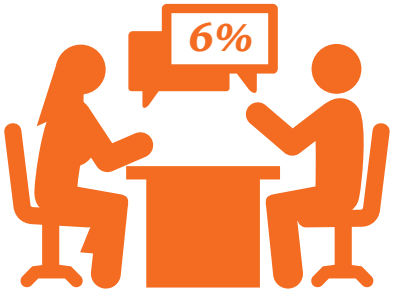


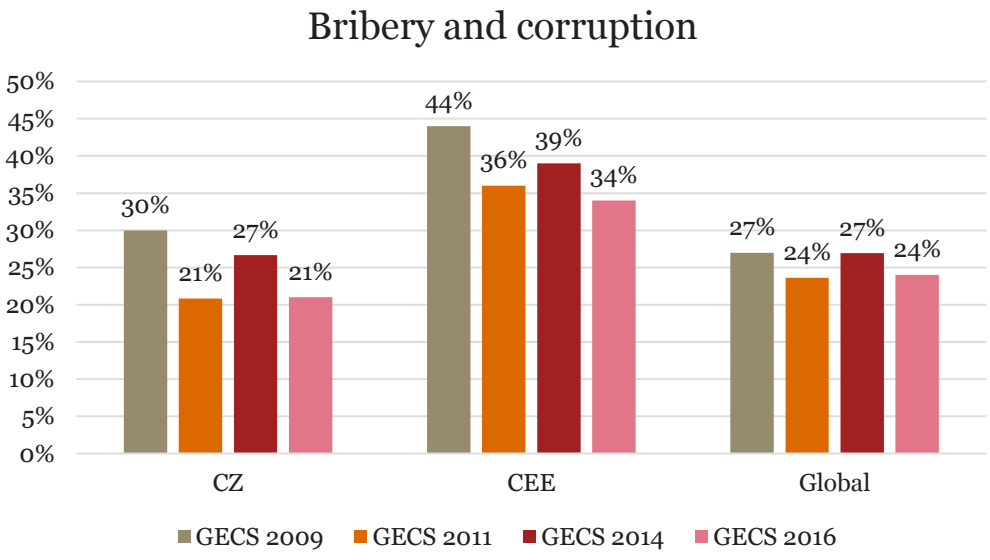
Bribery and corruption

In spite of the fact that our surveys report a decrease in bribery and corruption in the Czech Republic from 27% to 21%, in the CEE and globally as well, this type of economic crime has been significant since 2009. According to PwC Annual Global CEO Survey almost three quarters of organisations in the Czech Republic perceive corruption and bribery as a threat for their business.

Surveyed participants also reported that in the last 24 months their organisation was asked to pay a bribe (6% in the Czech Republic) and also lost an opportunity to a competitor who paid a bribe (12% in the Czech Republic). The current 6% for the Czech Republic represents a drop by 10 percentage points compared to the previous issue of the survey (16%).

This decreasing trend appears optimistic; however, we should be careful when drawing conclusions as the actual state of corruption and bribery can be much worse. Based on our experience, corruption and bribery are types of economic crime that are rather difficult to detect. The perception of bribery and corruption also might be subjective across the organisations – behaviour that one considers to be part of normal business practice, another might see as already crossing the line of corruption and bribery.





How much does fraud cost?

When considering financial losses due to economic crime, the survey shows that 40% of Czech organisations who suffered economic crime have lost CZK 1,200,000 or more.

Our survey respondents consistently note wider collateral damage from business disruptions, remedial measures, investigative and preventative interventions, regulatory fines, legal fees — and, critically, damage to morale and reputation — as having a significant impact on long-term business performance. These kinds of losses, of course not always quantifiable, can over time dwarf the relatively shorter-term impact of financial losses.

However, the consequences of economic crime for companies are much wider than just financial losses and the true cost of the economic crime is difficult to estimate, especially considering that actual financial loss is often only a small component of the fallout from a serious incident. Of those who had experienced damage as a result of fraud, 25% reported an impact on reputation and brand strength and 30% reported damage to employee morale.

Technology – an economic crime: blessing or curse?

Interview

Marek Novotný
Senior Manager, Advisory

How did Cyber Fraud evolve in the recent past?
The whole world is currently operating almost everything through ICT (information and communication technologies) and the complexity of solutions, amount of data and hardware performance is increasing significantly every year. Cyber Fraud is evolving as well on the same wave. For example, due to the price decrease in computation power, various approaches, which were not possible before, are currently quite common. Therefore, more complex scenarios could happen. It is important to realise that subjects, which are committing fraud, could use exactly the same technologies as you do and in many cases, they use them better. It is quite common for them to be able to use advanced analytics like machine learning algorithms e.g. just to simulate the behaviour of a regular customer.

What are the main critical areas where Cyber Fraud is involved?
The most critical area lies in services related to money transfers. Most cyber fraud incidents are related to money theft. The way how is it done differs even from the business point of view (it could be a shortage in a warehouse through the manipulation of warehouse records, changing banking accounts in the procurement or payroll system, layering transactions, identity theft to gain access to banking accounts, etc.). The second critical area is corporate espionage and reputation damage. For example, there are groups which aim to cause a significant reputation damage to you because your competitor "hired" them to do it. In general, even this usually has one goal to gain a better position on the market, which leads to increased profit. Corporate espionage nowadays relies heavily on cyber intelligence.

Which technologies are currently used within Cyber Fraud?
Cyber fraud can incorporate any technology currently available. It is a matter of usage and the perpetrator's intent on how to use it. Technology choices can range from the usage of special phrases in public search engines to highly sophisticated hacking techniques, which usually involve a social engineering component.
The important fact is that the amount of technologies is increasing and, as stated before, the complexity and number of functions in available devices is improved year by year. Therefore, Cyber Fraud is not a case for computers only as we know it. Almost everyone has a smart phone today with access to online/mobile banking. There are smart wearables, which will allow you to interact with some applications as well. The operating systems are part of TVs and Home Cinemas as well. You even have operating systems on gaming consoles or cars and, as we are more and more approaching the era of smart homes, the number of devices, which could be used for Cyber Fraud and Crime, will increase again as well.

What to do if something happened in my organisation?
This is something that depends on the maturity of internal procedures, controls, systems and readiness for such an incident within your organisation. Based on our experience, each type of fraud has a specific fingerprint, which could be detected within enterprise data regardless of whether it is a recurring or one-time-only fraud. We are able to analyse the data (both structured and unstructured), detect these fingerprints and investigate them. We help customers with prevention and also
in providing complete support during this unpleasant situation and supporting them with further steps.

Is it possible to do something better to avoid Cyber Fraud or at least to be ready when it happens?
Typically, the majority of fraudulent cases start because the process settings in an organisation are wrong, the discipline of application users is low and the risk of potential fraud is ignored before it happens.
Users must regularly use information systems and comply with internal and external policies and procedures. If you do regular risk assessments within your organisation, you are able to identify week spots and focus on them. If you are an international company, it is visible how these risks, threats are moving from continent to continent, and from country to country; therefore, you are able to react prior to any incident. On top of this you can add advanced systems for pattern recognition, suspicious activities detection, incident prediction and others, which are able to utilise and process all your enterprise data (both structured and unstructured data) and increase your level of protection and readiness. Here in PwC we are providing such support based on our long-term experience and proven quality.

It is no surprise that, in the current digital business environment, there is an increasing trend in the occurrence of cybercrime. Its frequency has grown almost three times since it was first introduced in our survey (13% in 2011 compared to 36% in 2016 of Czech companies which experienced economic crime were victims of cybercrime. Furthermore, in the Czech Republic, 28% of the all respondents' organisations reported that they were directly or indirectly affected by cybercrime. This result is slightly above the CEE and global average (22% and 26%, respectively). The increase in cybercrime incidents is also supported by the perception of the related risk – 57% of surveyed organisations think that the risk of cybercrime has increased. Moreover, according to PwC's Annual Global CEO Survey, almost half of Czech organisations see the pace of technology change as a threat.

Perception that the risk of cybercrime has increased

57% Czech Republic

44% CEE

53% Global

Damage to the reputation of an organisation, theft or loss of personal identity information and service disruption are globally the greatest concerns when it comes to cybercrime. Cybercrime appears to also be costly in financial terms. Globally, one fourth of the surveyed organisations has lost CZK 1,200,000 or more through cybercrime in the last two years.

The survey revealed that 46% of Czech organisations see the greatest cybercrime threat coming from external perpetrators. Another 33% of respondents think the threat could come from both internal and external perpetrators while only 9% of them believe it comes from internal perpetrators. The rest of the respondents did not have an opinion about possible cyber-attack threat origin. This is perceived similarly globally as well as regionally.

Board members of almost half of Czech companies do not request any information regarding readiness to deal with cybercrime:

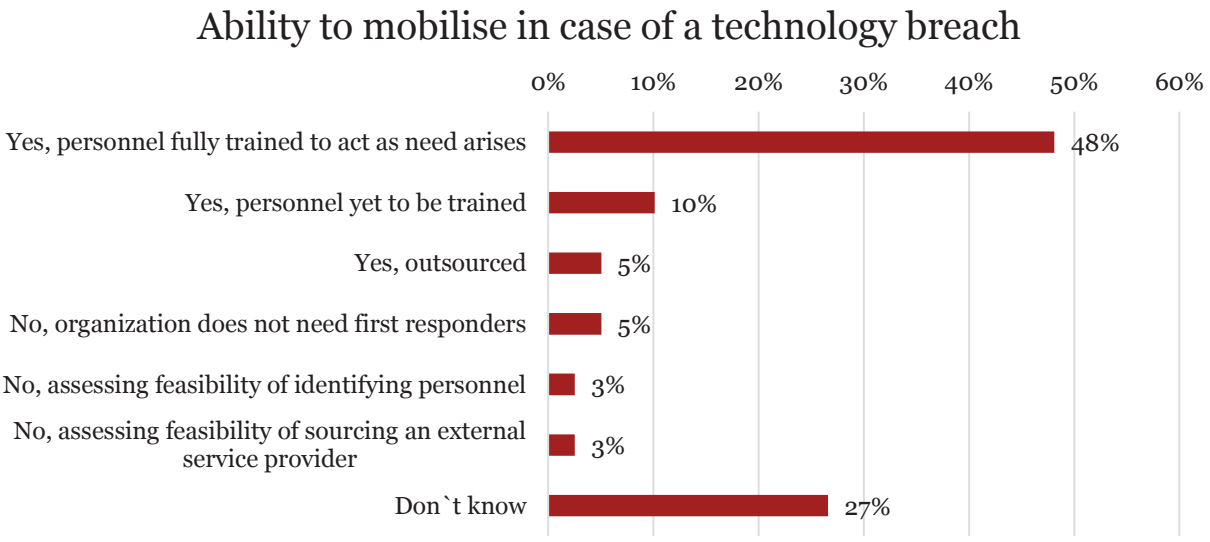
17% **of the respondents' organisations do not produce any information regarding the readiness of the organisation to deal with cyber incidents; and another** **28%** **do not even know about such requests.**

In the context of the increasing occurrence of cybercrime, the fact that almost half of companies do not have information about their readiness in case of these incidents is alarming.

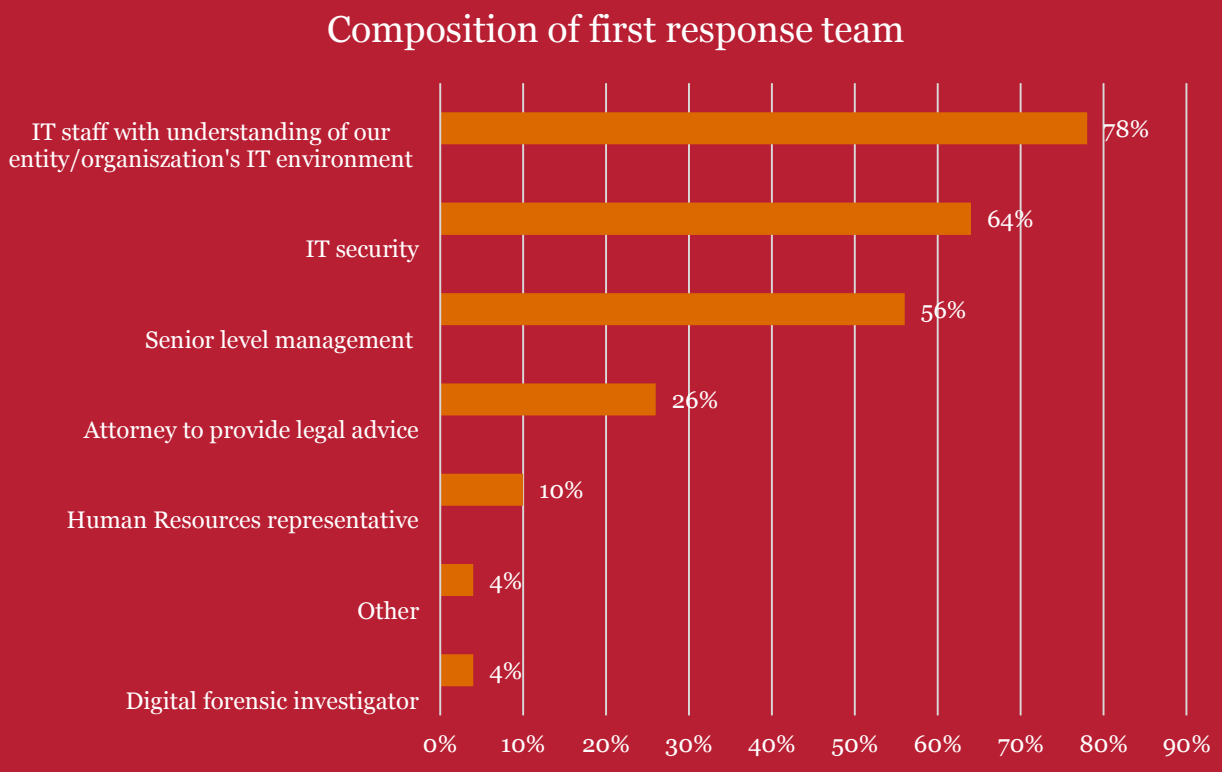
The same problem occurs with incident response plans to deal with cyber-attacks. Only 33% of the surveyed organisations have this plan fully in operation.

On the other hand, almost half of the Czech organisations surveyed (48%) has a response team that is fully trained and is able to deal with a technology breach.

This figure might seem quite high; however, considering the context of the ever-changing digital environment and the fact that no company is immune to attacks, companies still have work to do to mitigate the risk of the negative impact of potential attacks.



When it comes to respondents who can deal with a technology breach within a short time, response teams usually consist of IT staff with an understanding of the organisation's IT environment (78%), IT security specialists (64%), members of senior management (56%) and legal staff (26%). In contrast, only one in twenty incident response teams in the Czech Republic includes specialised digital forensic investigators (compared to one in ten globally).



Inadequate team composition and understandable haste to solve the problem after an incident could lead to higher risk of crucial evidence being potentially overlooked. This could hamper the company's ability to fully understand the impact of the breach, ability to prosecute perpetrators and most importantly to understand how the breach occurred. Activities and efforts of the response team should always be coordinated and responses should be sufficiently aligned with investigation goals.

Detection methods

It is a positive finding that an increasing number of fraud incidents is detected via systematic mechanisms (54% in 2011, 61% in 2014 compared to 68% in 2016). 68% of the Czech respondents reported that fraud was detected by corporate controls (compared to 54% in CEE and 47% globally).

In particular, apart from "traditional" means of detection such as fraud risk management (18%) and internal audit (14%), we would like to highlight the increasing share of data analytics (increase from 5% in 2014 to 14% in 2016) and suspicious transactions monitoring (increase from 8% to 14%). In a changing business landscape, when different fraud incidents leave a different specific footprints in the data, these automated electronic detection mechanisms can be very powerful tools. Moreover, when fully automated these tools can run in real time without or with very limited human intervention.

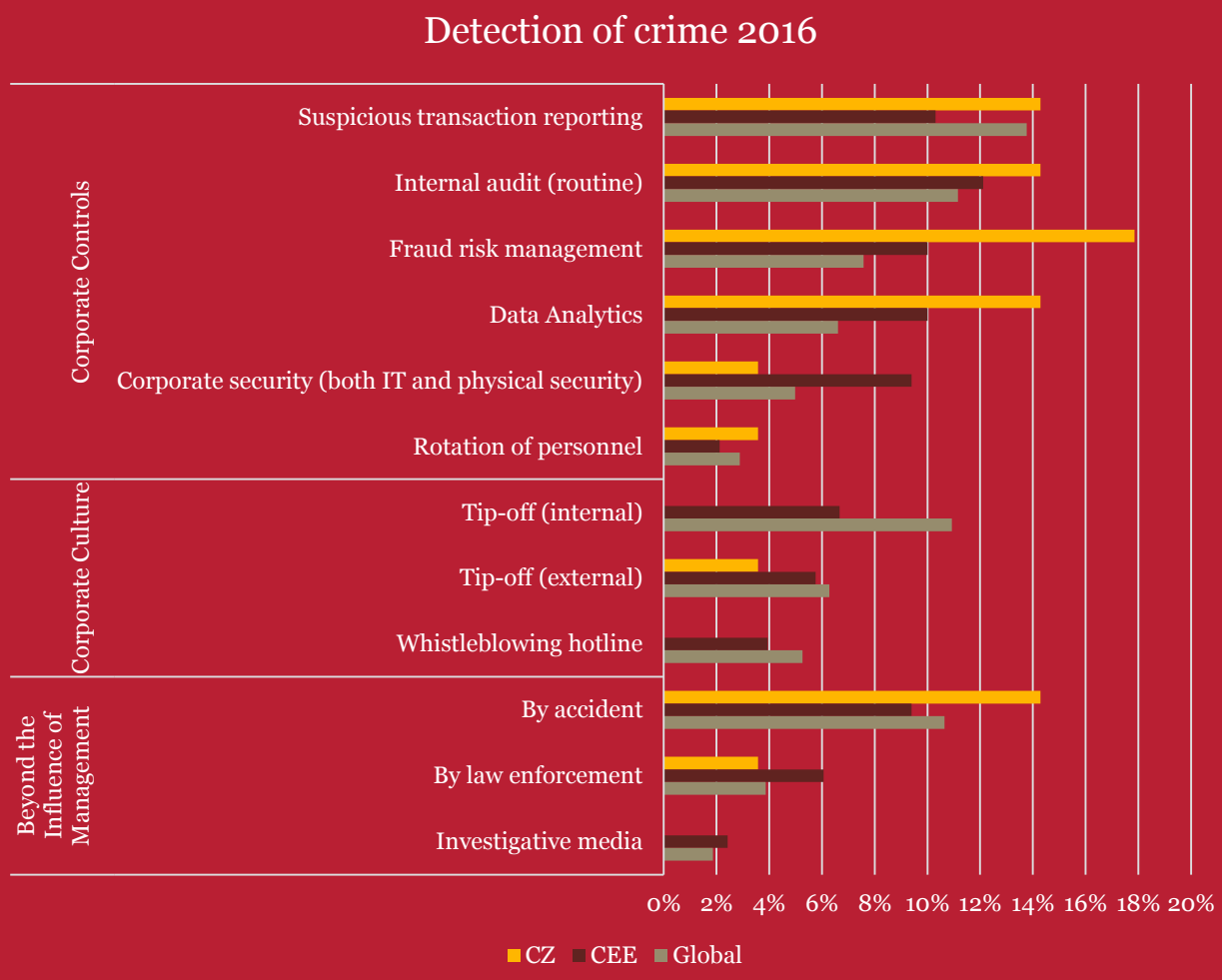
However, despite this encouraging result, this is no time to rest on our laurels. According to the organisations surveyed in the Czech Republic, 18% of economic crime was still detected beyond the influence of management; the most frequent - simply by accident - 14%. We also see room for improvement in detection methods which can be classified as corporate culture. Compared to the previous survey we noticed that none of the fraud accidents was reported through a whistleblowing hotline or internal tip-off (compared to 18% in 2014).

It is surprising that, when it comes to a whistleblowing hotline, on one hand almost half of the companies monitor reports from whistleblowing hotline, however, according to the results from our survey none of the incidents of economic crime was detected through the whistleblowing hotline. It may signal that a number of alerts received through this channel are false or the whistleblowing hotline is simply not working effectively. An effective whistleblowing system is not only a powerful tool for combating economic crime but it is also part of a sound and ethical business environment.

Features of an effective whistleblowing hotline

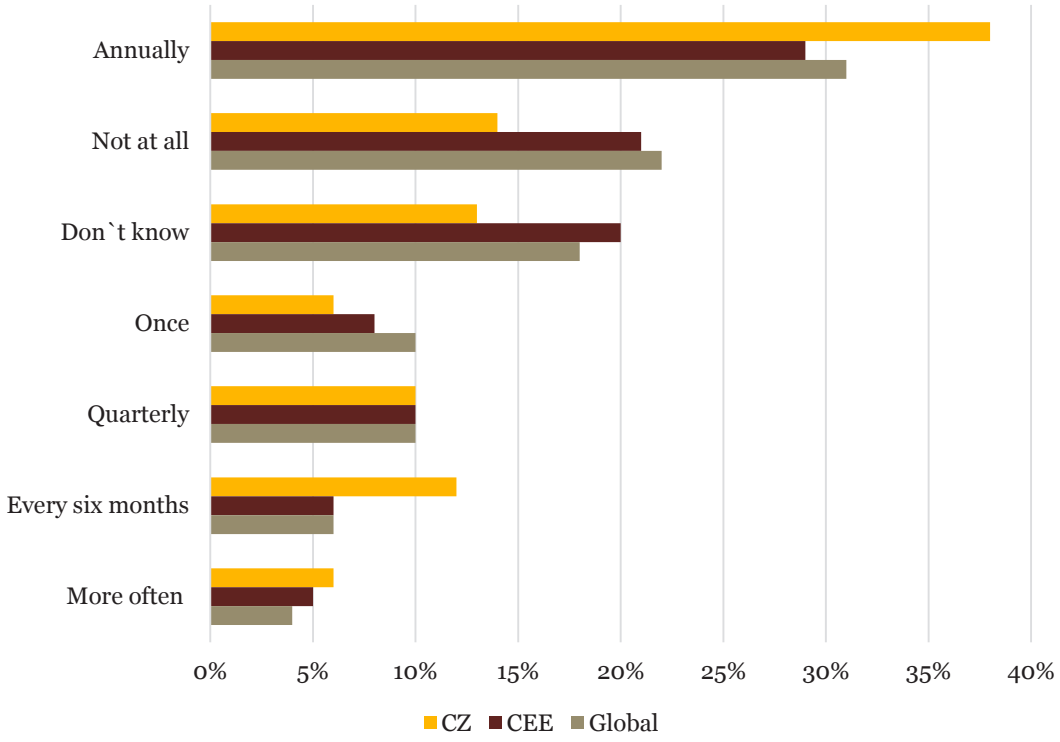
- Integral part of the organisation's ethics and compliance programme
- Multiple means (for example dedicated phone line, email box, contact point) to make the mechanism accessible and easy to use for all employees and whistleblowers from the environment outside the organisation
- Anonymity and confidentiality
- Protection of the whistleblower against any retaliation
- Communication and education
- Positive tone at the top
- Analysis of the alerts received through this channel and produce statistics
- Publication of "wins"
- Possibility of an external provider

Analysing the reports from whistleblowing hotlines faces a couple of challenges and it is part of the investigation to distinguish whether the report was honest or malicious, however dealing with malicious reports burdens the investigators and draws their attention away from the "real" incidents. To avoid misuse of this important detection channel, organisations should set up and communicate the environment that malicious reporting or submitting false reports is a violation of the core corporate values.



The utilisation of fraud risk management in Czech organisations for fraud detection is also above the regional and global level (10% and 8%, respectively). 72% of Czech surveyed organisations performed a fraud risk assessment at least once in the last 24 months. Globally it was only 61% and regionally even less, only 58%. This figure correspondents with the rather high number of instances when economic crime was discovered by corporate controls.

Fraud risk asessment performed



Perpetrators of economic crime

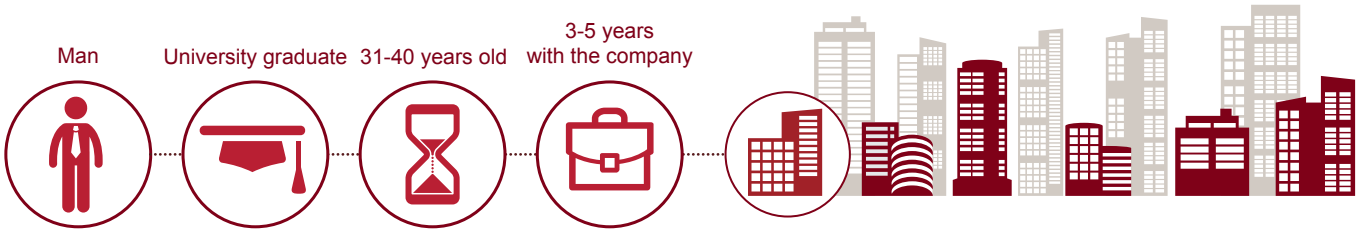
What is the typical profile of the fraudster?

Historically the split between the internal and external fraudster was usually equal. This year's survey in the Czech Republic shows the slight prevalence of the external perpetrator (54%) over the internal (43%). For the remainder of the perpetrators, the respondents did not know whether the company was attacked from inside the company or from the outside environment.

If it is an external perpetrator, the global results show it would very likely be a customer (25%). Customers held a higher share than agents/intermediaries (which were at the top in the last survey from 2014) or vendors (17% and 10%, respectively).

How can companies defend themselves from attacks committed by external actors? One of the key recommendations is simply to know who you are doing business with. Before entering business relationships, organisations should employ corporate intelligence and due diligence techniques. These procedures assist organisations to fully identify their business partners and verify the partner's integrity and probity. Any adverse history should trigger a red flag for the organisation. These procedures should be conducted to determine if there have been changes over time. Moreover, nowadays in light of sanctions and increasing requirements by regulators, these transparency methods have become increasingly important.

Internal perpetrator profile



According to the results from 2016, the internal perpetrator is mostly part of junior or middle management. The complete profile of an internal perpetrator obtained from all the surveyed companies gives us a male (79%) between 31 to 40 years (42%) of age, working for the organisation for 3 to 5 years (33%, which in line with the statement that the perpetrator would be from junior/middle management) and has a university degree (47%).

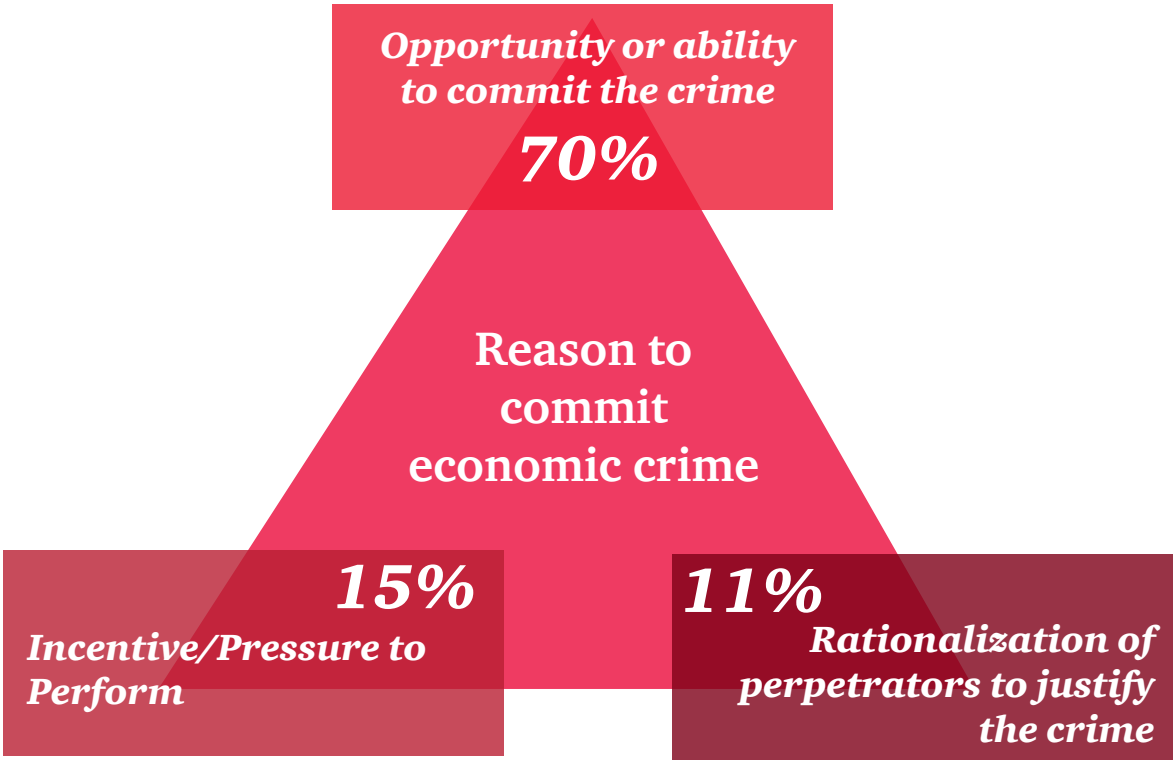
External perpetrator profile

What are the drivers of economic crime?

When we asked our respondents what factor they feel has contributed the most to economic crime committed by internal actors, the majority unsurprisingly answered opportunity or ability to do it.

However, the presence of the opportunity alone is not sufficient to commit fraud. The perpetrator of the fraud needs to have an incentive or pressure to commit fraud and has to be able to justify the crime. The results of this question indicates that companies consider opportunity to be the most important while they could omit the importance of the other two necessary motivators.

A crucial factor that contributes to the committing of economic crime is simply the opportunity to do it (globally 69%). So the best way to prevent this opportunity is to strengthen controls.



Examples of opportunities:

- Internal controls are not adapted to the current fast changing business environment and new types of threats including cyber crime;
- Limited ability of detection, insufficient number of investigative teams with inappropriate abilities and skills;
- Reactive, rather than proactive attitude;
- Company´s culture, tolerance of frauds, bad example of management; and
- Misuse of trust.

Ethics and Compliance: Aligning Risks and Responsibilities with Values and Strategy of the Organisations

Interview

Kateřina Halásek Dosedělová
Senior manager, Forensic services

What are the most common compliance- and/or ethics-related challenges companies currently face?
The regulatory environment, particularly in the financial services industry, is becoming more and more complex due to new regulatory requirements. Corporations are thus subject to almost on-going changes, for instance, in the global sanctions area. Considering the risk of evolving landscape, the companies face increasing vulnerability to risk of non-compliance if they do not have an effective compliance programme in place.

How have the companies' compliance function changed in reaction to the evolving risks and challenges?
Nowadays we can find compliance officers not only in financial institutions and the Czech subsidiaries of multinational companies, but also in purely Czech companies or state-owned entities. This is really a good sign. Unfortunately, there is still a number of companies that consider the compliance function to be pure cost and burden, and try to limit it to a minimum. On the other hand it is not sufficient to tick "we set up the compliance function". Primarily companies need to ensure that the compliance function has appropriate authorisation and is an equal partner to the top management, who should provide full support to compliance matters.
Last but not least, it is critical that the compliance function works effectively. And what does it mean? It means you address evolving risks using a risk-based approach, set up a compliance programme across the organisation to mitigate the non-compliance risk and have an escalation and reporting mechanism in place, for cases where an attempt or case of non-compliance is identified.

How should an effective compliance programme work?
An effective compliance programme should take a risk-based approach based on a holistic understanding of the financial crime risk across the whole company and its weaknesses. On one side, you should mitigate the relevant risks; and on the other side, it should position the company to reach its business goals.
The key prerequisite of an effective compliance programme is having the appropriate communication across the whole organisation and a link to the day-to-day operations in all locations. The compliance officer should ensure that the programme is practical and that the compliance team keeps its door open to any employees, at any organisational level, to provide clarification and respond to ad-hoc questions.
You, as compliance officers, should be aware that employees are mostly overloaded with information and employee turnover is, in certain industries, quite high. Consider embedding compliance topics in regular communication to your employees – firm-wide, department-wide, etc. As mentioned above, top management support is key. However, the most important in terms of communication is the middle management buy-in of the compliance programme. The Middle management is in daily contact with your staff and thus they are the messengers and role models. If your staff sees that his/her boss is living and breathing compliance, they will follow that example.

To conclude, can you give the typical reasons why the compliance- and/or ethics-related function fails?
As I mentioned earlier, it should not be a tick-the-box exercise. Even if compliance is a non-profit making function, it should not have a low priority. Rather, the other way round. Even if your firm needs to cut costs including headcount and training, you should not automatically cut the compliance function and its activities. This might be a strategic miscalculation. While risk and threats are ever-changing, the substance of a successful compliance programme is that it can foresee and address an evolving risk landscape. The other point is also disconnection between compliance and daily business.
Please do not forget that your client-facing and back-office staff are your so-called first line of defence against financial crime risks. Thus, you should already try to involve them in the compliance programme in the preparation stage. You should also regularly communicate with them and give them the feeling that you have your door open so they can express their concerns or pose questions when comfortable to them.

Compliance programmes

Five steps on the way to a more effective compliance programme

1. **Ensure your programme is in line with corporate strategy; and communicate this alignment**
2. **Evaluate and potentially reimagine the identity of your compliance function so it may adapt to an environment where risk and threats are ever-changing.**
3. **Ensure that all owners of compliance obligations fully understand the compliance "big picture" across the organisation, and the scope of their own responsibilities within it.**
4. **Remember that policies and training on values are not enough: credible, consistent engagement across the organisation are essential.**
5. **Don't downsize when risks are going up**

Four fundamental areas of focus for enhancing the effectiveness of compliance programmes

People and culture
Clear processes and principles, culture where compliance is hard-wired to values, measuring and rewarding desired behaviours.

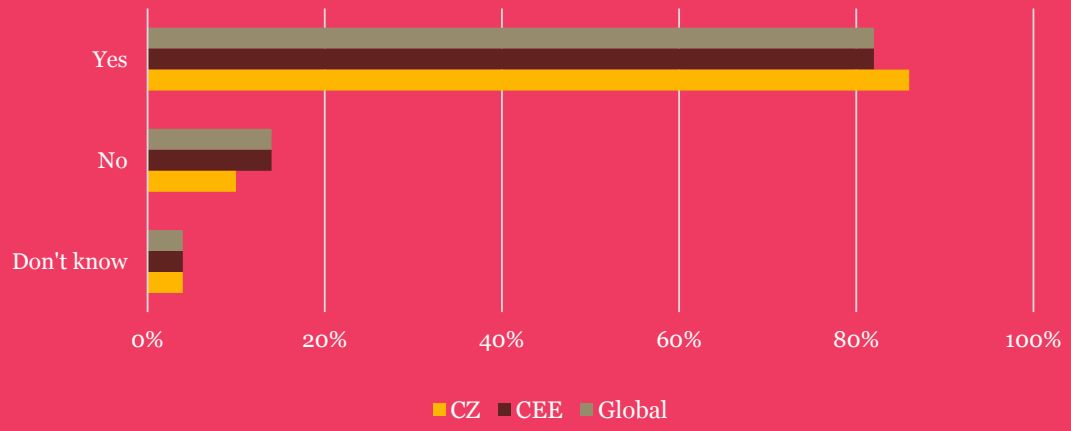
Roles and responsibilities
Formal compliance structure ensuring they are correctly aligned with current risks.

High-risk areas
Better implementing and testing in high-risk markets and divisions.

Technology
Better use of detection and prevention tools, including big data analytics.

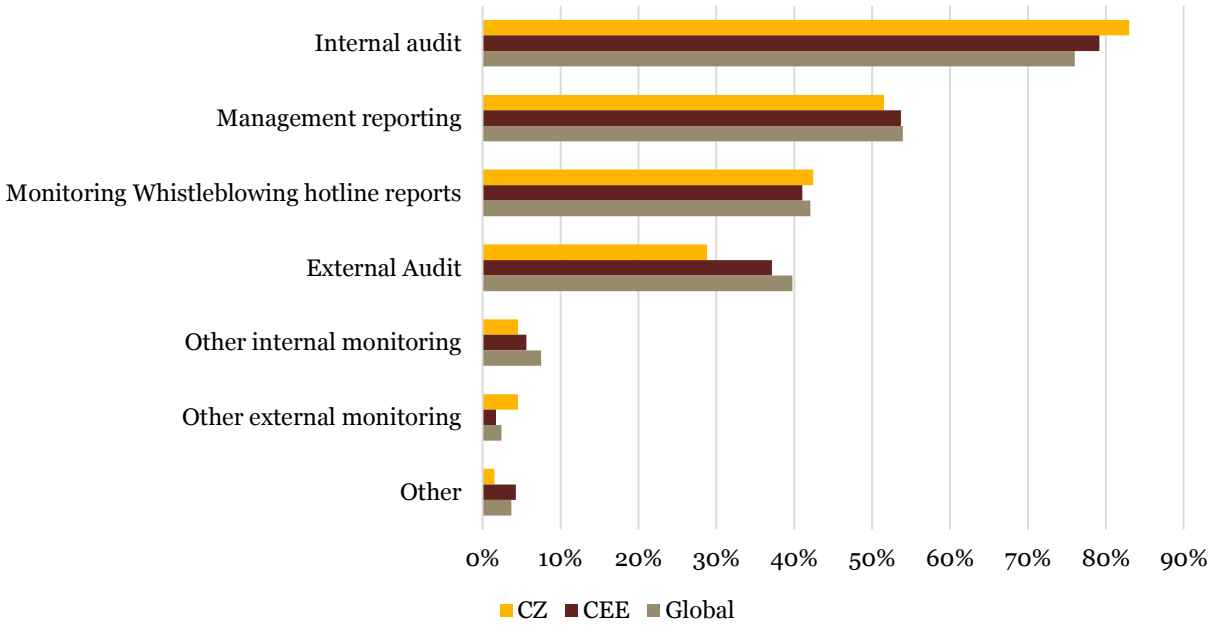
Our survey shows that formal business ethics and a compliance programme are established in 86% of Czech organisations. Even though this number is quite high, there is still room for improvement. In line with regional and global results, companies most frequently have a Chief Compliance Officer who takes care of the business ethics and compliance programme (46% in the Czech Republic, 38% in CEE and globally).

Formal business ethics and compliance program in organisation



To ensure that the company's compliance and business ethics program is effective, 83% of Czech companies' compliance programs are checked by an internal audit, 52% have management reporting and 42% monitor whistleblowing hotline reports. Such reports actually include not only fraud suspicions, but also incidents on management compliance and/or other staff matters.

How does your organisation ensure that your compliance and business ethics program is effective?



When looking closer at how ethics and compliance are in-built in the corporate environment, 79% of the organisations surveyed responded that the Code of Conduct in their organisation covers key risks/policy areas and sets out the organisational values.

Understanding the employees' needs and firm-wide communication are two of the essential features contributing to an effective compliance function. Our survey shows a positive highlight that, according to 79% of respondents, organisational values are clearly stated and understood and 55% of organisations provide regular training on the Code of Conduct and supporting policies.

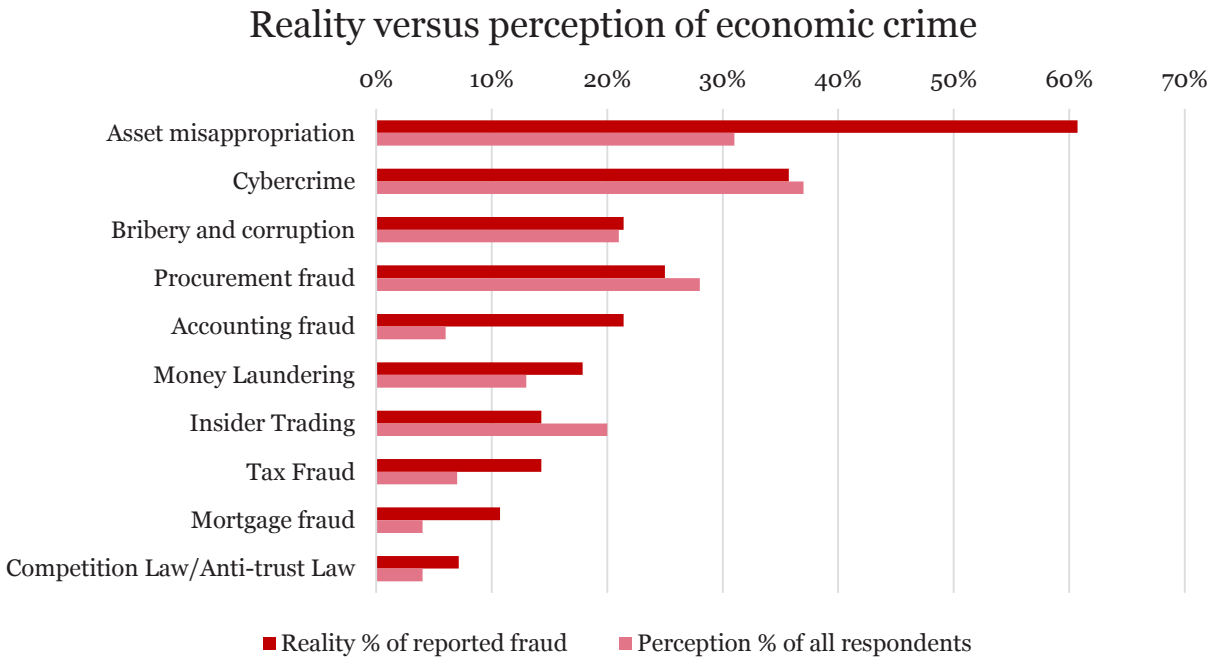
67% of respondents are of the view that the leadership of their organisation conveys the importance of ethical business conduct and sets a positive example. This is what we call the "tone at the top" setting the ethical climate of the organisation and is a vital element of effective internal control.

However, despite the growing emphasis on ethical values in corporate communications, and the widespread adoption of business ethics and compliance programmes, companies may experience a disconnect between the tone at the top and the reality on the ground (both behavioural and budgetary), leaving organisations vulnerable to compliance breakdowns.

Future of economic crime – real state of economic crime versus perception of the risk

We also asked our respondents which types of crime companies expect to face in the next 24 months.

We find it interesting to compare the perception of economic crime risks with real occurrences. It seems that companies underestimate the risk of asset misappropriation in spite of its reported occurrence. On the other hand, perception of cybercrime affecting the company is higher than its actual occurrence. Companies are quite right to fear that cybercrime could happen to them given the rising trend of actual cybercrime shown in our survey.



Contacts

Sirshar Qureshi
Partner, CEE Forensic Leader
+420 251 151 235
sirshar.qureshi@cz.pwc.com

Pavel Jankech
Director, Forensic Technology Solution
+420 251 151 336
pavel.jankech@cz.pwc.com

Kateřina Halásek Dosedělová
Senior manager, Forensic services
+420 251 151 293
katerina.halasek-dosedelova@cz.pwc.com

www.pwc.com/cz

Prague
Hvězdova 1367/2c, 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

pwc