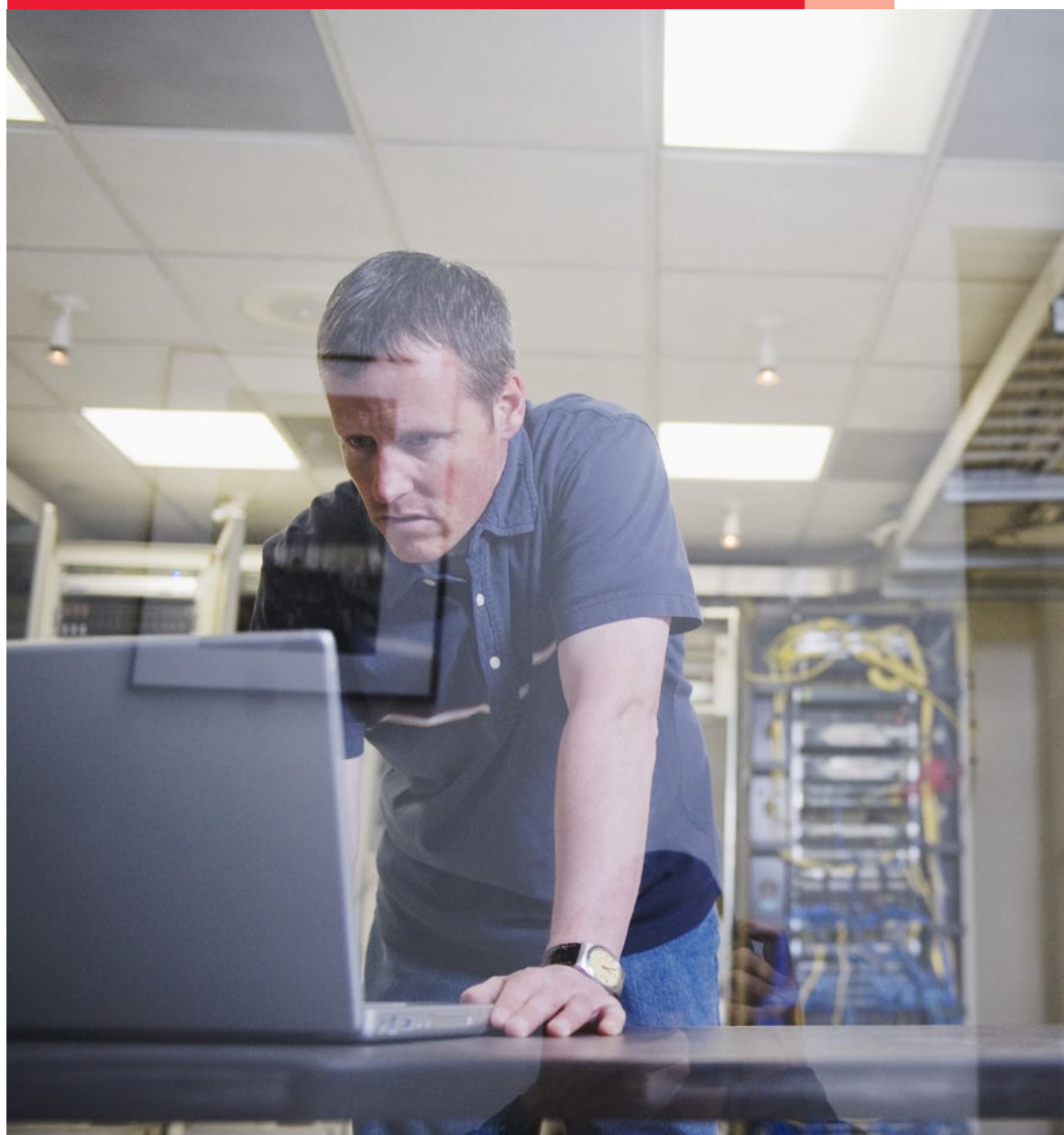


# *Cyber security in the spotlight*

## The Global Economic Crime Survey - Czech Republic

*Nearly 4,000 organisations  
in 78 countries help to  
provide a global picture  
of fraud and other crimes.*

*December 2011*



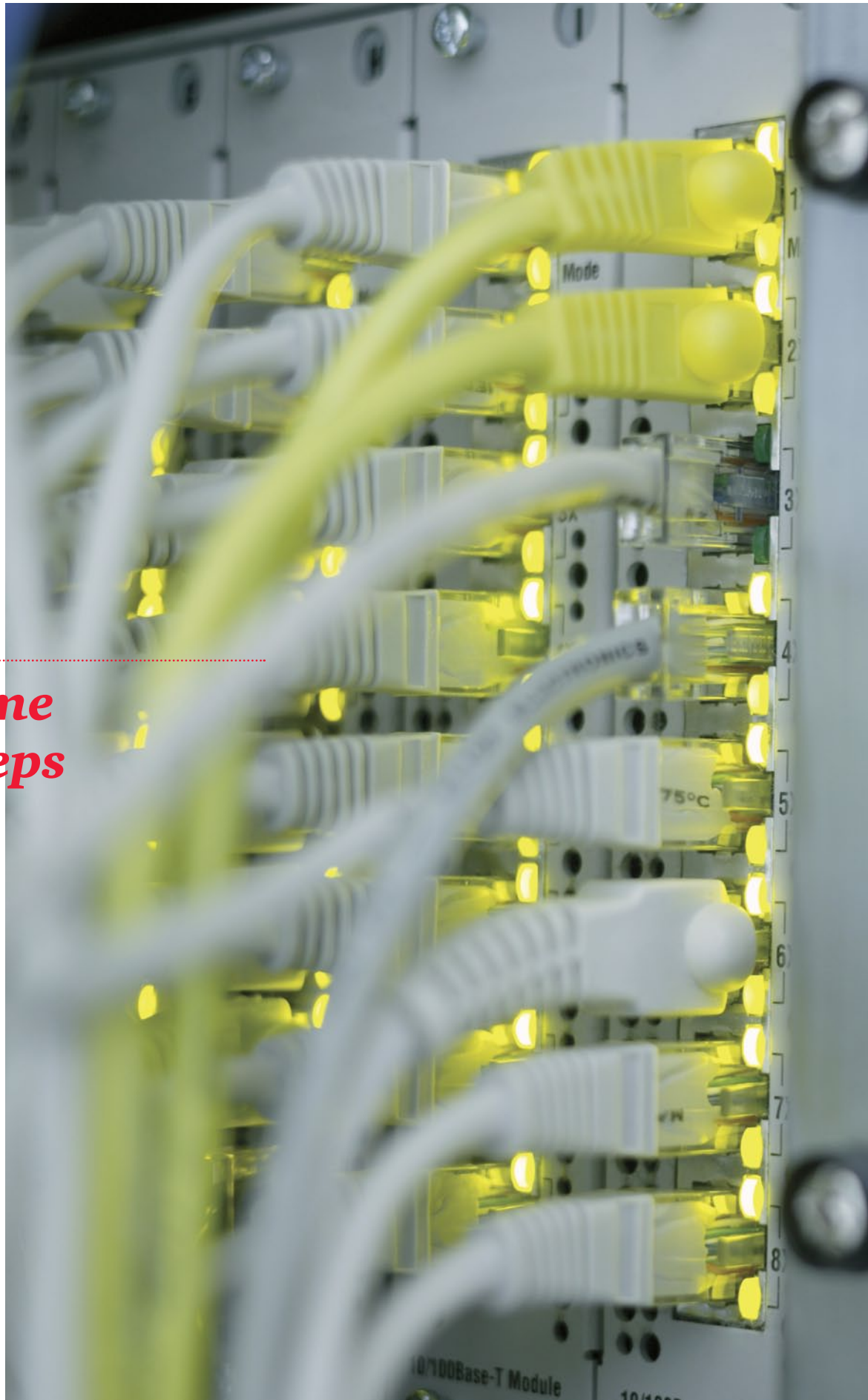


---

# Contents

<b>Introduction</b>	<b>5</b>
<b>The highlights</b>	<b>6</b>
Cybercrime	6
The current fraud environment in the Czech Republic	7
<b>Cybercrime in the spotlight</b>	<b>8</b>
Cybercrime enters the frame	8
Is cybercrime really just an external threat?	9
What are organisations really worried about?	10
Is your organisation like a deer in headlights?	11
Who is ultimately responsible for dealing with cybercrime in an organisation?	12
<b>The current fraud environment in the Czech Republic</b>	<b>13</b>
Do organisations know what they are facing?	13
So what types of economic crime are we talking about?	13
How much does fraud cost, and what is the collateral damage?	14
Who is committing fraud?	14
What do organisations do with the fraudster?	15
How do organisations detect fraud?	16
How fraud risk assessments can really help organisations?	17
Fraud in the future	18

***Cybercrime  
never sleeps***



---

# Introduction

We are pleased to present to you the **2011 PwC Global Economic Crime Survey results**. With **3,877** respondents from across **78 countries**, including 84 leading organisations within the Czech Republic, this study continues to be the largest of its kind available worldwide. We trust that our survey will provide Czech business leaders and corporate executives with unparalleled insight into the perceptions, awareness and impact of economic crime on businesses around the world.

Economic crime does not discriminate. It affects organisations all over the world and no industry or organisation is immune. The fallout is not just the direct costs; economic crime can seriously damage brands or tarnish a reputation, leading organisations to lose market share. As society becomes less tolerant of unethical behaviour, businesses need to make sure they are building – and keeping – public trust.

Our sixth Global Economic Crime Survey turns **the spotlight on the growing threat of cybercrime**. Today, most people and businesses rely on the internet and other technologies. So they are potentially opening themselves up to attacks from criminals anywhere in the world. Against a backdrop of data losses and theft, computer viruses and hacking, our survey looks at the significance and impact of this new type of economic crime and how it affects businesses worldwide.

We asked a number of questions specifically relating to cybercrime, the threats posed by cybercrime and how organisations try to counter any cybercrime attacks. And, to help us spot long-term trends, we asked several ‘core’ questions on economic crime in general, so we could compare this year’s data with previous surveys.

Accordingly, our report is divided into two key sections:

- Cybercrime – its impact on organisations, their awareness of the crime and what they are doing to combat the risks.
- The current fraud environment in the Czech Republic – focusing on the type of frauds committed, and how they are detected, who is committing them and what the repercussions are.



**Sirshar Qureshi**  
Forensic Services  
Partner, PwC



**Michal Kohoutek**  
Forensic Services  
Director, PwC

# The highlights



## Cybercrime

- While being statistically insignificant in the past, **cybercrime** has emerged as one of the top types of economic crime and is now in fourth place in the Czech Republic (13%). While this is below the average for Central & Eastern Europe (“CEE”) (18%) and globally (23%), we may well see its rise in years to come. **30%** of Czech organisations believe their organisation **will likely face cybercrime** in the following 12 months; together with bribery and corruption and insider trading the highest percentage among all types of fraud.
- Czech organisations are increasingly aware of the risk of cybercrime. **98% of Czech respondents** stated that their perception of the risk of cybercrime has either increased or remained the same over the last year. This is despite the fact that more than **2 out of 5** respondents in the Czech Republic **hadn’t had any cyber security training** in the past 12 months.
- **IP theft (including theft of data)** together with **reputational damage** and **theft of personal identifiable information** causes the biggest concerns to Czech organisations when it comes to the effects of cybercrime.
- The cybercrime threat is no longer seen as having primarily an external origin: **21%** of Czech respondents see the **internal threat** as more prevalent, a further **32%** consider cybercrime as an internal as well as an external threat. The **Information Technology department** is perceived as the most likely source of an internal cybercrime threat; this is consistent in the Czech Republic, the CEE as well as globally.
- **71%** of all respondents reported that they have **in-house capabilities to prevent and detect** cybercrime and almost half of all respondents believe they are capable to investigate cybercrime internally. Presumably, these capabilities often reside with Information Technology departments – the department seen as the most likely source of cybercrime threat. It is therefore alarming that **69%** of Czech organisations reported they **do not have any access to forensic technology investigators or are not aware of it**.
- **Only 20%** of Czech organisations **review cybercrime threats more frequently than on an annual basis**. While this is consistent with their CEE and global counterparts, it might not be frequent enough to keep up with the fast speed of the development of technology and IT threats.

## The current fraud environment in the Czech Republic

- Economic crime continues to be a serious issue affecting organisations worldwide, across the CEE and in the Czech Republic. **29% of organisations in the Czech Republic experienced one or more economic crimes in the past 12 months**; slightly below the average for the CEE (**30%**) and globally (**34%**). For the Czech Republic, this represents an **increase by 5 percentage points** compared to our previous survey.
- **Asset misappropriation** remains the most common type of economic crime reported in the Czech Republic (**75%**) and prevailing also in the CEE (**69%**) and globally (**72%**). This is not surprising, given the fact that it is easier to detect compared to other types of economic crimes. **Together with cybercrime**, asset misappropriation appears to be the main contributor to the overall increase in percentage of Czech organisations affected by economic crime.
- The next most common type of fraud in the Czech Republic is **accounting fraud (21%)** together with **bribery and corruption (21%)**. While the reported incidents of both these types of fraud decreased in comparison with 2009, we should be careful in drawing conclusions that are too optimistic. Our experience shows that the actual incidence of bribery and corruption is likely to be higher as this type of crime is difficult to identify and often goes undetected. As for accounting fraud, the significant decrease may have been caused by slightly lower pressure on management to manipulate financial statements due to partial recovery from the difficult times during the period when this survey was carried out. However, given recent developments in the world economy, and Europe in particular, the pressure may quickly increase to even higher levels.
- Fraud continues to be costly: **38%** of organisations who suffered economic crime **lost over USD 100,000**, including **8%** suffering a loss of more than **USD 5 million** as a result of fraud. However, the fallout from fraud is not simply the direct cost. Although difficult to quantify, collateral damage may be just as damaging: **67%** of Czech organisations highlighted the negative impact on **employee morale** as the most significant indirect cost of economic crime in the last 12 months.
- **67%** of the economic crimes Czech organisations experienced were carried out by **internal fraudsters**. This number has increased significantly in comparison to 2009 (**50%**). **Customers (43%)** and **vendors (29%)** were identified as the **main perpetrators of external fraud**.
- Our survey shows that Czech organisations are not afraid to take swift action against fraud perpetrators, whether internal or external: In the case of internal perpetrators, **dismissal** was the most frequent action taken in the Czech Republic, in **81%** of cases. Similarly, when external fraud is detected, **the business relationship was ceased in 71%** of cases; this represents a significant increase compared to 2009 (**30%**) and is well above CEE (**53%**) and global (**39%**) averages. While the low level of tolerance to fraudsters is definitely a positive sign, we would recommend that organisations increase their efforts on the prevention front: knowing your employees and your business partners prior to engaging with them is less costly than dealing with the consequences of fraud.
- It is encouraging that an increasing number of fraud incidents is being detected via systematic mechanisms: **38%** of Czech organisations have detected fraud through either **fraud risk management** or regular **internal audit procedures** (in 2009: **35%**). It seems that Czech organisations are **increasingly less willing to rely on chance** to detect fraud. However, with **1 out of 5 frauds** still being detected beyond the influence of management, there continues to be room for improvement in this area:
  - **42%** of Czech organisations surveyed reported that they had **not performed any fraud risk assessment** in the last 12 months or they did not know if they had. The main reasons for Czech organisations not to perform fraud risk assessment were the **perceived lack of value (57%)** and lack of knowledge about what risk fraud assessment involves (**21%**).
  - We have also noted that **71%** of Czech organisations **do not employ a whistle-blowing mechanism**. This is very surprising as in our experience the anonymous whistle-blowing mechanism helps to discover fraud in most cases when other means of fraud detection prove ineffective.



# Cybercrime in the spotlight

## What is cybercrime?

GECS 2011 focussed on financial crime and the fraud aspect of cybercrime and for the purposes of our survey questionnaire, cybercrime was formally defined as follows:

*“Cybercrime, also known as computer crime, is an economic offence committed using a computer and the internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a by product in order to create the fraud and only includes such economic crimes where a computer, the internet or use of electronic media and devices is the main element and not an incidental one”.<sup>1</sup>*

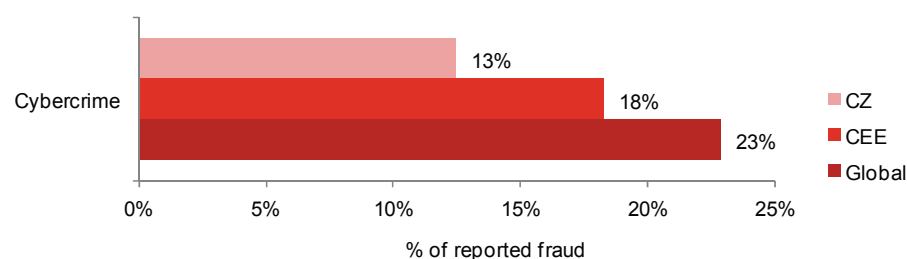
The above definition may be considered a fairly common definition of cybercrime, yet it would appear that many perceive this as a wider phenomenon which makes the definition open to different interpretations. There is no standard globally accepted definition of cybercrime, and the implications of not having a clear-cut definition could be that if organisations do not know what the dangers are, where the dangers come from and how cybercrime can impact their business, then it is harder to detect and combat cybercrime.

<sup>1</sup> As defined in GECS 2011 by PwC in conjunction with our survey academic partner, Professor Peter Sommer from London School of Economics.

## Cybercrime enters the frame

While being statistically insignificant in the past, **cybercrime** has emerged as one of the top types of economic crime in our 2011 survey and is now in fourth place in Czech Republic (13%). While this is below average for the CEE (18%) and globally (23%), we may well see its rise in years to come.

### Share of cybercrime within committed frauds



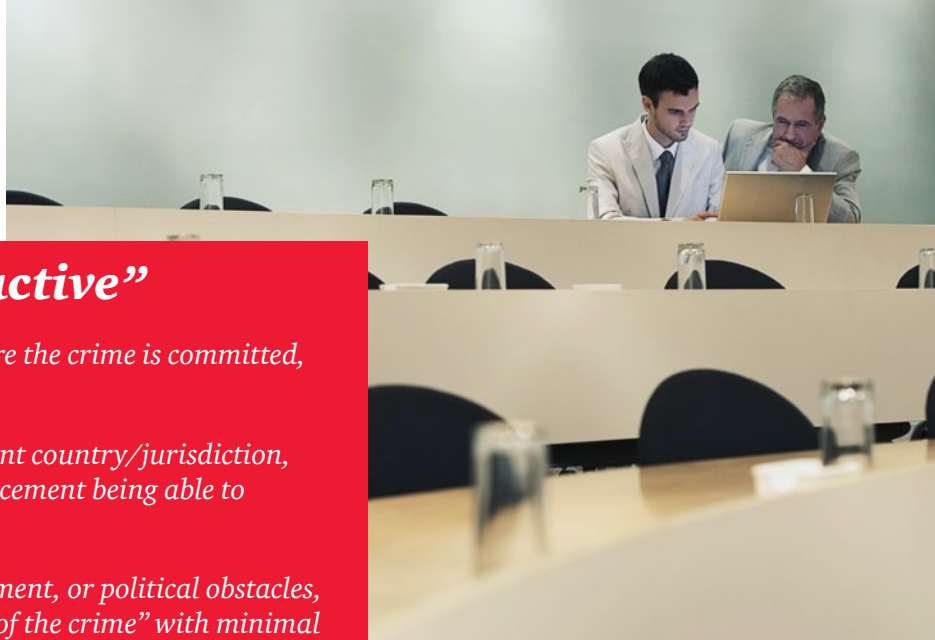
**98% of Czech respondents** stated that their perception of the risk of cybercrime has either increased (32%) or remained the same over the last year (66%). Only 2% perceive the risk to be falling.

Moreover, **30% of Czech organisations** believe their organisation **will likely face cybercrime** in the following 12 months; together with bribery and corruption and insider trading the highest percentage among all types of fraud. These statistics clearly show cybercrime to be an emerging and worrying threat.

*“In today’s technology world, more and more organisations are using web, mobile and social media platforms to improve their performance and serve customers more effectively. There is a dark side as well. As usage of new technologies increases, so do the scale and sophistication of cyber attacks. We clearly observe cybercrime to be on the increase in the current marketplace, in multiple cases we helped organisations to investigate how sensitive information leaked and who was responsible for that.”*

**Pavel Jankech**

Senior Manager, Forensic Technology Solutions,  
PwC Czech Republic



## Cybercrime is “attractive”

The fraudster is usually not present where the crime is committed, so there is less chance of getting caught.

The fraudster may be located in a different country/jurisdiction, there is then less of a chance of law enforcement being able to identify the perpetrator and punish him.

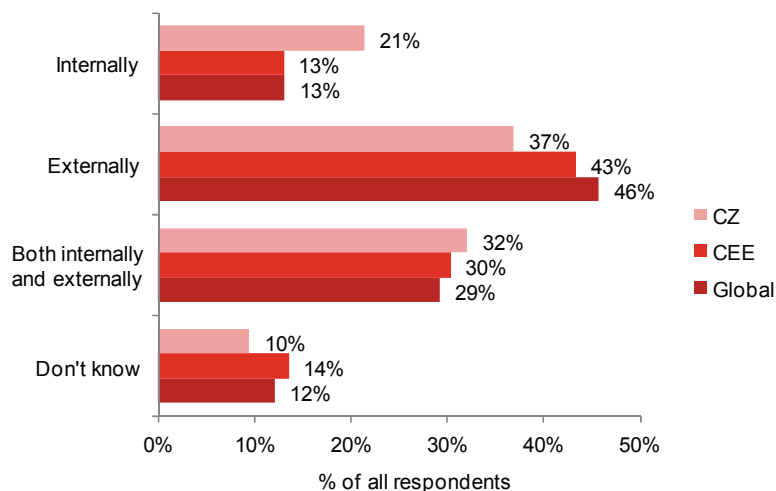
Due to a lack of geographic, law enforcement, or political obstacles, the perpetrator can return to “the scene of the crime” with minimal fear of detection.

The rapid change in technology makes it difficult for organisations to keep up with ways of preventing cybercrime.

## Is cybercrime really just an external threat?

Traditionally, cybercrime has been perceived as primarily an external threat. Our survey shows that this is starting to change: respondents in the Czech Republic see the cybercrime threat as coming from **within the organisation** itself (21%) and a further 32% consider the cybercrime to be an internal as well as external threat. This movement seems to be consistent across the globe.

### Where does the threat of cybercrime come from?



The **information technology (“IT”) department** is perceived as the most likely source of an internal cybercrime threat; this is consistent in the Czech Republic (51%), the CEE (53%) as well as globally (52%). It is not surprising that many respondents think this, because they expect IT personnel to have the necessary skills and opportunity to commit these crimes. In particular, IT personnel might have ‘super user’ access, which gives them extra administrative rights to access systems and the ability to delete audit trails, making it harder to detect their wrongdoing.

However, it is interesting to see that many Czech respondents also see a cybercrime threat coming from other departments: sales and marketing (31%), finance (22%), and operations (20%) also pose risks.

Respondents believe the risk of cybercrime is least likely to come from the legal (4%) or human resources departments (7%) – but organisations should not ignore these departments, as cybercrime can happen anywhere.



*“The way to get the business thinking about cybercrime is to talk about risk and not about encryption, penetration testing or firewall settings. Let them think about what can happen to the reputation of the firm if some of the critical data is lost.”*

**Filip Volavka**

Senior Manager, Forensic Technology Solutions,  
PwC Czech Republic

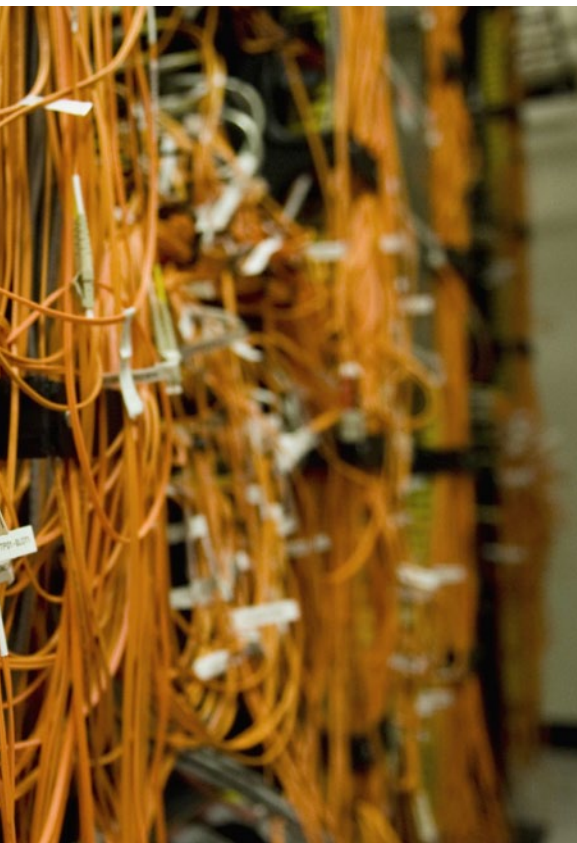
## What are organisations really worried about?

**IP theft**, including theft of data (71%), reputational damage (72%) and theft or loss of personal identifiable information (74%) are the top three effects of cybercrime that respondents in the Czech Republic are concerned about.

### Concerns about cybercrime



Due to the concerns that organisations have, it is very important for them to demonstrate that they are the most secure business in the market in order to achieve a competitive advantage. It becomes critical for organisations to market a safe and secure operational environment.



## Is your organisation like a deer in headlights?

As we saw earlier, **32%** of respondents perceive the risk of cybercrime to be growing. Based on reported frauds, cybercrime ranks in the top four types of fraud, and respondents said they are very concerned about the reputational damage cybercrime causes. But despite their concerns, the organisations are doing little about it and seem to be reactive rather than proactive to cybercrime threats.

Our survey shows that in the Czech Republic:

- **Surprisingly, 71%** of all respondents think that they have **in-house capabilities to prevent and detect** cybercrime; however
- **69%** do not have or are not aware of whether their organisation has access to Forensic Technology investigators;
- **2 out of 5** respondents have received **no cyber security training** in the past 12 months;
- **39%** of organisations do not have controlled emergency network shutdown procedures in place, or they are not aware of it.

### Keeping an eye on social media sites

**56%** of Czech respondents said their organisation does not monitor the use of social media sites, or they are not aware of it. This is startling, because these sites can present big security risks if employees abuse them.

While social media sites such as **Facebook or LinkedIn** may not be the real source of cybercrime, they can be used to social-engineer cybercrime more effectively (phishing attacks). For example, social media sites can be used to collect information about a targeted individual (also known as spear fishing), to research certain staff members or to install malware onto the user's computer, making the cybercrime more effective.

Of those Czech respondents who said their organisation is taking measures to prevent the risks, **92%** said they monitor internal and external electronic traffic including web pages, **62%** said their employee contracts cover how to use information and documents properly, and **35%** said they run training programmes. This suggests that those who are taking steps are doing it correctly, but the majority are exposed to threats like reputational damage and the loss of sensitive information by not having the right controls in place.

*“Social media is a revolution in the way in which people communicate. Also, businesses are engaging with social media for numerous reasons including marketing, communicating with customers, and collecting information. But there is a wide range of commercial risks related to their usage. In addition to increasing the amount of time that employees are unproductive, they create security risks for the organisation - they are another channel where sensitive data can leak or malicious code can get into the organisation.”*

**Pavel Jankech**  
Senior Manager,  
Forensic Technology Solutions,  
PwC Czech Republic

*“CEOs and Boards are still regarding information security as a technology issue. This is a perception that needs to be changed. The scale of the financial and reputational risks to a business means that information security should be one of the key board-level risk issues.”*

**Tomáš Kuča**  
Risk Assurance Partner,  
PwC Czech Republic  
and Slovakia

## **Who is ultimately responsible for dealing with cybercrime in an organisation?**

We have also asked respondents about who should ultimately own responsibility for managing cybercrime risks within their organisation. According to the results, **52%** of Czech respondents believe that the ultimate responsibility for managing cybercrime fraud within the organisation rests with the Chief Information Officer (“CIO”), and **29%** stating that the ultimate responsibility resides with the Chief Executive Officer (“CEO”) and the Board. This would indicate that, irrespective of whether the CIO sits on the Board, the ultimate responsibility is not shared with the CEO and the Board as a whole.

While we understand that managing the IT security risks is usually the responsibility of the CIO, the expectation is for the CEO and the Board to understand and probe into cybercrime risk related matters on a regular basis.

It is therefore not surprising that, according to our survey, the CEO and the Board do not routinely review the risks that cybercrime present to their organisation: **only 20%** of them review cybercrime threats more frequent than on an annual basis and **6%** do not review cybercrime threats at all.

The statistics indicate that the most senior people within organisations are not placing enough emphasis on the importance of managing the real threats that cybercrime present to their organisation. In the future, we believe that leadership by a CEO who truly understands the risks and opportunities of the cyber world will be a defining characteristic of those organisations – whether public or private sector – that realise the benefits and manage the risks most effectively.

## **What actions should organisations take to defend themselves against cyber security attacks?**

- 1. Get the CEO involved** – the CEO and Board need to be aware of the cyber threats. They need to understand the risks and opportunities of the cyber world.
- 2. Reassess the security function and preparedness** of the organisation should a cybercrime occur – unlike traditional ‘economic crimes’, cybercrime is fast paced with new risks emerging which means an organisation needs to continually adapt its procedures to reflect these.
- 3. Awareness** – organisations need to have a clear awareness of their current and emerging cyber environment. If this is in place, well informed and prioritised decisions and actions can be taken.
- 4. Create a cyber incident response team** – which needs to act with speed and agility. A well functioning cyber response team means that an incident spotted anywhere in the business will be tracked, risk assessed and escalated.
- 5. Educating all employees** – an organisation needs to embed a ‘cyber awareness’ culture, by recruiting those with the relevant skills so that this knowledge can be shared with all employees thus creating a cyber-aware organisation that is better able to protect itself.
- 6. Take a more active and transparent stance towards cybercrime** – take action by pursuing cybercrime perpetrators through legal means, and communicating more publicly regarding the actions the organisation is taking regarding the threats, incidents and responses.

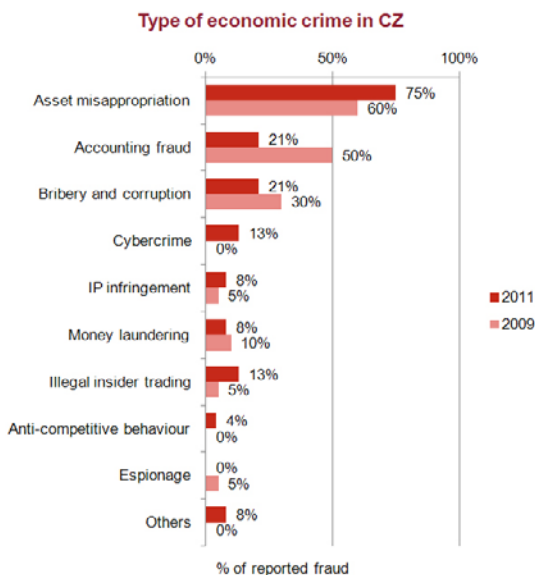
# The current fraud environment in the Czech Republic

## Do organisations know what they are facing?

Economic crime continues to be a serious issue affecting organisations worldwide, across the CEE and in the Czech Republic. **29% of organisations in the Czech Republic experienced one or more economic crimes in the past 12 months;** slightly below the average for the CEE (30%) and globally (34%). For the Czech Republic, this represents an increase by 5 percentage points.

## So what types of economic crime are we talking about?

### Type of economic crime in the Czech Republic



**Asset misappropriation** remains the most common type of economic crime reported in the Czech Republic (75%) in the CEE (69%) and globally (72%). This is not surprising, given the fact that it is easier to detect compared to other types of economic crimes. **Together with cybercrime**, asset misappropriation appears to be the main contributor to the overall increase in percentage of organisations affected by economic crime.

The next most common type of fraud in the Czech Republic is **Accounting fraud (21%)** jointly with **Bribery and corruption (21%)**. While the reported incidents of both these types of fraud decreased in comparison with 2009, we should be careful in drawing conclusions that are too optimistic:

- Our experience shows that the actual incidence of bribery and corruption is likely to be higher as this type of crime is difficult to identify and often goes undetected. The CEE average of 36% also indicates that the actual incidence of bribery and corruption in the Czech Republic is likely to be higher.
- As for accounting fraud, our survey shows that there was a global trend indicating an overall decrease in this type of economic crime. In the Czech Republic, however, this decrease was even more significant than in other countries.

There could be various reasons for the decrease in accounting fraud including:

- Organisations may have put tighter controls in place, which deter perpetrators;
- There is a possibility that senior management in organisations no longer feels similar pressures as two years ago when they struggled to survive in difficult times and, therefore, management felt the pressure to commit financial statement manipulations;
- Another possible reason for the drop in the number of accounting frauds since 2009 could be due to the fact that economic crime is not being detected accurately due to reductions in headcounts within organisations globally over the past couple of years resulting in fewer resources being available within departments responsible for detecting and preventing economic crime; or
- Given the focus of our survey on cybercrime this year, it is possible that some of the respondents who used to classify accounting frauds involving the use of computers, electronic devices, systems, and the internet may have reclassified it as a cybercrime this year.

## How much does fraud cost, and what is the collateral damage?

Almost **38%** of those Czech respondents who said they had experienced economic crime in the past 12 months reported losses of **more than USD 100 000**, **8%** suffered losses over **USD 5 million**.

Of those who had experienced economic crime as a result of fraud, **67%** reported perceived damage to employee morale, **38%** to business relations, and another **25%** to reputation/brand.

### Collateral damage in the Czech Republic



## Who is committing fraud?

In line with our experience, the most frauds in the Czech Republic had been committed by internal fraudsters (**67%**), this number has increased significantly in comparison to 2009 (**50%**). The prevalence of internal fraudsters may be because employees are involved in the day-to-day business and tend to have a better understanding of the “inside environment” and are therefore in a better position to perpetrate fraud.

**Customers (43%)** and **vendors (29%)** were identified as the main perpetrators of external fraud. The number of external frauds carried out by agents/intermediaries has dropped significantly in the Czech Republic compared to 2009, i.e. by more than **40 percentage points**.

One of the key fraud prevention techniques is to know who you are doing business with. Thus, know your customer and vendor due diligence is becoming more recognised as a critical element of risk reduction programmes. These transparency programmes remain one of the more effective preventative tools available to organisations.

*“As a confident choice goes hand in hand with precise information, it is recommended that organisations implement background checks into their normal business procedures. Background checks cannot only help organisations to assess potential risks coming from external parties such as vendors and intermediaries, but also to assess the risks coming internally. Background checks can be implemented into the organisation’s hiring process thus providing valuable information prior to the individual being hired and can also be performed regularly in order to assess any potential conflicts of interest that current employees could have.”*

**Eva Křištofová**  
Manager, Forensic Services, PwC Czech Republic



## *What do organisations do with the fraudster?*

In the case of internal perpetrators, **dismissal** was the most frequent action taken in the Czech Republic, in **81%** of cases, and **50%** said they informed the police. It is worth noting that the **number of cases where management decided to fire the fraudster has risen** in the Czech Republic (2009: 65%), CEE (75% in 2011 vs. 54% in 2009) and globally (77% in 2011 vs. 60% in 2009). This is a very positive result as it reveals that organisations are less likely to “sweep these incidents under the carpet”..

Similarly, Czech organisations showed a low level of tolerance with external wrongdoers: when dealing with the external fraudster, **86%** of Czech respondents said their organisation informed the police and **71%** of Czech organisations subsequently **ceased the business relationship** with the external perpetrator; representing a dramatic increase compared to 2009 (**30%**) and being well above the CEE (**53%**) and

global average (**39%**).

Overall, the results clearly indicate that most Czech organisations are taking the right approach towards fraudsters and thus send the right message regarding their perception of fraud within their organisation and to the outside. We would, however, recommend that organisations also step up their efforts on the prevention front: knowing your employees and business partners prior to engaging with them is less costly than dealing with the consequences of fraud.

*“In order to increase the effectiveness of a whistle-blowing system, there are a couple of critical steps to be done preceding its implementation such as understanding and correctly evaluating corporate culture, setting the targets and their communication, selecting appropriate instruments to be used. It is also important to have a clear plan of how the announced incidents will be solved and what messages will be sent to the other employees.*

*An effective whistle-blowing system not only increases the likelihood of preventing wrongdoing and criminal behaviour, it also sends a positive signal to business partners and the public at large and reduces the risk of a negative reputation emerging.”*

**Jiří Urban**

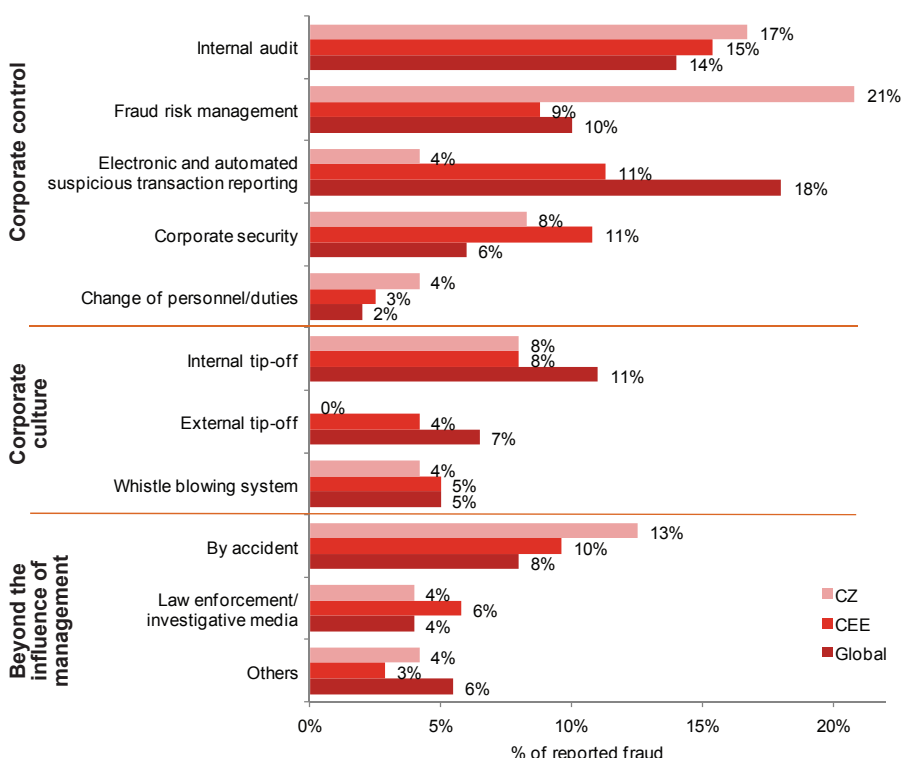
Senior Manager, Forensic Services, PwC Czech Republic

## How do organisations detect fraud?

It is encouraging that an increasing number of fraud incidents is detected via systematic mechanisms: **38%** of Czech organisations have detected fraud through either **fraud risk management** or regular **internal audit procedures** (in 2009: **35%**). In particular, we were pleased to see that the percentage of economic crimes detected by fraud risk management (21%) is significantly higher than in the CEE (9%) or globally (10%).

It is also positive to see a decrease in the number of incidents of economic crime being detected accidentally in the Czech Republic, or by other means that were beyond the influence of management (**21%**) compared to 2009 (**30%**). This suggests that Czech organisations are **increasingly less willing to rely on chance** to detect fraud. However, with **1 out of 5 frauds** still being detected beyond the influence of management, there continues to be room for improvement in this area:

### Detection methods



- 4% ‘electronic and automated suspicious transaction reporting’ plays only an insignificant role when detecting fraud in the Czech Republic, although it has grown globally from 5% in 2009 to 18% in 2011. In our view, this can be a very powerful tool as it is based on an electronic automated system that initially detects irregularities and suspicious transactions without human intervention.
- 71% of Czech organisations **do not employ a whistle-blowing mechanism**. This is very surprising as in our experience the anonymous whistle-blowing mechanism helps to discover fraud in many cases when other means of fraud detection prove ineffective.

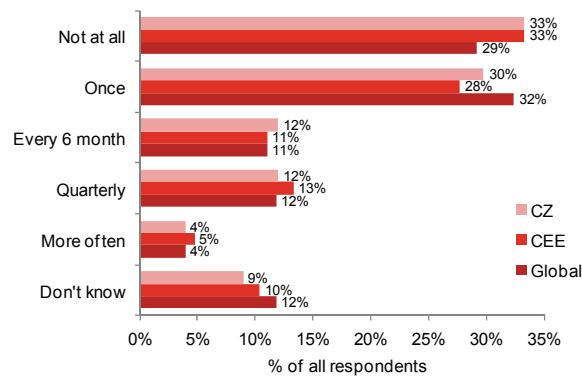
## How fraud risk assessments can really help organisations?

In order to prevent fraud, it is important for organisations to assess the risks and identify the gaps. Regular fraud risk assessments help organisations to analyse their exposure to fraud. The results of our survey show a clear correlation between the frequency of organisations performing fraud risk assessments and the incidents of fraud reported.

It is therefore of concern that 42% of Czech organisations surveyed reported that they had **not performed any fraud risk assessment** (33%) or they did not know if they had (9%); another 30% had performed only one fraud risk assessment in the last 12 months.

The main reasons Czech organisations gave for not performing fraud risk assessments were a **perceived lack of value** (57%) and lack of knowledge about what fraud risk assessment involves (21%). This suggests that there is an awareness problem.

Frequency of fraud risk assessments



*“Organisations need to understand the benefits of doing regular fraud risk assessments and how important they are in the fight against fraud. As fraud in its essence entails intentional misconduct, it is designed to evade detection. To busy managers who must deal with many urgent and critical business issues, conducting a fraud risk assessment might look like an activity of low importance, but a well designed and effective fraud risk assessment could identify where fraud might occur and anticipate the behaviour of a potential fraud perpetrator.”*

**Kateřina Halásek Dosedělová**

Senior Manager, Forensic Services, PwC Czech Republic

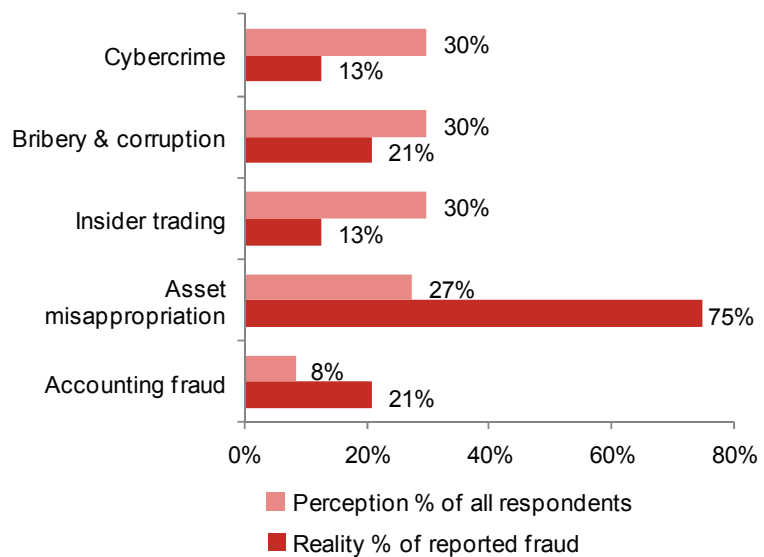


## ***Fraud in the future***

30% of Czech organisations consider each bribery and corruption, cybercrime and insider trading as types of fraud their organisation may face in following 12 month; another 27% considers asset misappropriation a likely future threat.

However, alarmingly, most organisations in the Czech Republic still think it is unlikely that their organisation will be subject to economic crime in the next 12 months. For example only 8% of Czech respondents think their company could face accounting fraud. Given the current development of the world economy this may well be just a false illusion of safety.

### Perception vs Reality in the Czech Republic



---

## ***Notes***

# Forensic services

## Contacts in the Czech Republic



### Sirshar Qureshi

Forensic Services Partner,  
PwC Czech Republic

telephone: +420 251 151 235

e-mail: [sirshar.queshi@cz.pwc.com](mailto:sirshar.queshi@cz.pwc.com)



### Michal Kohoutek

Forensic Services Director,  
PwC Czech Republic

telephone: +420 251 151 231

e-mail: [michal.kohoutek@cz.pwc.com](mailto:michal.kohoutek@cz.pwc.com)



### Kateřina Halásek Dosedělová

Forensic Services Senior Manager,  
PwC Czech Republic

telephone: +420 251 151 293

e-mail: [katerina.halasek-dosedelova@cz.pwc.com](mailto:katerina.halasek-dosedelova@cz.pwc.com)



### Jiří Urban

Forensic Services Senior Manager,  
PwC Czech Republic

telephone: +420 251 151 627

e-mail: [jiri.urban@cz.pwc.com](mailto:jiri.urban@cz.pwc.com)



### Pavel Jankech

Forensic Technology Solution Senior Manager,  
PwC Czech Republic

telephone: +420 251 151 336

e-mail: [pavel.jankech@cz.pwc.com](mailto:pavel.jankech@cz.pwc.com)



### Filip Volavka

Forensic Technology Solution Senior Manager,  
PwC Czech Republic

telephone: +420 251 151 269

e-mail: [filip.volavka@cz.pwc.com](mailto:filip.volavka@cz.pwc.com)