





Economic crime is a persistent threat

Global and Hungarian Economic Crime and Fraud Survey 2018



Content

	1. More impactful frauds committed in diverse ways	5
	Is fraud on the increase – or just our awareness of it?	5
	Blind spots: what are we still not seeing?	5
	Knowing what fraud looks like	6
	Be careful of the people you do business with	7
	The cost of fraud still substantial	8
	Beyond the costs	9
	Meeting the market expectations	10
	2. Hot topics among fraud types	11
	2.1 Cybercrime: a disconnect between ends and means	11
	2.2 Business misconduct and the underlying conduct risk	13
	2.3 Bribery and corruption: a likely blindspot	14
	2.4 Money laundering	15
	3. Are you prepared?	16
	3.1 Having the right policies in place sufficient?	16
	3.2 Systemic mechanisms plays important role in fraud detection	18
	3.3 Compliance programmes and funds used to combat fraud and economic crime	19
	4. Harness today's technology to fight today's fraud	20
	Technology adoption trends: finding the sweet spot	22
	Customers aren't just one consideration of your business	22
	Where would your customers money go?	23
	The business case	23

Preface

We are pleased to present to you the results of *Global and Hungarian Economic Crime and Fraud Survey 2018*, 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 organisations' awareness about economic crime we collected responses from 7,228 organisations from 123 countries, including 71 leading companies within Hungary.

Beyond offering valuable data on the evolution and current state of fraud this year's Economic Crime and Fraud Study 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.

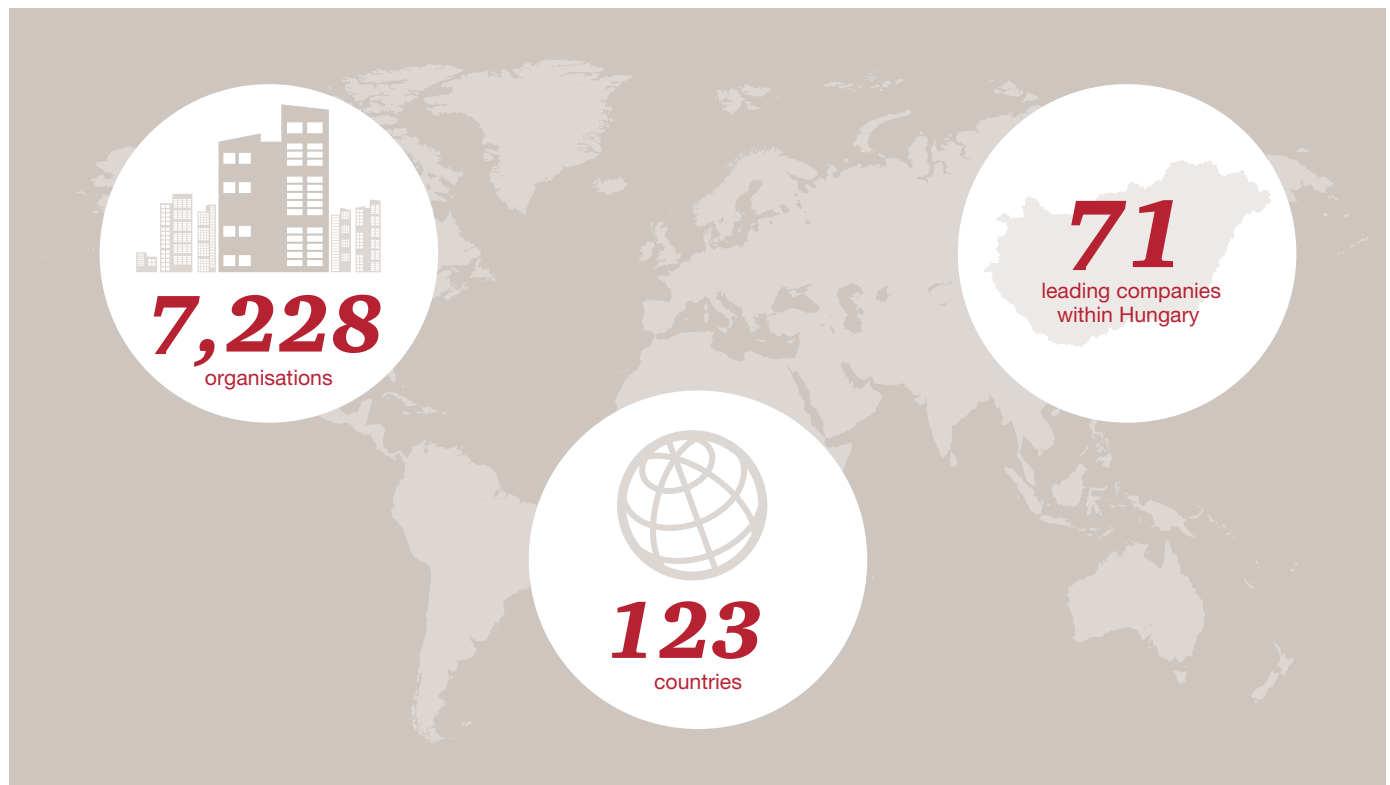
Our survey shows that many companies are under-prepared to face fraud, for both internal and external reasons. That's why a clear understanding of what constitutes 'fraud' – and what measures can and should be taken to prevent it – needs to be shared across the organisation. Throwing light on your blind spots can also unlock significant opportunities.

Fighting fraud has progressed from an operational or legal matter to a central business issue. Fraud today is an enterprise that is tech-enabled, innovative, opportunistic and

pervasive. Look at it as the biggest competitor you didn't know you had. It's not hard to see how we got here. Technology has advanced in leaps and bounds; fraudsters are more strategic in their goals, more sophisticated in their methods; and regulatory regimes have become far more robust – with enforcement intensifying around much of the world, often in cross-border cooperation.

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, a lack of awareness of its role within an organisation is a dangerous place to be. So the important question isn't: 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?

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



Highlights



The current fraud environment in Hungary

- In our *Survey* 49% of global organisations recognised that they'd been a victim of fraud and economic crime. For Hungary this figure is even higher at 51%.
- Asset misappropriation (42%) remained the first among most frequently committed economic crimes among the survey respondents in Hungary. It is followed by the 'new' frauds – ones whose prominence has grown so much that we have measured them as separate threats for the first time. These include fraud committed by the consumer (at 39%) and business misconduct (28%) – in 2nd and 4th place, respectively, among all reported frauds.
- The biggest threats are the people you have invited to do business with. The survey shows that the perpetrator of the most disruptive fraud and/or economic crime in Hungary was external (58%) – a notable change compared to our previous survey (33%). Even when the fraudster was external, a sizable percentage of that 'external' group includes so-called 'frenemies': third parties – agents, vendors – and customers.
- The cost of fraud still substantial: among the survey respondents 45% of organisations that suffered economic crime have lost approximately USD 100,000 in Hungary.



Cybercrime

- Cybercrime has long passed its infancy and adolescence and increased significantly compared to our last survey in 2016 – it is ranked the third most frequently committed crime.
- 31% of the respondents experienced cybercrime related fraud and now Hungary is on level with the global results. Historically cybercrime produced the greatest increase among all types of economic crimes compared to the last survey.

- It occurs in various forms – in Hungary malwares (44%) and phishing (37%) seemed to dominate.
- There is growing awareness in this topic among Hungarian companies which is reflected in the increasing number of Cyber Security Programs to deal with cyber attacks. 72% of the respondents stated that their companies have a Cyber Security Program to deal with cyberattack which is fully in operation compared to the 42% reported in the *2016 Survey*.
- Nevertheless 10% of the Hungarian respondents stated that their respective companies don't have a plan yet and not even assessing the feasibility to implement one.



Ethics and Compliance

- C-level executives are increasingly held personally responsible for economic crimes and fraud both by the regulator and by the public. This is supported by fact that 17% of Hungarian respondents stated that the CEO had primary responsibility for the company's formal business ethics and compliance programme.
- An increasing number of fraud incidents are detected via systemic mechanisms in Hungary, as the reliance on corporate controls in fraud detection has grown to 52% from 42% reported in the *2016 Survey*.
- Twenty-one percent of economic crime was still detected beyond the influence of management in Hungary.

1. More impactful frauds committed in diverse ways

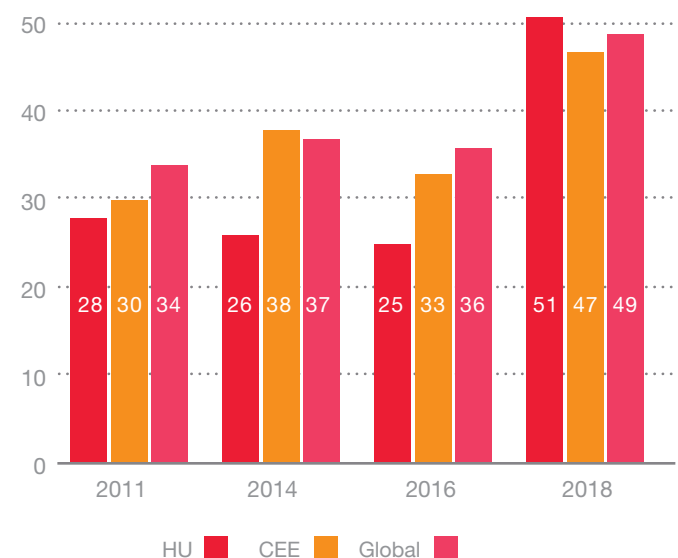
Is fraud on the increase – or just our awareness of it?

More than a half of Hungarian organisations have experienced economic crime in the past 24 months according to respondents to PwC's *Hungarian Economic Crime and Fraud Survey 2018*, which represents a 100% increase compared to our last survey.

But that's not the whole story – potentially, it's the opposite of the story. The reality is more likely that this statistic measures not actual fraud, but awareness of fraud. It is in that awareness gap that we venture to demonstrate with this report. We explore not only what is visible, but the blind spots that are blocking companies from seeing the fraud in their midst, and what they can and should do about them.

Fig 1

Question: Has your organization experienced any economic crime in your country within the last 24 months? (%)



Blind spots: what are we still not seeing?

As we will discuss in this report, every organisation is vulnerable to 'blind spots' – the awareness or responsibility gaps that can bedevil even the best-run companies. Most times, you discover it only after an incident – a major cyber breach, notification of a regulatory inquiry or enforcement action, an embarrassing story in the press, an external or

internal tip-off. But here's the upside: by throwing light on those 'blind spots', you will find opportunities to take preventive action and make significant improvements in your fraud-fighting efforts. That's the focus of this year's *Hungarian & Global Economic Crime and Fraud Survey*.

Knowing what fraud looks like

Asset misappropriation (42%) remained first among the most frequently committed economic crimes reported by the survey respondents in Hungary. It is followed by the ‘new’ frauds – ones whose prominence has grown so much that we have measured them as separate threats for the first time. These include fraud committed by the consumer (at 39%) and business misconduct (28%) – in 2nd and 4th place, respectively, among all reported frauds. We believe the inclusion of these two categories is partially responsible for the decrease (from 46% in 2016 to 42% in 2018) in the larger category of asset misappropriation. Cybercrime, at 31%, is ranked third. This is in line with Eastern European and global results as asset misappropriation, cybercrime and frauds committed by the consumer are present and cause problems everywhere.

The most frequently committed economic crimes and fraud cases were the most disruptive ones too: Hungarian respondents found fraud committed by the consumer the most disruptive (39%), asset misappropriation ranked second (22%) and cybercrime along with bribery and corruption ranked third (both 14%-14%).

Fig 2
Question: What type of fraud and/or economic crime has your organization experienced in your country within the last 24 months? (%)

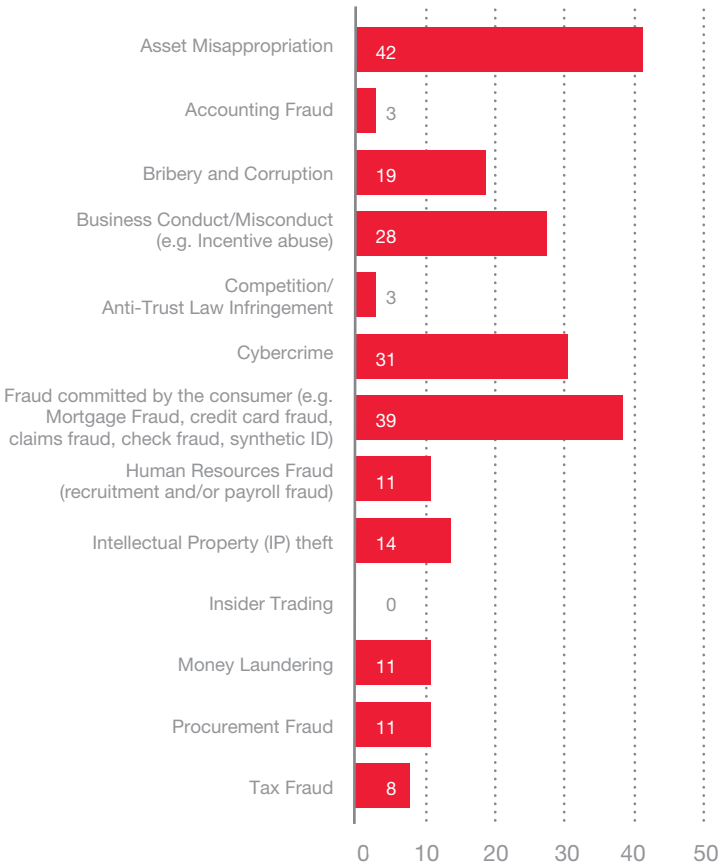
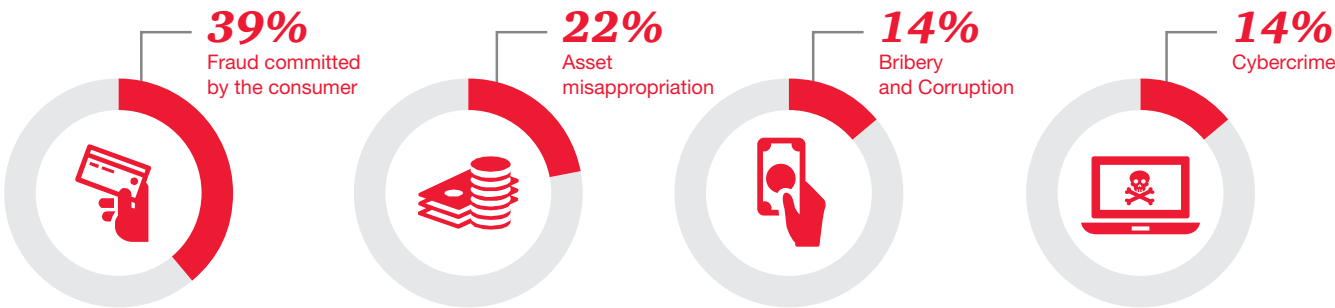


Fig 3
Question: Of the fraud and/or economic crimes experienced by your organization in the last 24 months, which was the MOST disruptive/serious in terms of the impact on your organization (monetary or otherwise)? (%)

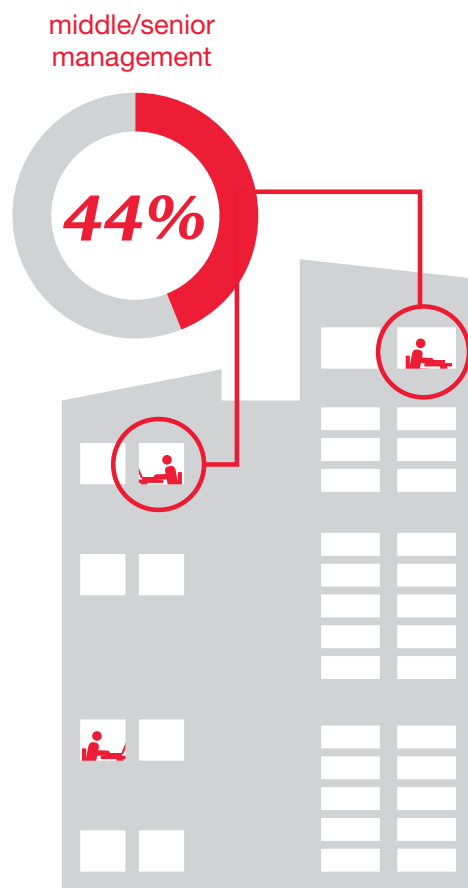
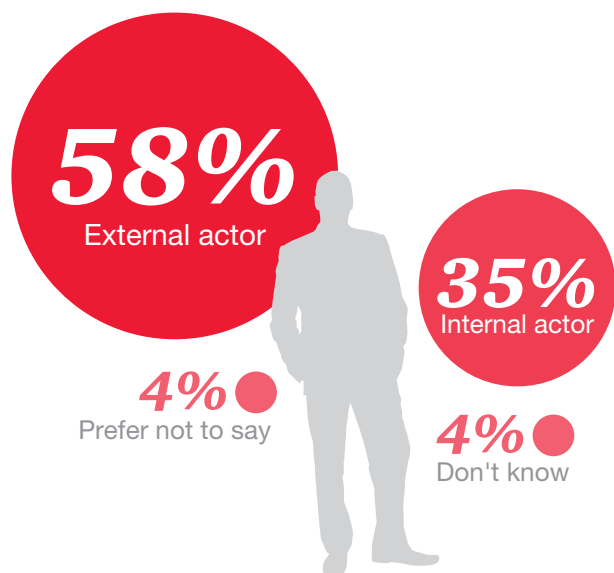


Be careful of the people you do business with

One of your biggest blind spots – and biggest threats – are the people you have invited to do business with. The survey shows that the perpetrator of the most disruptive fraud and/or economic crime in Hungary was more likely to be external (58%) – this is a notable change compared to the result of our previous survey (33%). Even when the fraudster was external, a sizable percentage of that ‘external’ group includes so-called frenemies: third parties – agents, vendors – and customers. In other words, people and entities with whom one would expect a certain degree of mutual trust, but who are actually stealing from the company.

Taking a closer look at the statistics profiling perpetrators, we also see that he or she typically has mostly operations and production roles, but can also come from any level of the organization (even in 44% of the cases the perpetrator was part of the middle/senior management!)

Fig 4
Question: Who was the main perpetrator of this fraud? (%)



The cost of fraud still substantial

When asked to quantify the direct financial loss to the organisation caused by its most disruptive crime over the past two years, 45% of organisations that suffered economic crime have lost USD 100,000 or more in Hungary. Globally 64% of respondents said the loss could reach up to \$1 million; 16% pointed to a loss of between \$1 and \$50 million; the only notable difference is that no Hungarian respondent reported a loss over 50 million.

But when secondary costs such as investigations and interventions are added in, the overall expense can increase substantially further. One in two companies in Hungary spent at least the same amount on investigations and/or other interventions as the fraud had initially cost. This illustrates well that the cost of remedial actions (such as investigations, litigation) can easily exceed the cost of establishing a robust anti-fraud programme.

Fig 5
Question: In financial terms, approximately how much do you think your organization may have directly lost through the most disruptive crime over the last 24 months? (%)

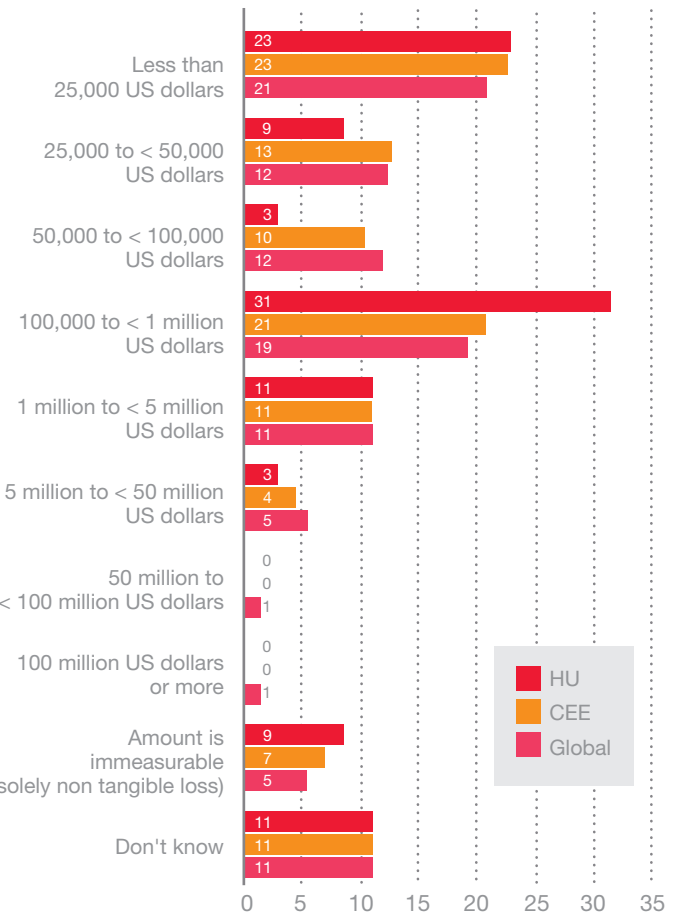
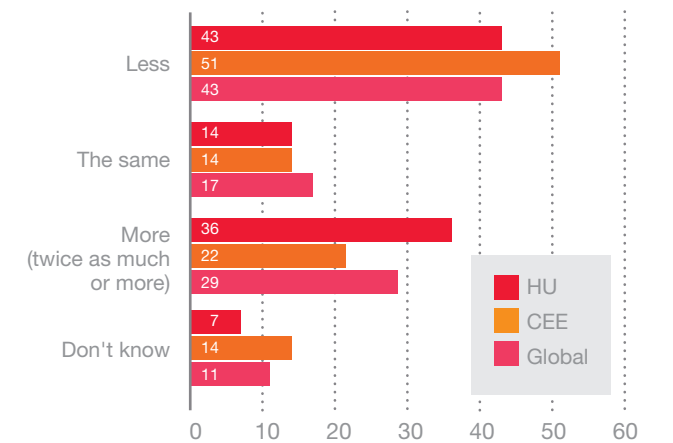


Fig 6
Question: As a result of the most disruptive crime experienced in the last 24 months, was the amount spent by your organization on investigations and/or other interventions, more, less or the same as that which was lost through this crime? (%)



Beyond the costs: Rightly or wrongly, the CEO and board are accountable

When the financial costs of fraud hit the bottom line, it's natural for senior management to be called on the carpet by the board and shareholders. Today, that responsibility doesn't stop there: it begins there.

Chief executives are increasingly seen as the personal embodiment of an organisation, expected at all times to have their finger on the pulse of every facet of its culture and operations. And when ethical or compliance breakdowns happen, business leaders are often held personally responsible – both in the court of public opinion and, increasingly, by regulators

Csaba Polacsek
Partner
Advisory Services
PwC Hungary



Whatever the merits of such an aggressive response, the C-Suite can hardly claim ignorance as an excuse. Our survey shows that practically always (97%), the most serious incidents of fraud have been brought to the attention of senior management in Hungary.

Furthermore, of the 81% of Hungarian respondents who indicated their organisation had a formal business ethics and compliance programme, 17% said the CEO had primary responsibility for it.

Fig 7

Question: Was the most disruptive incident you indicated brought to the attention of your board level executives or to senior leaders charged with governance?

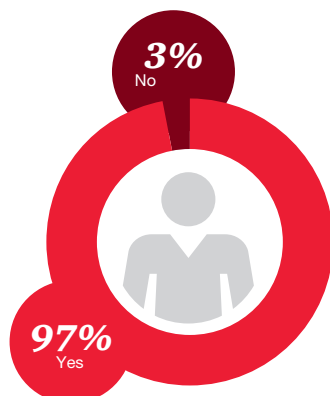


Fig 8

Question: Do you have a formal business ethics and compliance program in your organization?

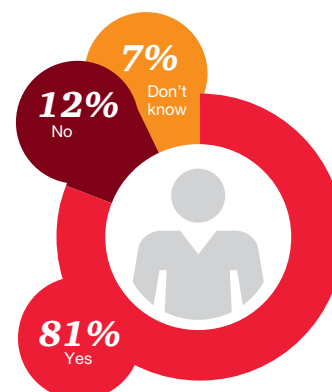
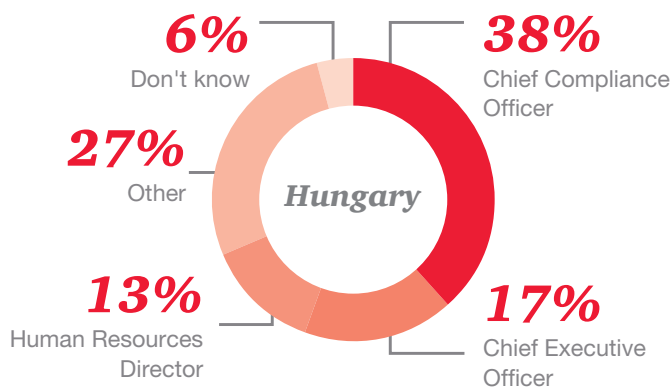


Fig 9

Question: Who has primary responsibility for the business ethics and compliance program in your organization?



This puts a sharp spotlight on how the front office is managing the crisis – and the extent to which they are (or are not) adjusting their risk profiles accordingly. Our *2018 21st CEO Survey* underscores this theme, with chief executives citing trust and leadership accountability as two of the largest business threats to growth.

Meeting the market expectations

Many companies are finding themselves caught in a tug of war between three business drivers: the market's appetite for innovative disruptors; shareholders' desire for financial outperformance; and society's expectations for ethical conduct. The truth is that when business is going gangbusters, investors tend to look the other way. The C-Suite should be careful not to. Organisations can easily be lured into a false sense of security when scenarios appear to be rosy, and when the 'tone at the top' appears to consist of the right words.

The market may love disruptors or outperformers – but not enough to tolerate bad behaviour. No matter how much of a stock-market darling a company is today, if every aspect of conduct risk has not been managed carefully and soberly, both company and leadership could lose much of its goodwill faster than it acquired it.

There is plenty of promise, however, among the start-up generation. Many of these fast-growing firms are led by younger entrepreneurs with an ethical viewpoint baked in. Unburdened by legacy processes or poorly integrated systems, they are ideally positioned to embed up-to-date fraud data analytics from the start – a tremendous competitive advantage in an era of multiplying fraud. These fresh-faced firms could help model a new era of both transparency and profitability.



2. Hot topics among fraud types



2.1 Cybercrime: a disconnect between ends and means

Cybercrime long past its infancy and adolescence. Today's cybercriminals are as savvy and professional as the businesses they attack. This new maturity calls for a new perspective on the many aspects of this threat – and on the ways in which it can lead to dangerous fraud.

This sentiment is echoed in Hungary, as Cybercrime has increased significantly compared to our last survey in 2016. Thirty-one percent of the respondents experienced cyber-crime-related fraud and now Hungary is on the same level as the global results (31%). Historically this was the greatest increase among all types of economic crimes. A contributing factor to the growth in cybercrime is the appearance of global ransomware (including Petya and WannaCry) in Hungary, as they have infected several local companies in the past 24 months.

Unsurprisingly, cybercrime occurs in various forms and many of them have been identified in Hungary, but malware (44%) and phishing (37%) seemed to dominate.

The most frequented type of cyber attacks in Hungary (percentage of respondents faced this kind of attacks in the past 24 months)

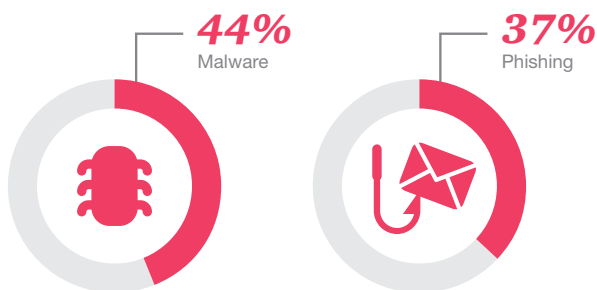
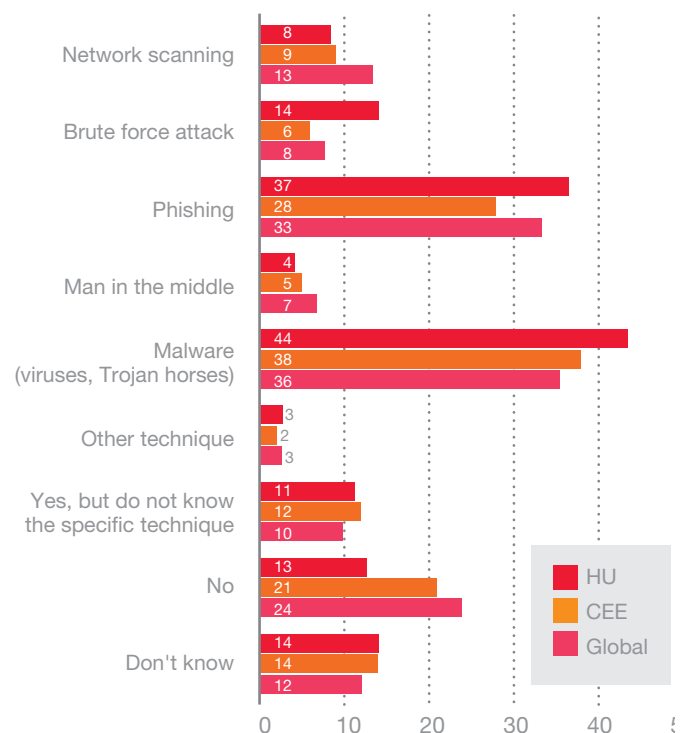


Fig 10

Question: In the last 24 months, has your organization been targeted by cyber-attacks using any of the following techniques? Please select ALL that apply

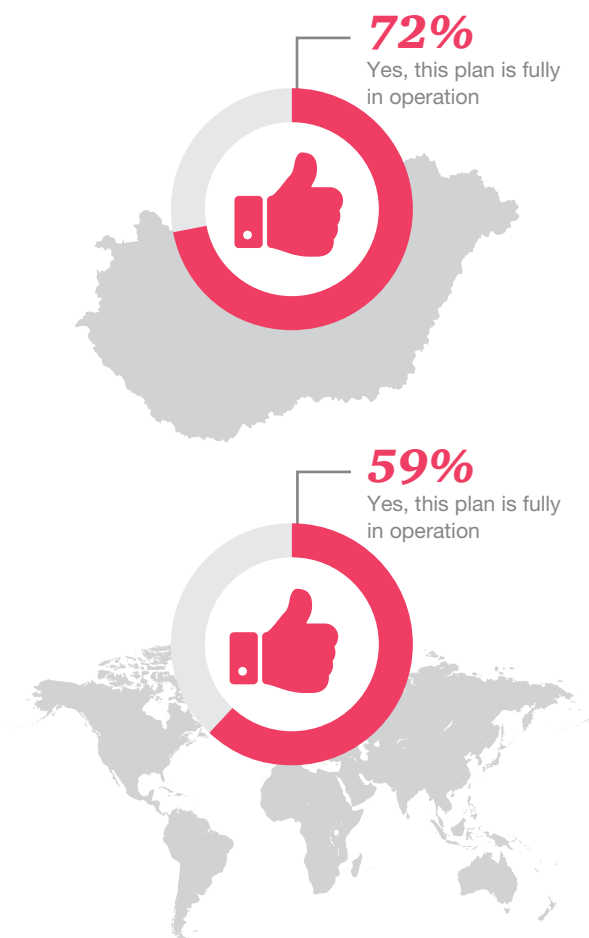


It should also be noted that there is growing awareness of this topic among Hungarian companies, which is reflected in the increasing number of incident response plans for dealing with cyber attacks. Seventy-two percent of the respondents stated that their companies have an incident response plan for dealing with cyberattacks that is fully in operation compared to the 42% reported in the *2016 Survey*, which represents an enormous increase and significantly exceeds the global average (59%).

Nevertheless companies who don't have a plan yet and who are not even assessing the feasibility of implementing one (10% of the Hungarian respondents), are exposing themselves to serious risks.

Oftentimes, the first sign an organisation will get that something systemic is amiss will be through some kind of cyber-enabled attack. The increasing frequency, sophistication and lethality of such attacks is spurring companies to look inside at their operations for ways to pre-empt the attack. This can have the benefit of pushing them into a deeper focus on fraud prevention. But here again, there is a potential blind spot – beyond prevention, it's one of perception. Where once all forms of cyber attack were lumped together, from a fraud perspective it is important to distinguish between the breach itself (the breaking and entering by the threat actors) and how the breach actually affects the organisation. What is of interest today is not so much the smashed door as what happened after the culprit got in – and how to stop it happening again.

Fig 11
Question: Does your organization have a Cyber Security Program (preventative/detective) to deal with cyber-attacks? (%)





2.2 Business misconduct and the underlying conduct risk: the ‘hidden risk’ behind most fraud

Conduct risk is a relatively new phenomenon to which regulators have shifted their attention in recent years after some high profile scandals (financial benchmark rigging and product mis-selling, for instance), but its relevance is by far not limited to the financial services industry.

Csaba Polacsek

Fraud is too easily brushed under the carpet, seen as ‘someone else’s problem’. We have found that in most organisations, not only are compliance, ethics and enterprise risk management separate functions, they often exist in separate universes. And, like all silos, they rarely add up to (or act as) a strategic whole.

The best way to approach these disparate areas is to reframe them as components of a larger, more fundamental category called conduct risk – the risk that your employees’ actions will

contravene their training. From there you can measure and manage them horizontally, and embed them in your larger strategic decision-making process. Unlike operational breakdowns or external threats, which can often be checked by internal controls and processes, conduct risk requires a more holistic response – and a shift in attitude. When the issue is reframed as conduct risk, it can be approached more dispassionately – as a fact of life with which every organisation, without exception, has to deal.

Adopting this more systemic (and realistic) stance toward conduct risk not only enables cost efficiencies between your ethics, fraud and anti-corruption compliance programmes, it can also help de-intensify the emotions that frequently accompany ethical breaches. Most important of all, it can break down the silos between your key anti-fraud functions – and help pull fraud out of the shadows.

Another reason for misconduct in Hungary is the lack of training and culture, and insufficient management oversight. SMEs and startup companies are prone to fast growth without investing in compliance and establishing lines of defense which can be the hotbed of fraud.





2.3 Bribery and corruption: a likely blindspot

Surprisingly, bribery and corruption were not ranked among the three most common economic crimes in Hungary for first time since the 2007 survey; it was ranked only 5th as 19% of the respondents have experienced corruption at their companies in the past 24 months – in spite of the slightly increasing Eastern European and global trends.

Additionally, the growing number of enforcement actions (including cross-border actions), the updated OECD framework, and newly adopted national anti-corruption legislation (for instance the new French anti-corruption act) will keep compliance departments dealing with ABC busy in the forthcoming months.

The high proportion of Hungarian respondents who are unsure if their respective organization had been asked to pay bribe (44%), or had lost an opportunity to a competitor they believed paid a bribe (59%) in the last 24 months, however, is worrisome, and adds real cause for a concern/suspicion. This also illustrates well the hidden nature of corruption - this is why we consider corruption a likely/genuine blindspot in Hungary.

Csaba Polacsek

Fig 12

Question: In the last 24 months has your organization Been asked to pay a bribe? (%)

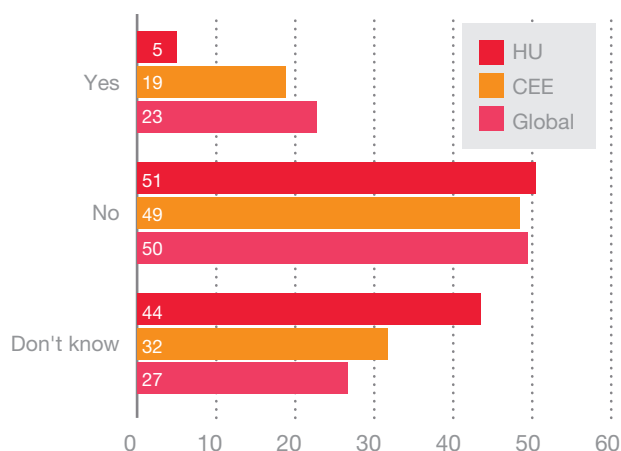
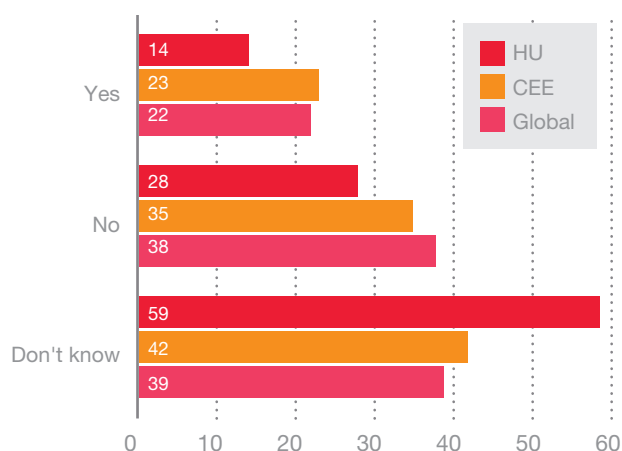


Fig 13

Question: In the last 24 months, has your organization been targeted by cyber-attacks using any of the following techniques? Please select ALL that apply





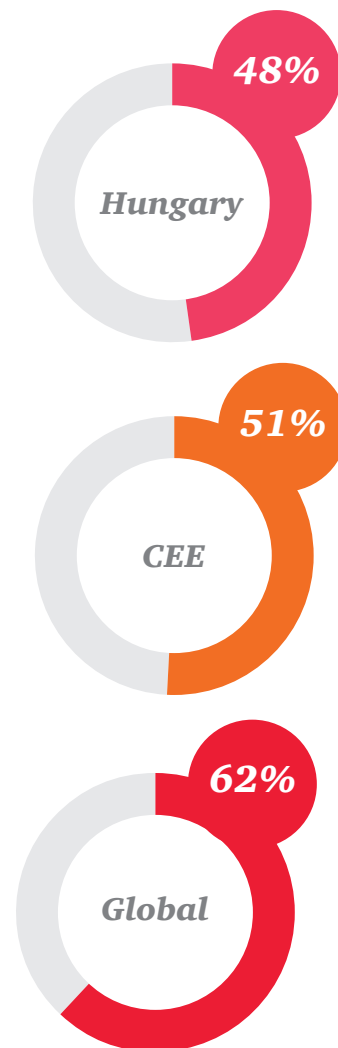
2.4 Money laundering: legislation changes are driving the growth in AML risk assessments at institutions

Since our last survey, the European Parliament has adopted the fourth Anti-Money Laundering Directive. EU Member States, including Hungary, had to transpose this Directive into national legislation by 26 June 2017. We assume this legislation change was one of the key driving force behind the rising number of AML/CFT (Anti Money Laundering/Combating Financing of Terrorism) risk assessment as 48% of the Hungarian respondents stated that their respective organization performed such assessment across its business and geographies in the last 24 months - this ratio is slightly below the Eastern European (51%) and the global (62%) average. It is hard to evaluate these results without detailed information about the background of the respondents but one of the key messages of recent money laundering scandals was that many non-financial companies – commercial/trading and manufacturing companies – were exposed to the danger of money laundering and some were actually involved. In addition, non-financial companies usually have less cautious approaches towards AML/CFT compliance than traditional financial institutions while trade-based money laundering red flags are among the hardest to detect.

Interestingly, only 5% of Hungarian respondents stated that they are/were under an AML-related enforced remediation program or they had AML compliance shortcoming related regulatory inspection and received major feedback to address in the past 24 months. In contrast, this ratio was 23% in Eastern Europe and 32% globally among the respondents. With a few exceptions there were not many serious AML related fines and penalties in Hungary unlike in Western Europe or in the US. However, this might change in the future.

Fig 14

Question: Organizations which performed an AML/CFT (Anti Money Laundering/Combating Financing of Terrorism) risk assessment across its business and geographies in the last 24 months (%)



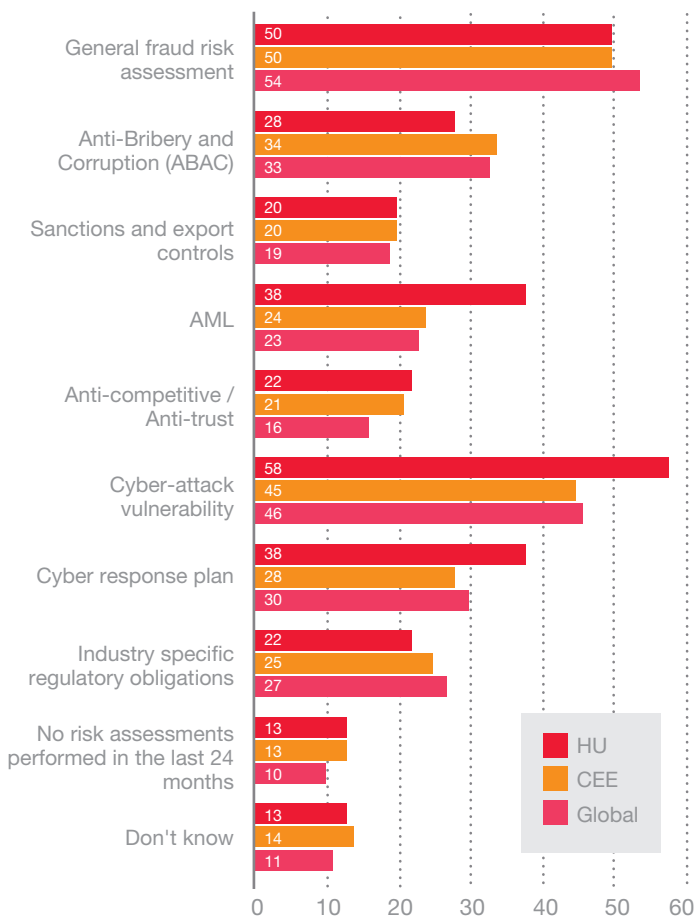
3. Are you prepared?

3.1 Having the right policies in place sufficient?

Since our last survey, we have seen some progress in the amount of fraud detection measures taken by respondent companies. This is a good thing: not only can a fraud risk assessment help you identify the unique and specific fraud risks you should be looking for, these assessments are increasingly favoured by regulators in enforcement actions. Still, our survey shows there is significant room for improvement. Only 50% of Hungarian organisations said they have conducted general fraud or economic crime risk assessment (is it any wonder that a similar percentage, 49%, believe they haven't been touched by fraud?)



Fig 15
Question: In the last 24 months, has your organization performed a risk assessment on any of the following areas? (%)



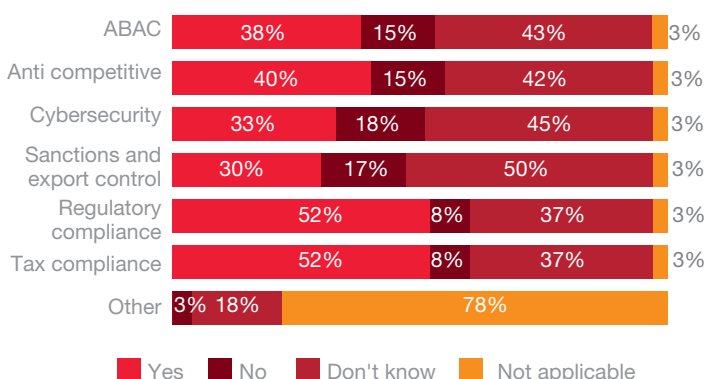
And when it comes to acquisitions and other transactions – with the risk of ‘buying’ successor liability and bad controls – a fraud risk assessment is even more critical, as part of pre-deal due diligence.

Csaba Polacsek

Such enhanced due diligence is as critical to the acquiring company as it is to the private equity sector, which not only needs to rely on a clean bill of health on the investment side but also would need to tout it when selling an asset. Enhanced fraud, cyber and anti-corruption due diligence will allow acquirers to know what risks they face and how they can either be carved out of a deal or remediated post-deal. Furthermore, the results of both can significantly increase the return on the sale side. Despite these benefits, less than half of the Hungarian respondents stated that their respective companies perform the following additional due diligence as part of their acquisition process: Anti-Bribery and Corruption 38%, Antitrust 40%, Cybersecurity 33%.

Fig 16

Question: Organizations which performed an AML/CFT (Anti Money Laundering/Combating Financing of Terrorism) risk assessment across its business and geographies in the last 24 months (%)



Fraud detection moves up to the first line of defence

Where fraud prevention and detection would have traditionally been the domain of the organisation’s second line of defence – risk management, legal, compliance, etc. – today’s enterprises are increasingly embedding their newly reinforced fraud prevention measures into the fabric of their first line of defence.

Csaba Polacsek

Our survey results support this: 17% of respondents indicated the CEO (who is part of the first line of defence) has primary responsibility for the organisation’s ethics and compliance programme, and therefore more instrumental in the detection of fraud and response to it.

This is likely just the beginning of a significant shift, where first-line fraud prevention and detection capabilities continue to mature and strengthen. As they do, they will enable the second line of defence to shift to a more traditional second-line approach – governance and oversight, and setting risk tolerance, frameworks and policies.

3.2 Systemic mechanisms plays important role in fraud detection

Moving from assessments to controls we see that increasing number of fraud incidents are detected via systemic mechanisms. The reliance on corporate controls in fraud detection has grown to 54% in Hungary (globally: 52%) from 42% (globally: 48%), however there is a notable difference in the role of corporate culture as it has much less impact on the detection of fraud in Hungary (15%) than globally (27%). Therefore, the chances of detecting the fraud within the influences of management is significantly lower and 21% of economic crime was still detected beyond the influence of management in Hungary.



Reliance on corporate controls in fraud detection

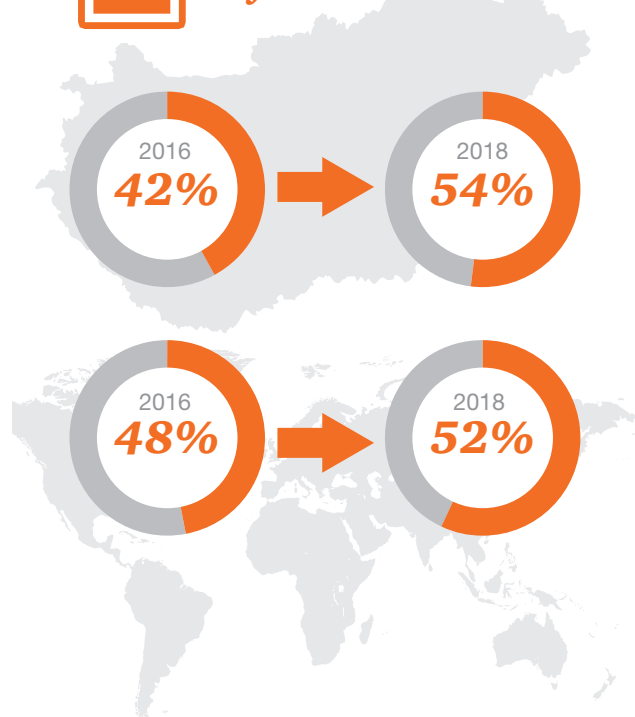
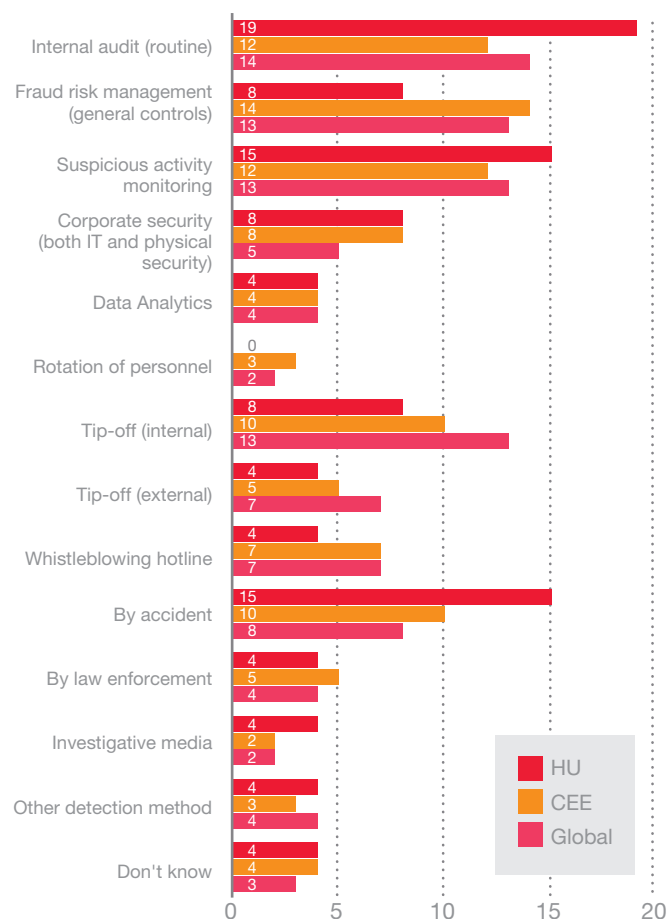


Fig 17

Question: How was the most disruptive fraud and/or economic crime initially detected? (%)



3.3 Compliance programmes and funds used to combat fraud and economic crime

Our survey revealed that approximately one in eight (12%) respondents in Hungary stated that they knew of no formal ethics and compliance programme in place in their companies – this is a minor decrease compared to 19% reported in the 2016 Survey. To ensure that the company's compliance and business ethics program is effective, 81% of companies pursue internal audits, 67% pursue management reporting and 31% also carry out an external audit.

Also, 56% of the respondents in Hungary stated that their company uses a whistleblower hotline to ensure that its compliance system works effectively – this represents a 12% increase compared to the 44% reported in the 2016 Survey. While internal audit is an important piece of the framework for assessing a compliance programme's effectiveness, it is not by itself a sufficient means of assuring compliance, due to the fact that its interventions are both periodic and historical. Moreover, the fraud risk profile has changed (e.g. an increase in new fraud and cybercrime), and incidence of some fraud types is rising or persistent in certain types of organisations.

Interestingly, only 38% of Hungarian respondents indicated that they have seen an increase in funds used to combat fraud and/or economic crime, while 62% stated that their spending remained unchanged (or even decreased). At the same time, we have seen a significant jump in the occurrence of economic crime – a 100% increase compared to our last survey.

Fig 18

Question: How does your organization ensure that your compliance and business ethics program is effective? (%)

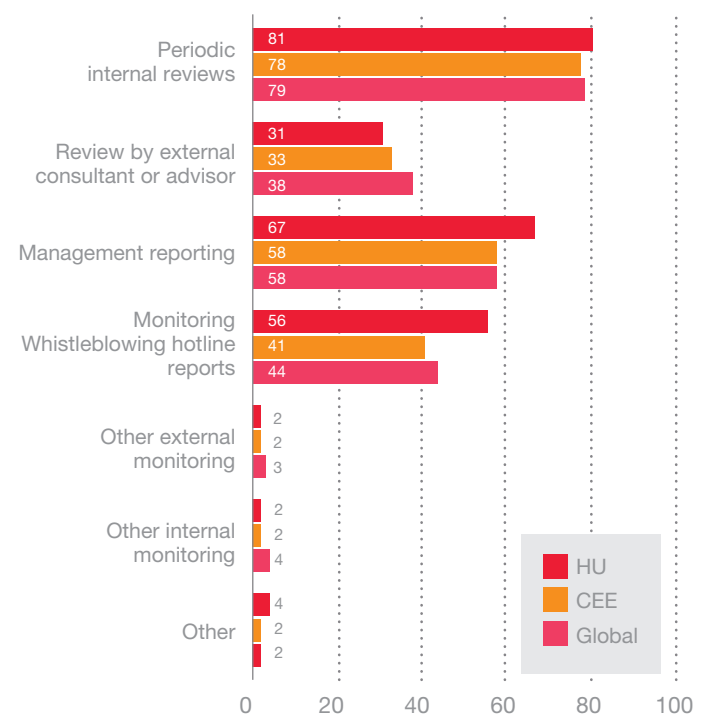
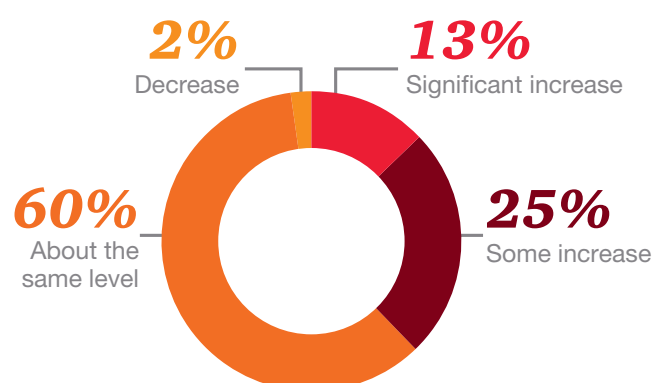


Fig 19

Question: How has your organization adjusted the amount of funds used to combat fraud and/or economic crime in the past 24 months? (%)



4. Harness today's technology to fight today's fraud

When it comes to fraud, it's common to remark that technology is a double-edged sword: both as business threat and business protector. These areas have traditionally been the domain of the operational level of the business – the second line of defence of an organisation. But technology has become so ubiquitous across every business process, including customer-facing areas, that how you leverage it to combat fraud – the balance you strike between safety and overzealousness – is now central to the customer experience. And that makes it a vital issue for senior management as well. Fundamentally, companies are realising that fraud, regardless of how it manifests, is first and foremost a business problem which could seriously hamper the growth agenda. In response, many have made a strategic shift in their approach to external fraud, and are making a business case for robust new investments in areas such as detection, authentication and reduction of customer friction.

On the fraud defence front, organisations today have available a wealth of innovative and sophisticated technologies aimed at monitoring, analysing, learning and predicting human behaviour. And the data shows they are using them, with varying degrees, depending on sector. Technology is expensive to buy and to adopt across a large organisation – prohibitively so, for some. And the decision of what to purchase, and when, is a delicate one. Some organisations invest in emerging or disruptive technologies that they don't use optimally. Others jump in too late, and find themselves behind the curve in the struggle to catch fraud or flag potential trouble spots. The responses of Hungarian participants also confirm this sentiment. While companies embrace the technology in combating fraud and/

or economic crime and have positive views on the capabilities it enables, 1 in 5 companies (19%) agree or strongly agree with the statement that its organization's use of technology produces too many alerts or false positives. We have good news for these companies: they probably don't need further costly investments into technology – just to recalibrate and fine tune their existing systems.

Fig 20
Question: To what extent do you use technology as an instrument to monitor fraud and/or economic crime in each of the following areas? (%)

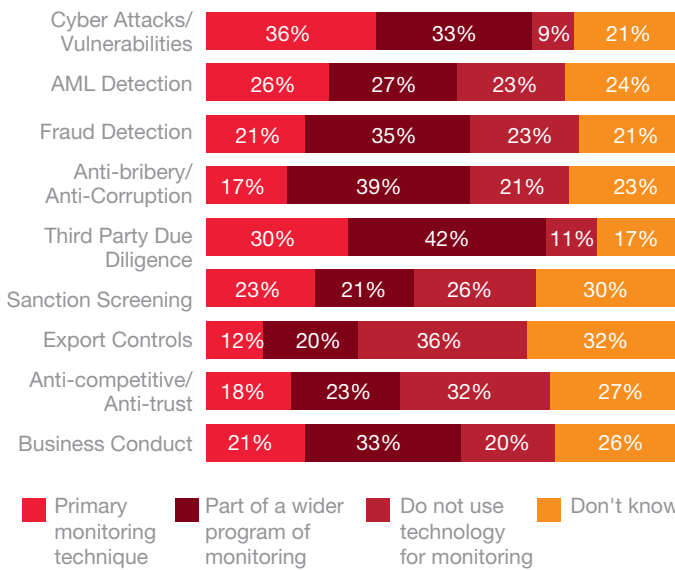
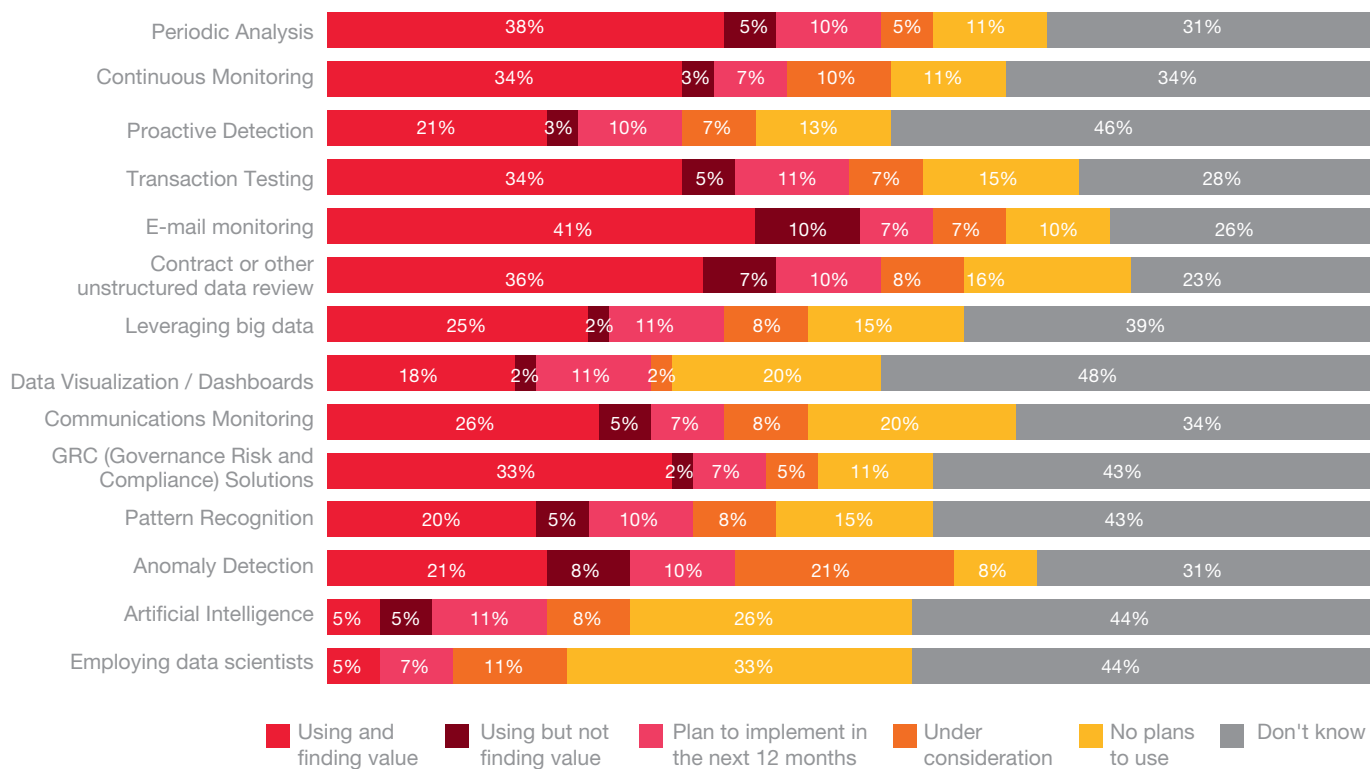


Fig 21

Question: To what degree is your organization using or considering the following alternative/disruptive technologies and techniques in your control environment to help combat fraud and/ or economic crime? (%)



Technology adoption trends: finding the sweet spot

Our survey surprisingly shows that companies in emerging markets are actually investing in advanced technologies such as artificial intelligence at a faster clip than developed nations – possibly as a way to catch up in an area where other nations have already sunk considerable infrastructure cost. Hungarian responses also confirm this sentiment: Several type of advanced technologies are used for various purposes.

Either way, it's clear that the use of innovative technologies to combat fraud is now a worldwide phenomenon. The ubiquity of technology and the stealthy growth of fraud are creating a double challenge for all organisations: finding the sweet spot between effectiveness and cost; and not getting outpaced by fraudsters that are also combining brain and machine power to go on the attack.

Customers aren't just one consideration of your business – they are your business

Your customers are the lifeblood of your business. As business models continue to evolve through the digital revolution, many are getting exposed to payment fraud for the first time. How you handle that fraud will profoundly affect your own outcomes.

Here are some of the characteristics and challenges of today's digital fraud:

- **New digital products are creating new attack platforms.** To bring products to market, companies once followed an established B2B process involving resellers, distributors and retailers. On today's innovative B2C digital platforms, there is a much wider front to attack – and much more room for fraud to break through.
- **Industry lines are blurring.** In the digital economy we are witnessing a crossing over of some non-financial services companies into payment systems. Whereas financial services traditionally have the most advanced antifraud measures and the legacy knowledge of fraud and money-laundering risk, some of these relative newcomers to the payment space lack this experience and know-how – making them, and their third-party ecosystem, susceptible to both fraud and regulatory risk.
- **The technical sophistication of external fraudsters continues to grow.** Digital fraud attacks continue to get more sophisticated, thorough and devastating. Consider how a single ransomware attack in 2017 crippled Britain's entire National Health Service (along with hundreds of thousands of computers the world over), putting lives at risk. Or how, in a 2016 hack, fraudsters managed to subvert several banks' SWIFT accounts – the international money transfer system that all banks use to move billions of dollars daily among themselves – stealing nearly US\$100 million from the Bangladesh Central Bank.
- **You can change your credit card number, but you can't change your date of birth.** The knowledge-based authentication tools long used to control fraud are outdated, but most companies haven't replaced them yet. When a national entity suffers a massive breach, what's stolen isn't a replaceable asset such as cash – but unique, deeply personal identity markers such as date of birth or social security number. Since this is the very data that's typically used to verify identity and prevent fraud, such a breach essentially opens the door for any fraudster to take over a person's identity. Unfortunately, many companies have not yet adopted the new techniques – such as digital device ID and voice biometrics – that are now necessary to protect their customers' assets.

Where would your customers money go?

While keeping customers happy is the first order of business, there are deeper dimensions to fraud prevention. These involve the fraud underworld, and the regulation and enforcement regimes whose mission it is to control it. Imagine the case of a customer whose identity gets stolen — a fraudster opens a credit card in her name and runs up a significant balance. The bank or the merchant will cover the loss, absolving the customer of further responsibility. Up until now, the system of remedying such external fraud has worked this way, and all parties – banks, merchants, consumers and regulators – have accepted it as part of the cost of doing business together.

But here's the problem: the fraud doesn't stop there. In some ways, that crime is only the starting point. Because while the customer may well have been made whole, that stolen money is now circulating in the deeper fraud system. And increasingly, the funds are going to finance nefarious activities such as terrorism, human trafficking and organised crime. While these fraudulent activities can be

detected by existing transaction monitoring systems that have been built in response to the AML/CFT laws and similar rules, it is likely that both banks and MSBs (money services businesses) are missing the manner in which these transactions manifest themselves in the system – as has been shown in recent regulatory enforcement around lack of detection by both types of businesses in the context of human trafficking. Non-financial companies may not have the same regulatory obligations as their FS counterparts, but they too could still find themselves running afoul of the law. That's because regulators and law enforcement are now looking beyond the primary impact of a crime – for example, trafficking in counterfeit goods – to examine what illicit activities the stolen assets went to finance. And, as part of their remit, they are scrutinising non-FS companies' compliance and antifraud measures for signs that they may be, consciously or not, 'aiding and abetting' such criminal activities – a further illustration of the increasingly blurred boundaries across sectors when it comes to fraud prevention.

The business case

The business case for investment in anti-fraud technology goes beyond protecting against reputational, regulatory or financial damage. It also includes reducing the cost of fraud prevention through efficiencies; enabling you to safely build and sell new products and services on a digital

platform; and fine-tuning your fraud programme to reduce 'customer friction' – allowing your good customers to interact more freely with your platform and your product, without excessive fraud prevention controls getting in the way.

Contacts



Csaba Polacsek

Partner
Advisory Services
+36 1 461 9751
csaba.polacsek@hu.pwc.com



Ferenc Pataki

Senior Consultant
Advisory Services
+36 30 958 3604
ferenc.pataki@hu.pwc.com



<http://www.pwc.com/hu/en/crimesurvey>

© 2018 PriceWaterhouseCoopers Magyarország Kft. All rights reserved.
In this document the expression „PwC” refers to PriceWaterhouseCoopers Magyarország Kft., and in certain cases to the PwC network. All member companies are independent legal entities. For more information, please visit the <http://www.pwc.com/structure> web page.
This publication is intended for general information only, and does not constitute professional advice.