www.pwc.com

Global Economic Crime and Fraud Survey 2018 Adriatic region

Are you aware? Fraud can happen to you

pwc

Contents

Foreword

The fraud you do not see is more important that the fraud you see

Welcome to our 2018 Global Economic Crime and Fraud Survey ("GECS") for the Adriatic region[1]. Globally, it is the largest survey of its kind, with 7,228 survey participants from 123 countries. This is the eighth time we have prepared the global survey, and the first time we have prepared a survey focused on the Adriatic region.

One hundred and forty eight respondents from the Adriatic region participated in the Survey and shared their experience and perception of economic crime in business. The majority of the respondents were publicly traded companies (38%), followed by privately owned companies (31%), state-owned companies (13%), and portfolio/private equity companies (13%). The respondents represented in the Survey come from various industry sectors, but predominantly from financial service sector. More than half of respondents are large multinational companies (62%) headquartered outside of the Adriatic region.

Therefore, the results of this Survey reflect the views of the representatives of the larger, mostly multinational companies. We understand that these respondents usually have much more developed compliance and anti-fraud programmes than medium-sized and small companies. However, they can also be comforted into a false sense of security thinking that "*fraud cannot happen to them*". Therefore, we would encourage all to read the report and consider improving or setting up their compliance and anti-fraud programmes tailored according to their particular needs and capacities.

We would like to thank those individuals and respondents that took the time to respond to our Survey. Without your support, this report for Adriatic region would not be possible. We invite all business leaders to use the results of this Survey and we would encourage an exchange of best practices between respondents. We trust you will find it a useful tool for yourself and your respective respondents to assist in your battle with fraud risks and to help improve our markets overall.

[1] Adriatic region: Albania, Bosnia and Herzegovina, Croatia, Montenegro, FYR Macedonia, Kosovo*, Serbia and Slovenia

At a glance

Economic crime is a persistent threat, but awareness is not keeping pace

- Economic crime is a serious with no industry being immune. Our Survey indicates that approximately one in three respondents in the Adriatic region experienced one or more instances of economic crime in the last two years. Although the reported rate of economic crime is lower than the global (49%), it may be that fraud incidents were not always detected.

- Fraud committed by the consumer was reported as the most pervasive type of economic crime/fraud. This has been reported also as the most serious in terms of its impact (monetary or otherwise) – 41% of respondents in the Adriatic region that experienced fraud, cited fraud committed by the consumer to have had the most serious impact, 35% in wider South East Europe[2] ("SEE") and 15% globally.

- Every third respondent in the Adriatic region (28% globally) has experienced economic crime/fraud committed by their business partners. It seems, therefore, that there is room for respondents to step up their efforts in the area of background checks of external parties. As a key prevention measure, knowing your business partners prior to engaging with them is less costly than dealing with potentially later unpleasant consequences.

- Bribery and corruption is perceived to be a serious issue and a hot topic to discuss in the Adriatic region. However, based on the results of this Survey this type of crime is only in 5th place (14%) of the most experienced economic crimes in the last two years. This is a lower percentage compared to the global results where 25% respondents experienced bribery and corruption in the same period. This could be a reflection of various factors, such as possibly lower fraud detection or the respondents' number and structure, mainly financial services sector. However, the reality is that almost all organisations are likely victims of bribery and corruption and reported numbers are likely more useful as a metric of organisational awareness than of actual fraud.

- Over 60% of the participants in the Adriatic region responded that the most disruptive economic crime in their organisation over the last two years had low or no impact on reputation, share price, employee morale, business relations and relations with regulators. These percentages are not in line with the fact that we are living in era of increased transparency and information accessibility where news about business frauds or misconducts can rapidly splash across the headlines. The question is why is the perception different?

Cyberwarfare: threats and opportunities

- Forty seven percent of respondents in the Adriatic region have been targeted by cyber-attacks in the last two years, in line with global reported rates. Cyber-attacks most frequently caused disruption of business processes (37%) and also led to substantive losses to the respondents: 15% of the respondents that were attacked suffered asset misappropriation and 20% were digitally extorted.

- Sixty one percent of respondents reported having an operational cyber incident response plan in place. While developments are very promising, a question remains: Will your cyber security programme withstand the test of reality? Our study reveals that over the last two years, only 18% of respondents have performed an assessment of their cyber response plan. The reported rate is well below the global average (30%). It is crucial for companies to understand that cyber threats are not static.

- As technology is constantly changing, regular monitoring and examination of the cyber response plan implemented is key to maintaining its relevancy.

Risk assessment

- In terms of risk assessment, our Survey shows that in the Adriatic region there is room for improvement, since less than 50% of respondents conducted general fraud or economic crime risk, vulnerability to cyber-attacks, anti-bribery/anti-corruption risk, an AML risk, a cyber response plan, or sanctions and export controls risk assessment. In

[2] SEE countries: Albania, Bosnia and Hercegovina, Bulgaria, Croatia, Macedonia, Moldova, Montenegro, Romania, Serbia, Slovenia

addition, 1 in 6 respondents has not performed any risk assessment at all, and 1 in 6 respondents did not know if a risk assessment was performed in their organisation.

Compliance and ethics

- Eighty percent of respondents have formal compliance programmes. Furthermore, of respondents who indicated their organisation had a formal business ethics and compliance programme, 35% said the Chief Compliance Officer and 22%,the CEO had primary responsibility for it. 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.

Regulatory

- Fifty seven percent of respondents indicated they had not experienced a regulatory enforcement, inspection related to AML, or that they were not aware if such an inspection happened in the last two years. Considering that majority of respondents are from the financial services sector and are subject to both local and international AML regulations, this could potentially indicate need for stronger regulatory enforcement in the AML arena in the Adriatic region.

Technology

- The ubiquity of technology and the silent growth of fraud are creating a double challenge for all respondents: finding the sweet spot between effectiveness and cost and not being outpaced by fraudsters that are also combining brain and machine power to go on the attack.

- That said, in the Adriatic region use of technology is still limited. Technology is mainly used:
  - as a primary monitoring technique for cyber-attacks/vulnerabilities (35%) and as a part of a wider programme of monitoring for cyber-attacks/vulnerabilities (30%); and
  - as a primary monitoring technique for fraud detection (20%) and as part of a wider programme of monitoring of fraud (35%). For all areas such as AML, sanction screening, export controls, anti-competitive, anti-bribery and corruption - technology is less used.

Thinking ahead

- Our Survey results show that economic crime risks are not diminishing whilst risks and threats are ever changing. When asked how likely or unlikely it is that respondents will experience different economic crimes within the next two years, respondents believe their organisations are likely to experience the leading economic crimes the most – cybercrime (30%), fraud committed by the consumer (14%), bribery and corruption (11%), asset misappropriation (9%).

- In terms of funds allocated to fight fraud, only one in three respondents are considering some increase in their investigative and compliance spend in the next two years, significantly lower than the global rate (44%). This rather conservative approach to budgeting for anti-fraud efforts might translate to companies' slight disregard of the changing business environment and of the seriousness of the new emerging threats.

1. State of economic crime

Prevailing types of economic crime

Our 2018 GECS shows that various types of economic crime or fraud continue to be a persistent threat to the economic and social justice worldwide. Moreover, our Survey shows that globally reported fraud is up by more than a third, from 36% to **49%**.

A deeper dive into the global data shows that this reported increase may in fact be mostly attributable to three factors:

1. A greater global awareness of fraud — and therefore greater transparency in identifying it by the respondents;

2. A more robust response rate, especially from companies in Africa and Asia Pacific, where the prevalence of crimes such as bribery and asset misappropriation make fraud relatively easier to detect; and

3. Additional clarity this year around the definition of fraud and economic crime.

Compared to the global results the Adriatic region's rate is lower, which can be a reflection of various factors, such as possibly lower fraud detection or the respondents' number and structure. However, the reality is that almost all organisations are likely victims of economic crime and reported numbers are likely more useful as a metric of *organisational awareness* than of actual fraud.

In our experience, in many cases, crimes remain undetected, especially bribery, cybercrime and procurement fraud. It is extremely difficult for an organisation to uncover all instances of fraud, especially if the organisation does not have strong internal controls, does not make available anonymous methods of reporting economic crime/fraud and does not perform fraud risk assessments regularly. Companies are encouraged to pay more attention to the different fraud schemes they may be facing, re-think their controls and test them on a regular basis.

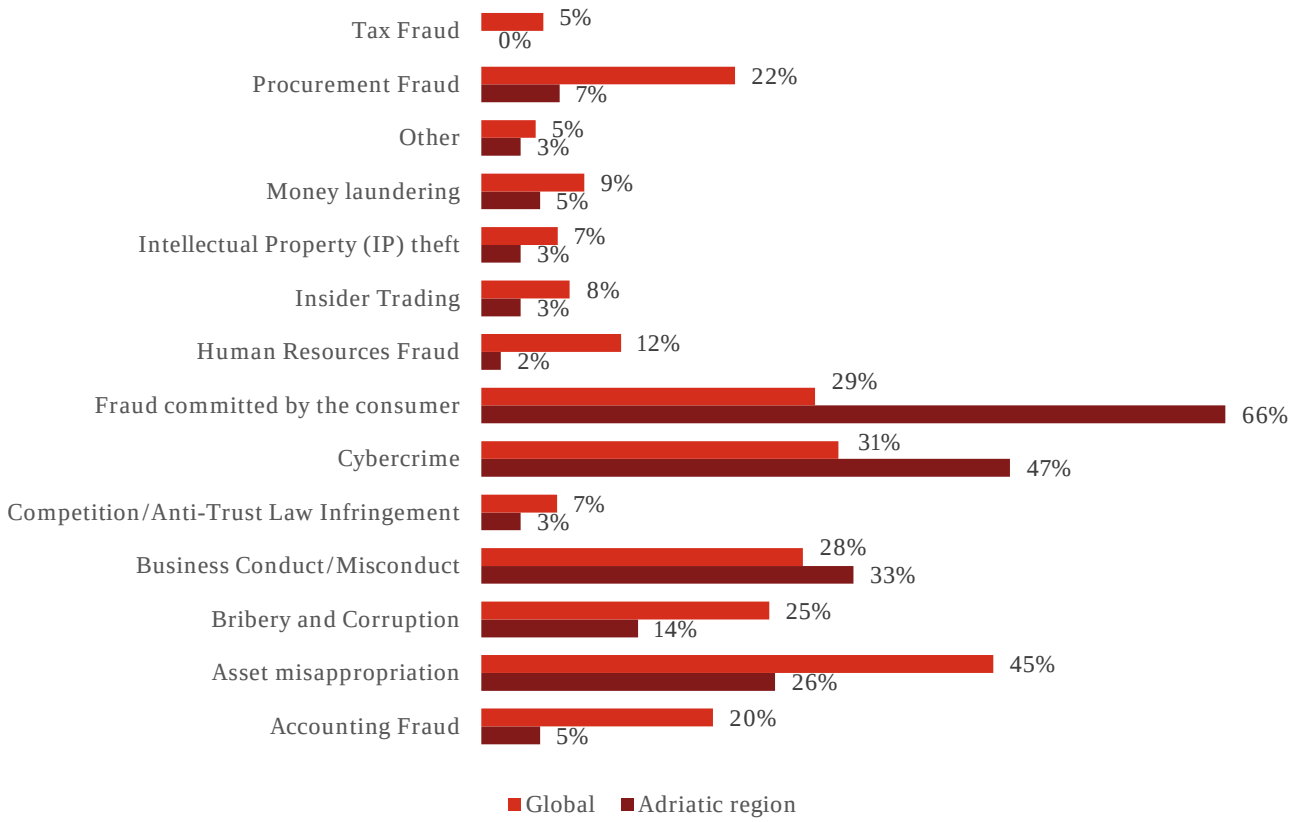
The prevailing types of economic crime are presented in the chart below.

Table 1 - ***Organisation experiencing economic crime in the Adriatic region***

	Yes	No	Don't know
Adriatic region	39%	56%	5%
SEE	39%	53%	8%
Global	49%	43%	7%

In the Adriatic region 39% of respondents reported that they were subject to economic crime in the last two years.

Figure 1 - ***Type of economic crime experienced in respondents in the last 24 months globally and in the Adriatic region***



More detailed information on selected types of economic crime/fraud from Figure 1 is presented below:

#1 Fraud committed by consumer

Consumer fraud was reported as the most pervasive type of economic crime/fraud, having been experienced by 66% of respondents in the Adriatic region that were affected by any fraud/crime. On a global scale, 29% of respondents have reported experiencing this type of fraud over the past two years.

Consumer fraud is fraud committed by the organisation's customers or others, through illegitimate use of, or deceptive practices associated with, its products or services. Examples include e.g. mortgage fraud, credit card fraud, claims fraud, cheque fraud and synthetic IDs.

Although occurrence of this type of economic crime/fraud has been reported by respondents from various industries, such a high occurrence of this type of fraud is likely primarily associated with a higher number of financial services sector respondents. Such respondents typically experience this type of economic crime/fraud on a larger scale.

This fraud has been reported also as the most disruptive/serious in terms of its impact (monetary or otherwise) – 41% of respondents in the Adriatic region that experienced any fraud, cited fraud committed by consumer to have had the most serious impact (35% SEE and 15% globally).

#2 Cybercrime

Cybercrime has long passed its infancy and adolescence. Today's cybercriminals are as perceptive and professional as the business 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.

That said, 47% of all respondents in the Adriatic region (31% globally) have been targeted by cyber-attacks. Respondents indicated that cybercrime occurred in various forms, out of which malware 37% (36% globally) and phishing 28% (33% globally) were dominant. On the other hand, 14% of respondents did not know the name of the technique used by cybercrime attackers and 11% did not know if an attack happened. There is a potential blind spot to be aware of, namely the level of knowledge about cybercrime. Is your knowledge of cybercrime sufficient?

Most of these attacks were reported to have severely disrupted business processes (37% Adriatic region and 30% globally), and led to substantive losses to companies: 15% of respondents who were attacked suffered asset misappropriation and 20% were digitally extorted.

#3 Businesses conduct/misconduct

Every third respondent (28% globally) have experienced this type of economic crime. It seems, therefore, that there is room for respondents to set-up their efforts in the area of background checks of external parties. As a key prevention measure, knowing your business partners prior to engaging with them is less costly than dealing with the unpleasant consequences.

#4 Asset misappropriation

Twenty six percent of respondents were victims of asset misappropriation in the Adriatic region, significantly, a lower percent compared to global results (45%). Asset misappropriation has traditionally been regarded as the easiest of frauds to detect but, if not tackled on time, besides the direct impact of loss of funds, it can also lead to a culture of low morale within respondents and cause bad reputations.

There are basic means that, if properly applied, could prevent theft of assets:

- Proper documentation of custodianship of assets;
- Segregation of duties; and
- Background checks on employees that have custody of assets and physical safeguards.

#5 Bribery and corruption

Bribery and corruption is perceived to be a serious issue and a hot topic to discuss in Adriatic region. However, based on the results of this Survey this type of crime is only in 5th place (14%) of the experienced economic crimes in the last two years. This is a lower percentage compared to the global results where 25% of respondents experienced bribery and corruption in the same period.

Table 2 - **Respondents that have been asked to pay bribe**

	Yes	No	Don't know
Adriatic region	11%	63%	27%
SEE	10%	59%	31%
Global	25%	50%	27%

In addition, 11% of the Adriatic region respondents indicated that their company had been asked to pay a bribe over the last two years (compared to 25% globally). Twenty four percent of the Adriatic region respondents in 2018 (26% in 2016) believe their company had lost out an opportunity to a competitor, which they believed paid a bribe in the same period (in line with global results).

We do however consider that this is only relative and mostly attributable to the following factors:

1. Lower detection of bribery and corruption, attributable to the inherently more hidden nature of this fraud,
2. Less than one third of respondents performed anti-bribery and anti-corruption risk assessment in the last two years.

Effects of economic crime

No discussion of economic crime would be complete without trying to quantify the impact of fraud. After all, the anti-fraud effort is just another function of the business, which should pay off to justify its existence.

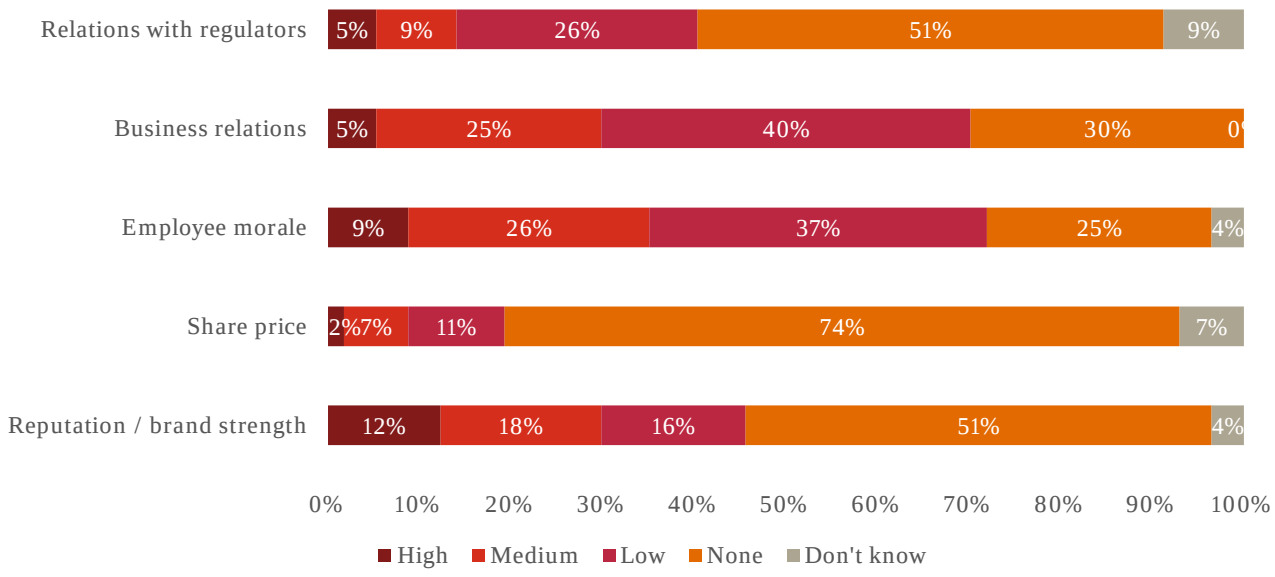
In financial terms, in the Adriatic region, for a majority of the respondents (31%) a loss due to economic crime over the last two years was less than USD 25,000. Besides the direct loss itself, another financial burden associated with economic fraud/crime is the costs associated with the investigations and/or other interventions relating to these fraud incidents. Forty percent of respondents in the Adriatic region have spent the same amount or more on investigations and/or other fraud related interventions than the amount of direct loss from the fraud incidents (53% globally). Therefore, when you account for all costs associated with economic fraud/crime – the direct financial impact/loss plus the secondary investigative costs – the total cost of fraud can be quite burdensome.

However, the true cost of economic crime should not be judged only in monetary terms. There are also other, intangible costs associated with fraud. Irreparable damage to reputation and negative impact on the employees' morale or existing business relations could be even worse than the severe financial losses. Consequences might go as far as bankruptcy.

Companies in the Adriatic region reported the impact on employee morale as the greatest non-financial impact of fraud 35% (48% globally).

On the other hand, over 60% of participants in the Adriatic region responded that the most disruptive economic crime in their organisation over the last two years had little or no impact on reputation, share price, employee morale, business relations and relations with regulators. These percentages are not in line with the fact that we are living in an era of increased transparency and information accessibility where news about business frauds or misconducts can rapidly splash across the headlines damaging reputation, brand, business relations and employee morale.

Figure 2 - ***Non-financial impact of the most disruptive economic crime over the last 24 months in the Adriatic region***



2. Combating economic crime

Fraud detection

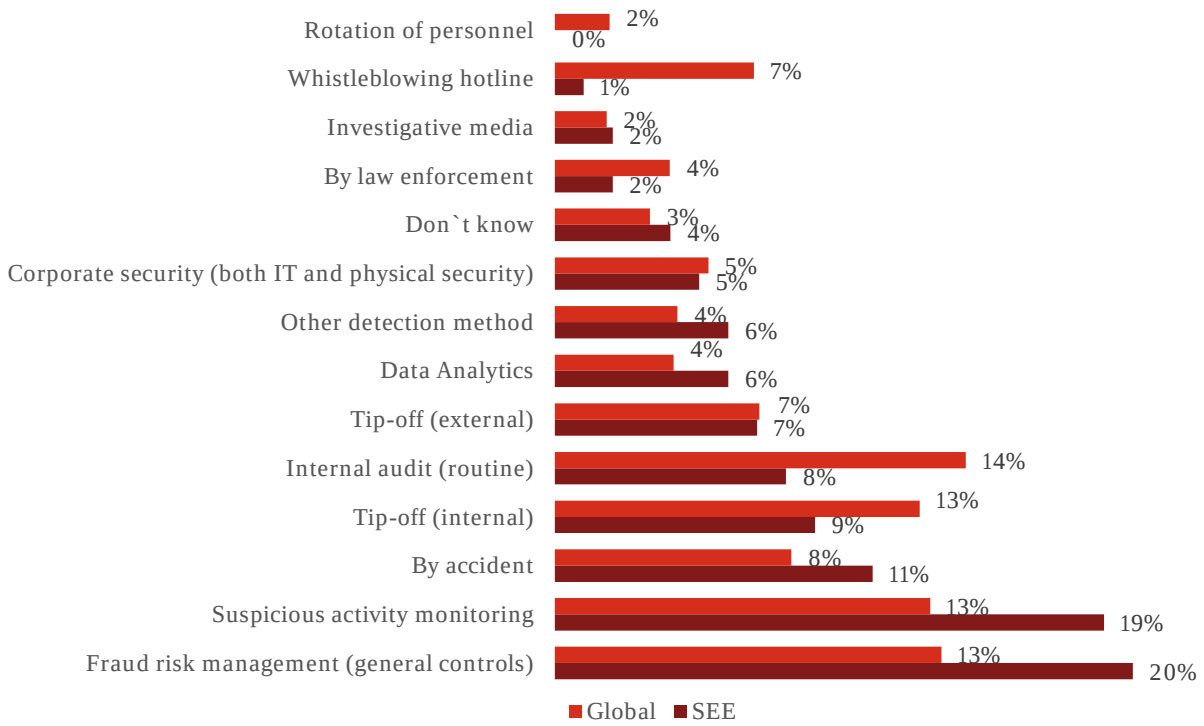
With respect to fraud detection measures, expectedly, corporate controls are still the largest contributor to detection, with 20% of SEE[3] respondents indicating that the most disruptive fraud was initially detected through corporate controls (13% globally). Proactive identification and detection of economic crime are the most powerful tools in the fight against fraud, and most of respondents seem to understand this and persist more systematically in their fraud combat efforts.

Meanwhile, 16% of SEE respondents indicated corporate culture (via internal and external tip-offs) was the form of initial detection. Whilst the whistleblowing hotline is an important part of the corporate culture and typically important detection tool, SEE companies reported that just 1% (7% globally) of cases had come to their attention through this function. Although throughout the Survey, it was evident that the SEE companies use whistleblowing hotlines to some extent, the low level of reported fraud cases from the hotline could likely be a result of:

1. whistle-blower reports containing inaccurate information (which is not completely uncommon);
2. whistle-blower reports containing information that companies themselves could not substantiate (as companies are not necessarily sufficiently trained to deal with investigations around whistle-blower allegations on their own and need help from specialized forensic investigators); and
3. employees being reluctant to use this function to a greater extent due to still undefined specific legislation that would ensure protection for whistle-blowers in the SEE.

On the other hand, 11% of frauds were detected by accident and 2% by law enforcement; therefore, without the active involvement by the company. Although one could interpret this result from a positive angle, saying that law enforcement might be more efficient, we still think that there is room for more directed fraud detection efforts on behalf of respondents.

Figure 3 - ***How was the incident of the most disruptive fraud and/or economic crime that your organization experienced initially detected? (SEE region)***



[3] The response rate for Adriatic region was below the threshold level in order to make viable conclusion. Therefore, results are presented for SEE.

Risk assessment

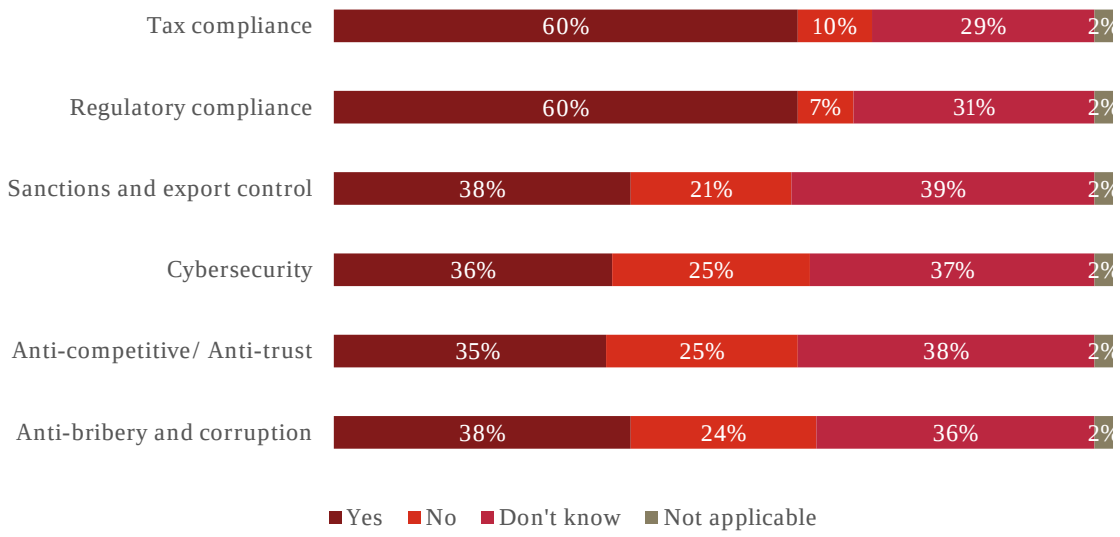
Our experience with businesses across the globe shows that a key pre-requisite for efficient crime prevention and detection is an awareness of the risks an organisation actually faces. In this respect, respondents should be encouraged to implement risk assessment exercises on a regular basis. Fraud risk assessments can help identify unique and specific fraud risks, which should be looked for and are increasingly favoured by regulations in enforcement actions.

However, our Survey shows that in the Adriatic region there is a room for improvement. Only 44% of respondents in the Adriatic region said they have conducted a general fraud or economic crime risk assessment and 38% had assessed vulnerability to cyber-attacks. Only 26% of respondents had conducted an anti-bribery/anti-corruption risk assessment. This is an especially worrisome statistic, considering how impactful and expensive this crime has become, on both the regulatory and financial side, around the world. In addition, less than 25% of respondents in the Adriatic region had performed a risk assessment in the areas of cyber response plan, AML, or sanctions and export controls. One in six respondents has not performed any type of risk assessment. The real number might be even higher, as an additional 17% of respondents did not know if such an assessment was performed in their organisation.

Most respondents that performed risk assessments have done so as part of their annual or routine process (77%), but also as part of their Enterprise Risk Management Plan ("ERM") strategy (47%) and audit plan (37%).

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 the pre-deal due diligence. 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. However, the results of our Survey indicate that anti bribery and corruption, cyber security, anti-trust and sanctions and export controls due diligences were performed in less than 40% of respondents in the Adriatic region.

Figure 4 - ***Does your organisation perform any of the following additional due diligence as part of your acquisition process? (Adriatic region)***



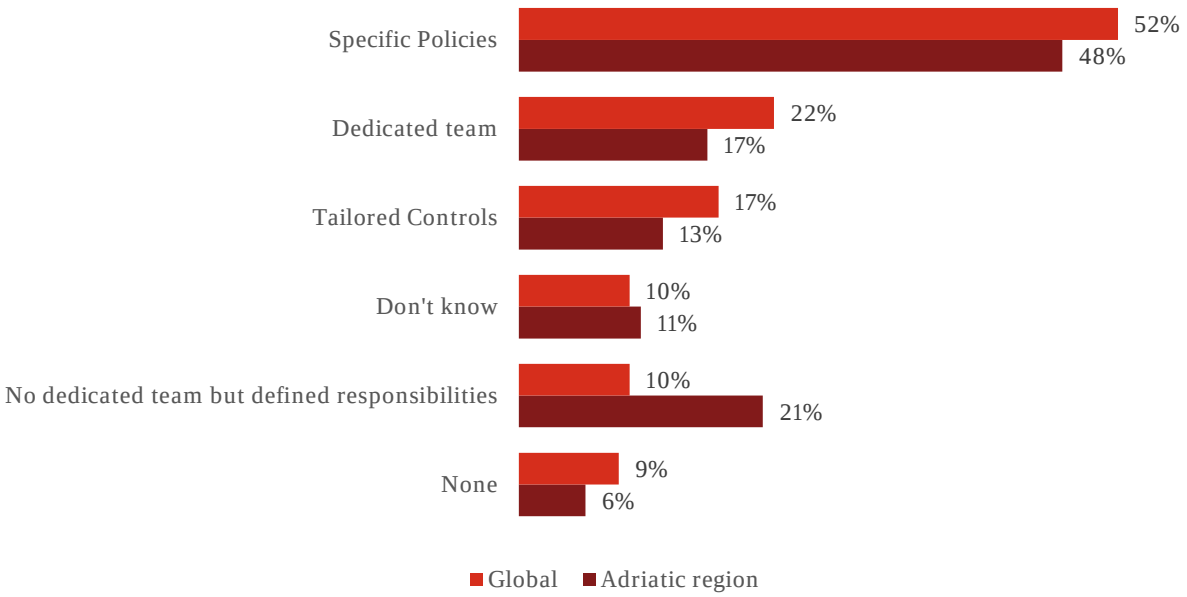
Compliance and Ethics

Companies also have another important role in the arena of combatting crime. Attitudes and practice, with regards to ethics and compliance is changing with many companies having put in place formal compliance programmes.

Eighty percent of respondents in the Adriatic region have a formal compliance programmes. Furthermore, of respondents in the Adriatic region who indicated their organisation had a formal business ethics and compliance programme, 35% said the Chief Compliance Officer and 22% that the CEO are primarily responsible for it. This puts a sharp spotlight on how the front office is managing this area — and the extent to which they are (or are not) adjusting their risk profiles accordingly. A deeper dive into the data on formal business ethics and compliance programmes indicates that less than half of the respondents in the Adriatic region with formal business ethics and compliance programmes have specific policies that deal with anti-bribery and corruption risks 48% (52% globally).

However, one must not mistake the difference between having a compliance programme formally in place and having a programme that is working efficiently. Businesses can assist in the fight against economic crime by acting proactively to prevent it. Based on the Survey findings that more than one in three respondents experienced economic crime over past two years, it may seem that efficiency of compliance programmes is not at the desired level.

Figure 5 - ***Ways of addressing risk categories in anti-bribery and corruption by formal business ethics and compliance programme globally and in the Adriatic region***



Regulatory

Fifty seven percent of respondents in the SEE[4] indicated they had not experienced a regulatory enforcement, inspection related to AML, or that they were not aware if such an inspection happened over the last two years. Considering that, a majority of all SEE respondents are from the financial sector and 67% are subject to both local and international AML regulations, this clearly indicates lack of regulatory enforcement in the AML arena in SEE. An even lower percent of respondents, 41%, expect that changes in regulatory environment will have an increased impact on their organisation. The remaining respondents, 38%, do not expect any impact of changes in regulatory environment on their organisation, 2% expect decrease in impact and 19% do not know.

[4] The response rate for Adriatic region was below the threshold level in order to make viable conclusion. Therefore, results are presented for SEE.

Cyber security

There is an imperative for respondents to develop mechanisms to minimise external threats. One of those mechanisms should be an implemented incident response plan to deal with cyberattacks. Sixty one percent of respondents in the Adriatic region stated that their organisation have an incident response plan (increase from 40% in 2016), which is to be expected as the majority of respondents are from the financial sector, which is the sector most sensitive to cyber-attacks.

Table 3 - **Does your organisation have a Cyber Security Program?**

	Yes fully operational	Yes not implemented yet	No currently assessing feasibility of implementation	No	Don't know
Adriatic region	61%	8%	8%	12%	11%
SEE	61%	9%	9%	9%	11%
Global	59%	12%	10%	9%	10%

While developments are very promising, with more and more companies seemingly prepared to understand and address the risks faced, one question remains: Will your cyber security programme withstand the test of reality?

Our study reveals that over the last two years, only 18% of respondents in the Adriatic region have performed an assessment of their cyber response plan. While reported rates are well below the global average (30%), it is crucial for companies to understand that cyber threats are not static. As technology is constantly changing, regular monitoring and examination of the cyber response plan implemented is key to maintaining it relevant.

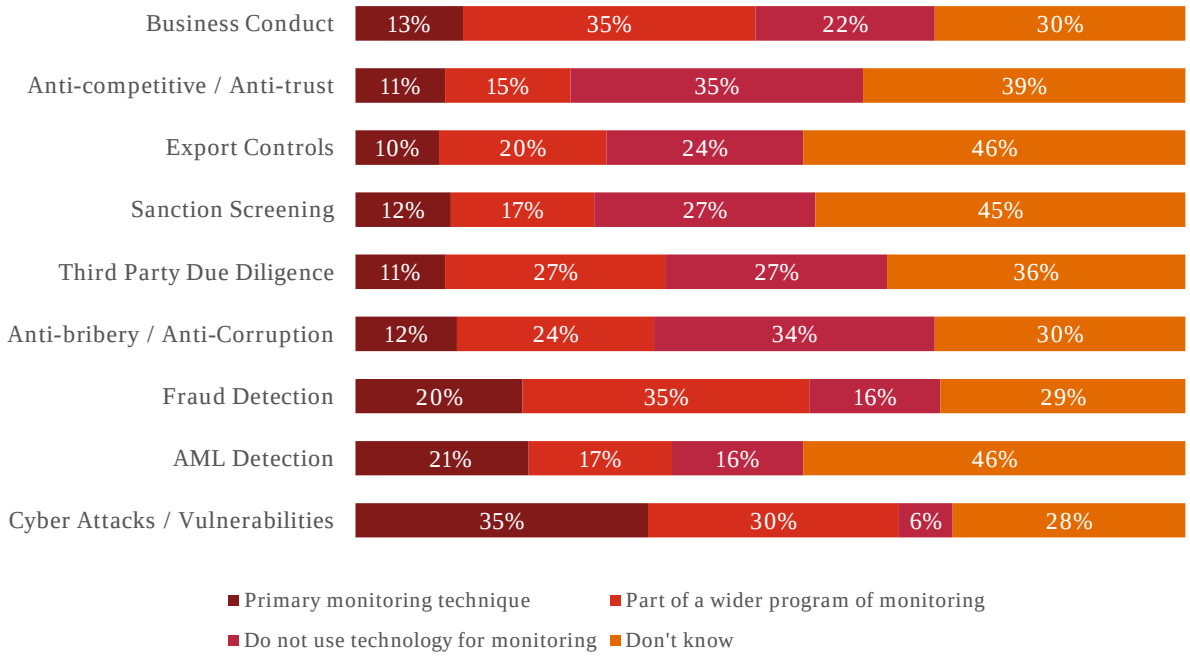
Cyber-attacks are here to stay, and all companies must enforce data protection policies, set up proactive defences and focus on being ahead of the curve in cyber security.

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

When it comes to fraud, it is common to remark that technology is a double-edged sword: both as a business threat and a business protector. These areas have traditionally been the domain of the operational level of the business — the second line of defence of an organisation. However, technology is expensive to buy and to adopt across a large organisation — prohibitively so, for some. The decision of what to purchase and when is a delicate one.

Sixty seven percent of respondents in the Adriatic region indicated that their budgets in relation to combatting economic crime in the last 24 months remained at the same level, and 61% expect this to be the case over the next two years. The ubiquity of technology and the silent growth of fraud are creating a double challenge for all respondents: finding the sweet spot between effectiveness and cost and not being outpaced by fraudsters that are also combining brain and machine power to go on the attack.

Figure 6 - ***To what extent do you use technology to monitor economic crime in each of the areas? (Adriatic region)***



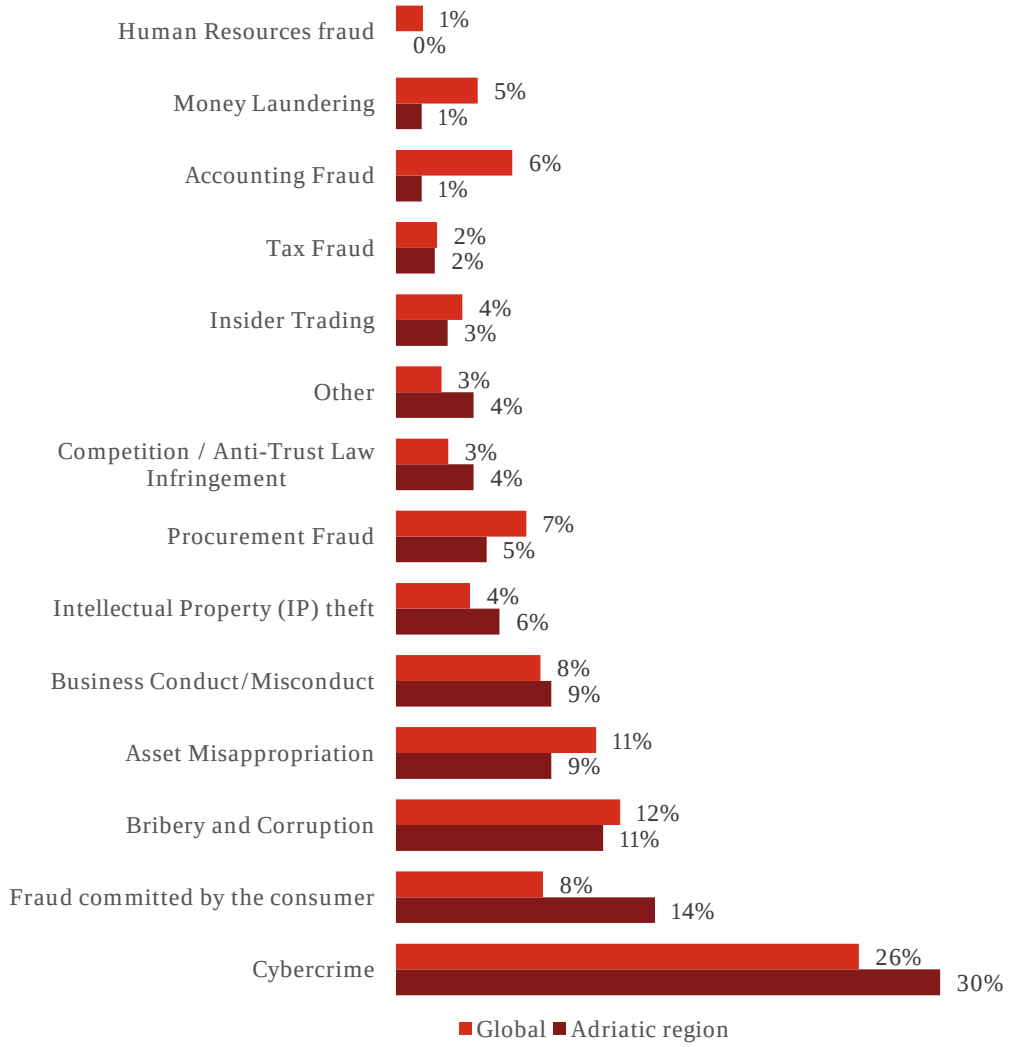
On average 64% of respondents in the Adriatic region, think that technology is important to use as a means of combating economic crime. The technology is clearly a fundamental tool in the fight against fraud, but it is not the only one. When it comes to fighting fraud (and in particular, internal fraud), technology investments invariably reach a point of diminishing returns.

That is because fraud is the product of a complex mix of conditions and motivations, only some of which may be contravened by machines or processes. The most critical factor — the "last step" to a bad decision — is the human choice. Ultimately, focusing on human behaviour offers the best opportunity for reducing or preventing it.

4. Thinking ahead

Our Survey results show that economic crime risks are not diminishing and that risks and threats are ever changing. When asked how likely or unlikely it is that their respondents will experience different economic crimes within the next two years, respondents responded that they believe their respondents are likely to experience the following types of economic crimes the most – cybercrime, fraud committed by the consumer, bribery and corruption.

Figure 7 - ***Type of economic crimes likely to be the MOST disruptive/serious in terms of the impact on your organisation in the next 24 months (monetary or otherwise) - Adriatic region***



In terms of funds allocated to fight fraud, only one in three Adriatic region respondents are considering some increase in their investigative and compliance spend in the next two years, significantly lower than global rate (44%). This rather conservative approach to budgeting for anti-fraud efforts might translate to the companies' slight disregard of the changing business environment and of the seriousness of new emerging threats.

Our 2018 Survey findings exhibit present and future fraud red flags and trends whose effects respondents must attempt to reduce. Fraud is damaging for a business and perpetrators adapt their methods on an ongoing basis. As one barrier is implemented, fraudsters will pursue and exploit other weaknesses within respondents. Facing such motivated adversaries, businesses must seek to adjust to an ever-evolving environment, prevent, above all, but also uncover and correct potential fraud occurrences.

Fraud is not going away, but a forward-thinking organisation can be one-step ahead and mitigate the challenges posed by economic crime.

5. Contacts

Want to know more about what you can do in the fight against fraud?

Contact one of the subject matter experts:

Sirshar Qureshi
Partner, CEE Forensics
☎ +420 602 348 926
sirshar.qureshi@pwc.com

Per A. Sundbye
Partner, SEE Forensics
☎ +386 51 687 079
per.sundbye@pwc.com

Filip Bojovic
Director, SEE Forensics
☎ +381 62 8830 928
filip.bojovic@pwc.com

Mojca Koder
Senior Manager, Forensics Slovenia
☎ +386 30 707 104
mojca.koder@pwc.com

Oliver Currie
Manager, Forensics Slovenia
☎ +386 30 606 654
oliver.currie@pwc.com

Jelena Savic Ramic
Manager, Forensics Serbia
☎ +381 64 8573 905
jelena.savic@pwc.com

Ivana Rapic
Manager, Forensics Croatia
☎ +385 91 1312 803
ivana.rapic@pwc.com

Arben Sulko
Manager, Forensics Albania
☎ +355 42 290 702
arben.sulko@pwc.com