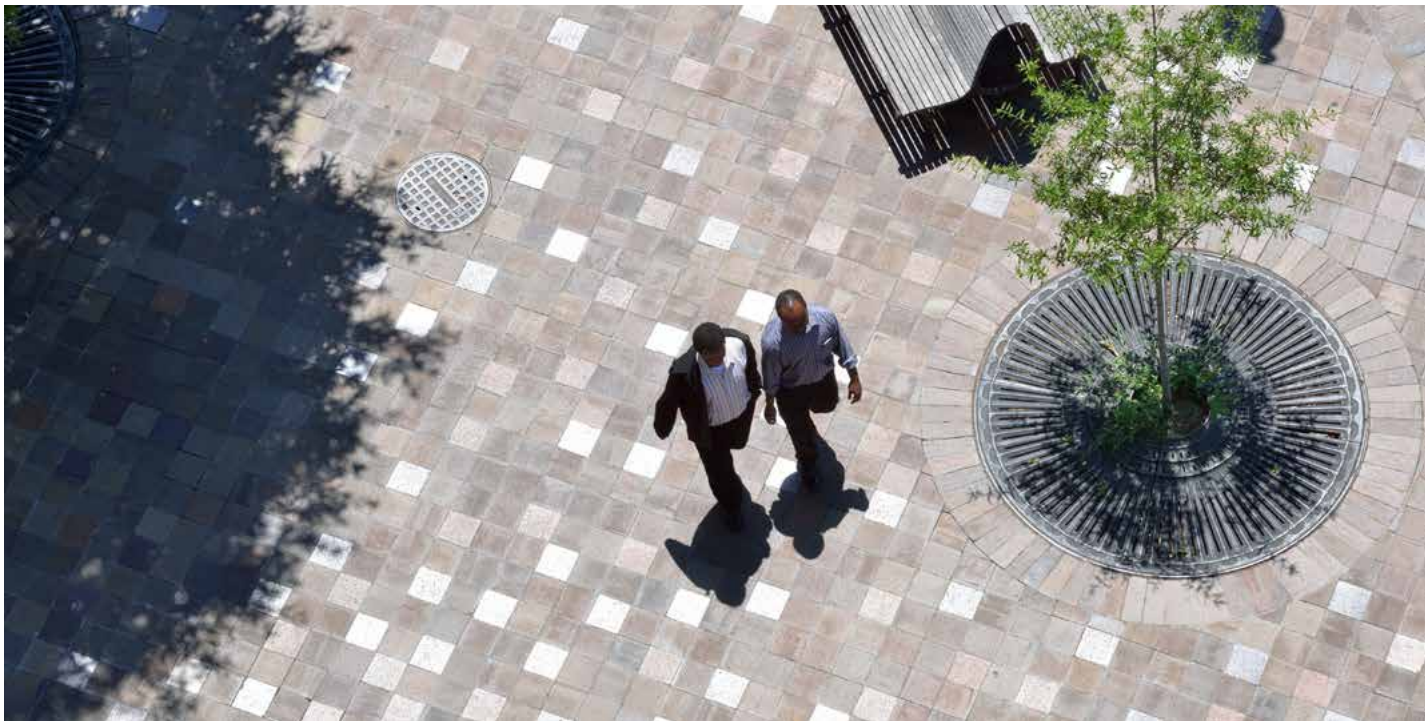
Economic Crime: A Swiss Perspective



37%
More than one in three organisations report being victimised by economic crime.

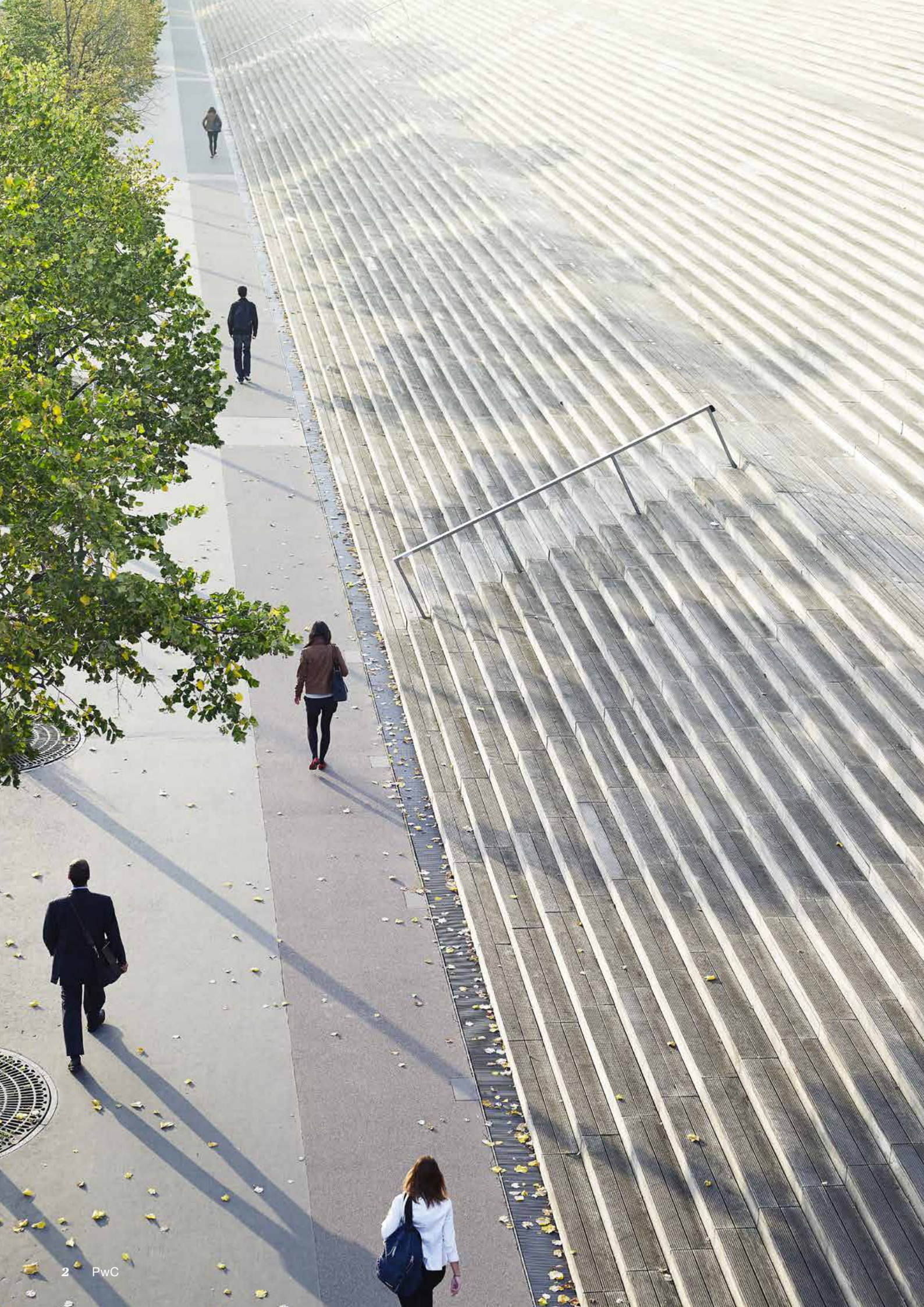
71%
of economic crime was detected through corporate controls and anti-fraud corporte culture mechanisms.

26%
After asset misappropriation, cybercrime is the second most reported type of economic crime.

pwc

Economic crime continues to be a major concern for Swiss organisations.

Contents



Foreword

Given the trend identified in our previous survey, it comes as no surprise that economic crime still persists, affecting one in three Swiss organisations. This year, the Global Economic Crime Survey looks at the major types of fraud in more detail, focusing on how these acts threaten business processes, whilst the Swiss-specific edition of the survey provides a local view of how economic crime has developed in the past 24 months. Some of our highlights include:

Incidents of fraud have not lessened – The percentage of respondents having experienced economic crime in the last 24 months increased from 18% to 37%.

Cybercrime is here to stay – 26% of Swiss respondents that were affected by economic crime, reported incidents of cyber-attacks at their company. Although awareness of cybercrime has improved, a significant percentage of respondents were not able to determine the extent of damage to their organisation caused by this type of crime.

Less reported bribery and corruption – Only 3% of Swiss respondents that have been affected by economic crime over the past 24 months reported incidents of bribery and corruption despite operating in high-risk countries. However, a significant number recognise it as a threat, with 37% ranking this type of economic crime as the greatest risk to their organisation when doing business globally.

The fraudster profile and actions taken – This year we have observed the return of the traditional fraudster who is male, between the age of 41 and 50 and has been with the company for several years. We also see that Swiss companies are more stringent in dealing with internal infractions; more of them are choosing to dismiss (2011: 60% versus 2014: 82%) or even take civil action against the fraudster (2011: 30% versus 2014: 59%).

Detection methods – This year's survey shows that, whilst the overall effectiveness of corporate controls has remained relatively unchanged during the survey period, there has been an increase of fraud detected thanks to corporate culture (from 24% in 2011 to 35% in the past 24 months). This suggests heightened awareness of the need to foster an anti-fraud corporate culture at Swiss companies.

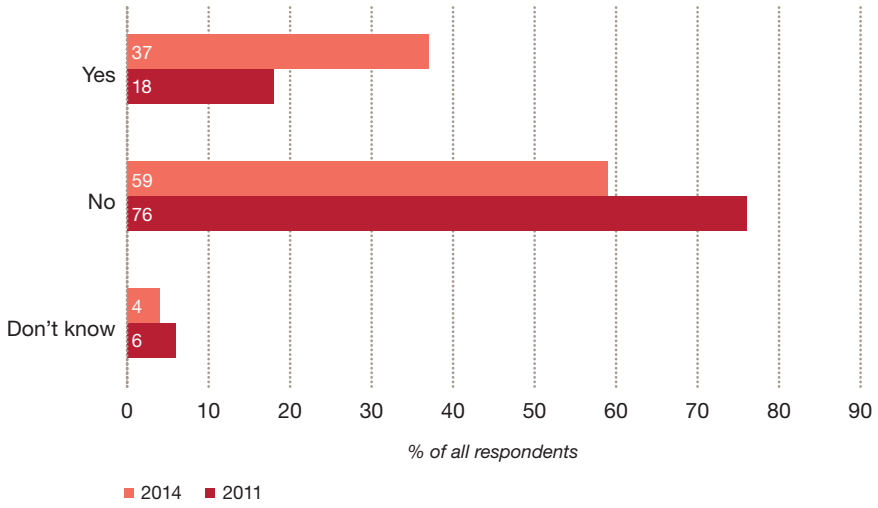
According to our respondents, asset misappropriation continues to be the most significant economic crime affecting Swiss organisations.

The current fraud environment

Economic crime and Switzerland

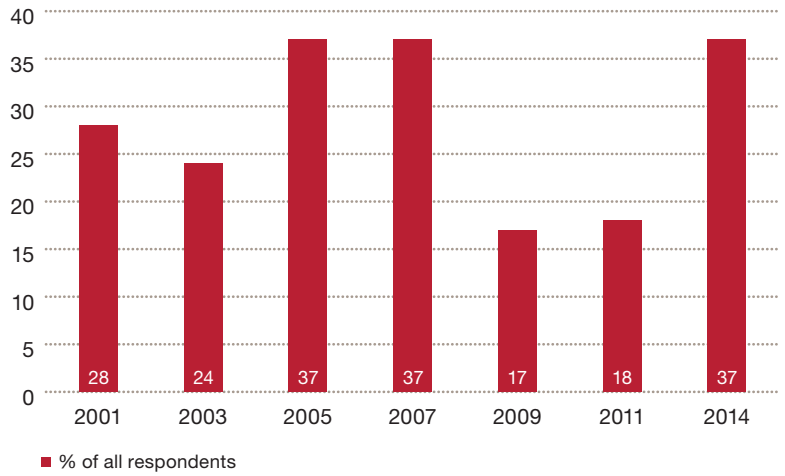
In our 2014 survey we see a significant increase in fraud where 37% of our respondents experienced incidents of economic crime in contrast to 18% in 2011 [Figure 1]. Some of this shift may be attributable to the shorter length of time surveyed in 2011 (12 months) in comparison to 2014 (24 months), which gave companies more time and, therefore, more opportunity to detect fraudulent incidents. If the perpetrator is skilful in covering his tracks, it may often take companies several months before the wrongdoing is unearthed.

Figure 1: Economic crime suffered in 2011 and 2014



When analysing our previous survey results in terms of the percentage of Swiss companies affected by economic crime, we noted that this year we returned to the trends evident in 2005 and 2007 [Figure 2]. Interestingly, during that period we were experiencing favourable economic conditions, so the number of reported fraud cases is what we expected to see from our surveys in 2009 and 2011 during an economic downturn.

Figure 2: Swiss companies reporting fraud 2001–2014



As mentioned at the time, during a period of recession the fraud rate tends to increase; however, we notice that this may not be the case in Switzerland as the opposite in fact occurred. The reason for this could be that, although there is more pressure and incentive to commit fraud in an economic downturn, there is also less opportunity to do so because of the decreased availability of assets in circulation and the tendency of companies to reduce their headcount. On one hand, the declining headcount may have affected internal functions that are traditionally responsible for fraud detection, such as internal audit, controlling or compliance, and therefore weakened their ability to effectively detect fraud incidents. On the other hand, however, this wave of layoffs may also have hit potential and actual fraudsters, thereby depriving them of the possibility to commit fraud.

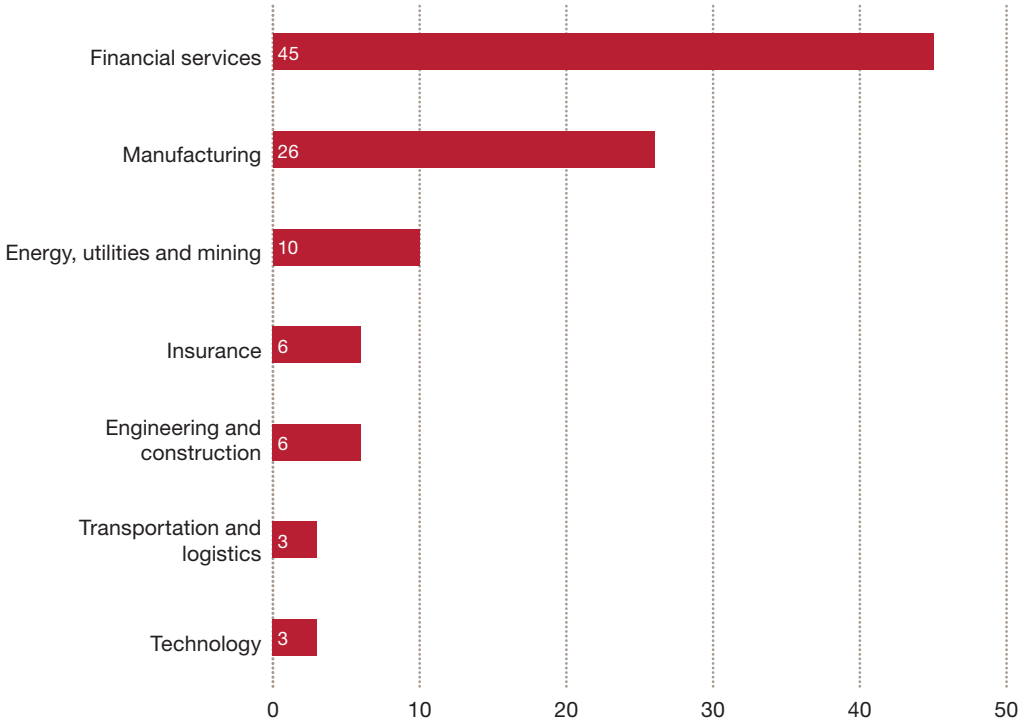
Furthermore, the 2014 results are more in line with the global trends, where 37% of respondents experienced economic crime in the past 24 months compared to 34% of respondents from Western Europe.

The corporate landscape

Over half of the Swiss survey respondents come from three industries: financial services, manufacturing, and engineering & construction. Given the importance of these industries in Switzerland, the participant mix is in line with our expectations.

Financial services are also the leading industry in terms of survey participation in Western Europe (17%) as well as globally (19%); however, in Switzerland they contributed to almost one-third of the results with 30%. We believe that such a strong financial services contribution is endemically Swiss and the results of the survey reflect our unique corporate landscape. This is especially evident when it comes to incidents of cybercrime and money laundering, which are discussed in more detail below. It is therefore not surprising that entities in the financial services industry have experienced the highest rate of economic crime over the past 24 months (45%) [Figure 3].

Figure 3: Top 5 Swiss industries affected by economic crime – 2014 Survey

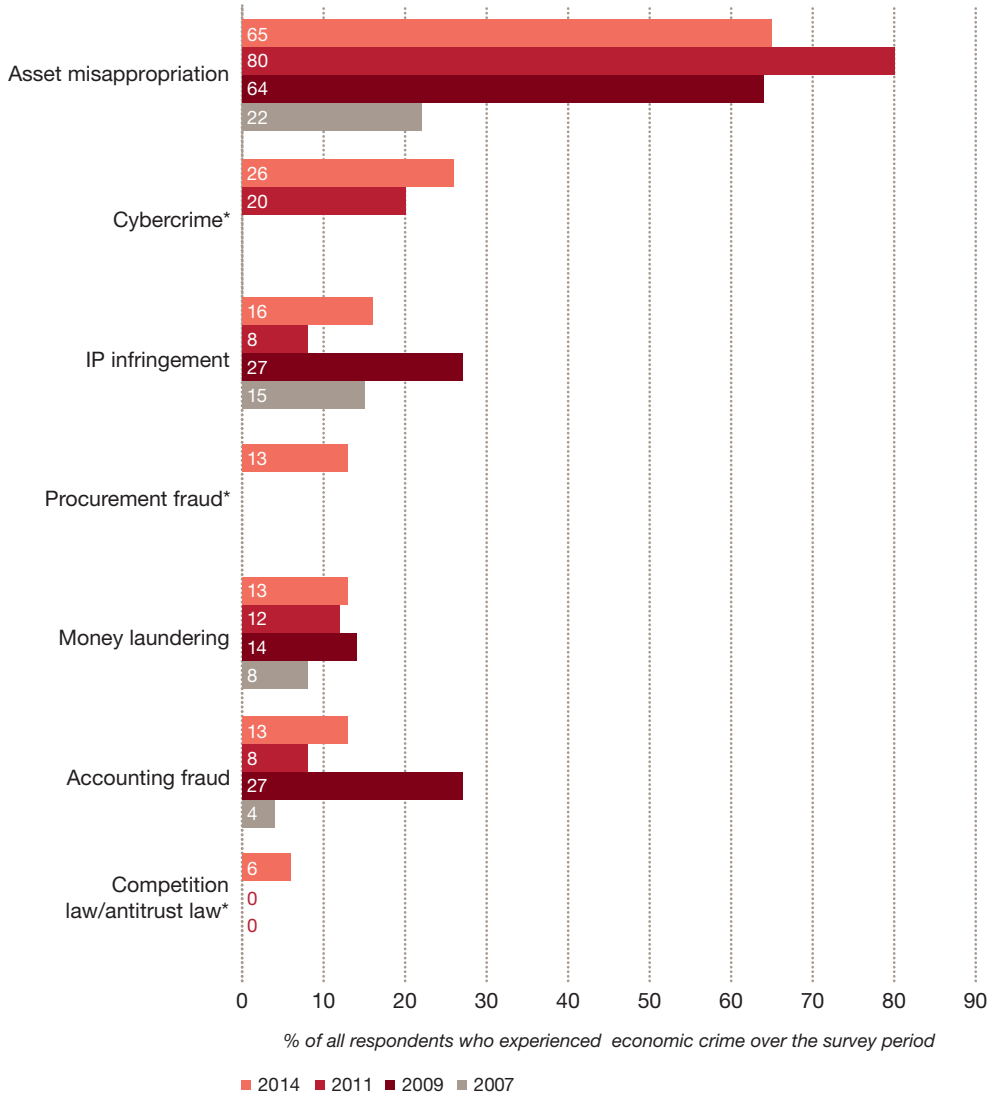


Types of economic crime

Asset misappropriation has traditionally ranked highest in the type of fraud reported by our respondents, with 65% being affected by this particular economic crime in 2014 [Figure 4]. This is a significant drop since 2011 when a whopping 80% were affected. Despite the decline, we believe asset misappropriation will continue to be the most prevalent type of economic crime impacting Swiss organisations as it is often easily committed and detected.

The second type of fraud affecting Swiss entities is cybercrime, which was reintroduced as a separate category in our last survey in 2011. We noted an increase from 20% to 26%, as expected. This type of fraud is predominant in the financial services industry, where 75% of the reported incidents of cybercrime relate to entities from that sector. We are of the opinion that cybercrime is here to stay, given the unrelenting reliance on technology – from coping with an ever-increasing amount of data to the introduction of new devices that help us in our everyday work life.

Figure 4: Top 5 types of economic crimes reported



* Cybercrime: reintroduced in 2011 as a separate category; Procurement: introduced as a separate category in 2014; Competition law/antitrust law introduced as a separate category in 2009

Intellectual property infringements also continue to be amongst the top economic crimes (ranking number three out of the 5 most frequent categories) and increased from only 8% in 2011 to 16% in 2014. As Switzerland is an economy that is characterised by high innovation and know-how, this emerging trend comes as no surprise.

Procurement fraud, which is a newly introduced category, ranks in the fourth place affecting 13% of respondents who experienced economic crime in the past 24 months. We believe that this time around a number of respondents might have more aptly reclassified some incidents of fraud to this category, given that it was previously equated to asset misappropriation. This may partly explain the decline in companies being affected by the latter type of fraud. Sharing places with procurement fraud are money laundering (2011: 12%) and accounting fraud (2011: 8%), with the former being a focus of further discussion later on in this report.

Procurement fraud and business processes

Despite having robust controls in place fraud can occur in all stages of the procurement process – starting with the bidding phase to the post-award and administration phase which can lead to use of low-quality products. Common procurement fraud schemes include:

- Invoicing frauds (false invoicing through dummy suppliers, personal purchases)
- Conflicts of interest (overbilling, pre-payments)
- Bribery and corruption (kickbacks and suppression of rebates)

Consider an employee who has significant power within the organisation working with a legitimate supplier in order to receive kickbacks through overbilling. The key element to this scheme is collusion – a secret agreement involving fraudulent activity. Collusion is extremely difficult to detect as it mainly happens outside of the transactional cycle and therefore creative accounting entries are generally not required. Typically, such a scheme is characterised by the fact that the employee and the vendor are closely acquainted.

So what can companies do to minimise the risk of procurement fraud? A combination of robust controls and well-designed data analytic tests may do the trick. Some examples include testing for:

- Unusual number of disbursements that fall just below a threshold that requires additional approval for payment
- Unusual payments to a particular supplier over a specified period of time
- Purchase orders which have been raised at the same time or after an invoice has been entered
- Payment date on or before invoice date
- Matches between contact person in the vendor master file to employee name within the employee master file (including identical or similar addresses, phone numbers, tax identification numbers or other relevant contact details)
- Corporate expense analysis

The human element is also essential when it comes to combating purchasing fraud. Those entrusted with combating fraud within the organisation should also regularly check the company's payment authorisation matrix to ensure that it is still relevant to the existing processes. Not only will this reveal any weaknesses in the segregation of duties within the company, but it will also help detect any individuals who may be overstepping their job description boundaries.

In addition, a company should have several suppliers wherever possible, and a list of pre-approved vendors who have been subject to a strict vetting exercise should be set up and regularly reviewed. Payments should only be made to these pre-approved vendors and for their pre-approved services. Any potential related party relationships between employees and suppliers should also be scrutinised before accepting a vendor for provision of services.

Procurement fraud – can you spot the red flags?

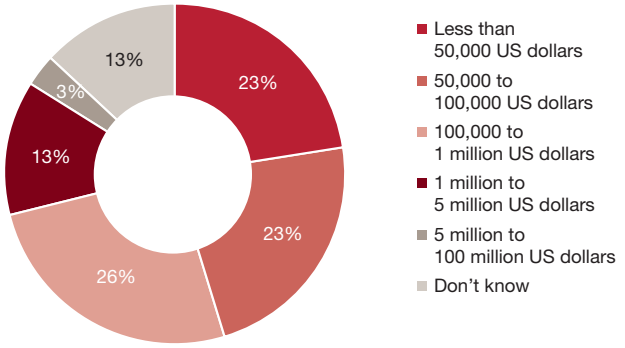
Indications that the organisation might be an easy target for a fraudster:

- Too much trust placed in key employees
- Weak internal controls
- Lack of purchasing guidelines
- Missing supplier documentation
- Use of agents/advisors/brokers to facilitate business, in particular in emerging markets

Indications that the organisation has already been affected by procurement fraud:

- Significant price changes as well as changes in orders and contracts after the award
- Suppliers' accounts with a high volume of debit and credit entries
- Large/unusual commission payments and advance payments
- Vendor complaints

Figure 5: The cost of economic crime – 2014 Survey



% of all respondents who experienced economic crime over the survey period

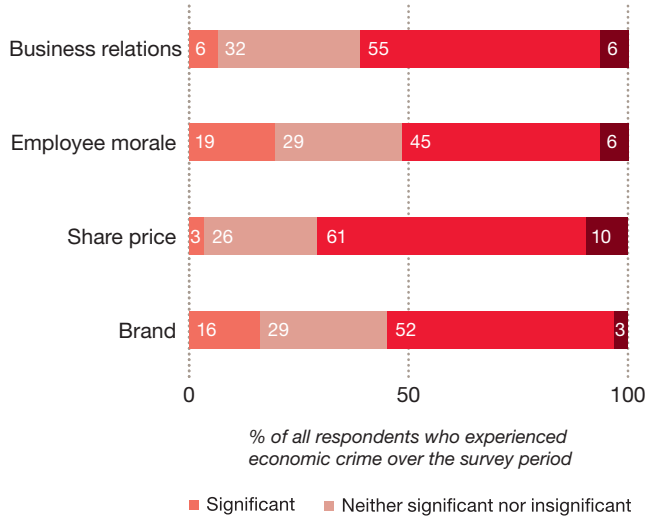
The damage is done

When asked about the aggregate financial impact of economic crime suffered in the past 24 months, 71% of Swiss companies indicated that they had incurred losses amounting to less than USD 1 million, compared to 77% of Western European companies and 73% of companies globally. Although the trend seems to be roughly in line with other regions, 13% of the respondents do not actually know what the financial impact of fraud is on their organisation, thus the overall effect may be underestimated [Figure 5].

Unfortunately, the occurrence of economic crime is not only limited to adverse monetary effects; it may also leave a wider swath of damage on our businesses. Despite not being all too worried about the collateral effects of reported instances of fraud, Swiss businesses do confess to being slightly more concerned than they were in 2011 [Figures 6 & 7]. The most significant impact of fraud on businesses other than the financial dimension is its effect on employee morale, with 19% of respondents experiencing this type of collateral damage as well as an adverse influence on the company's brand (16%).

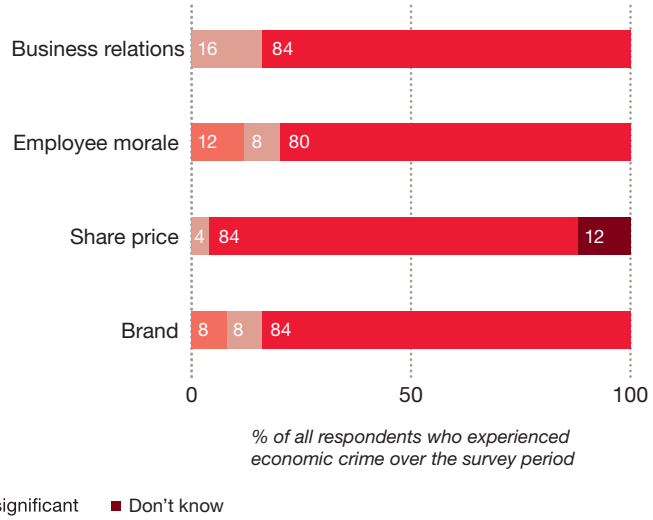
Furthermore, 6% of the organisations that experienced fraud also say that it had a detrimental impact on their business relations, whilst in 2011 there were no such cases. And only 3% of the respondents think that economic crime had a significant impact on their share price.

Figure 6: Non-financial impact of the economic crime – 2014 Survey



% of all respondents who experienced economic crime over the survey period

Figure 7: Non-financial impact of the economic crime – 2011 Survey



% of all respondents who experienced economic crime over the survey period

Significant | Neither significant nor insignificant | Insignificant | Don't know

12% of all respondents believe it is likely that their organisation will experience bribery and corruption in the next 24 months.

Under the eye of enforcement

Some economic crimes cause not only significant harm to the company; they are also of particular concern to society. They worsen the overall corporate climate and are a source of inefficiency and waste. We believe this is the case with incidents of bribery and corruption, money laundering and anti-competitive behaviour which for the purposes of this report are referred to as government enforcement-related crimes.

Over the years, these crimes have been and continue to be under increased scrutiny by regulators and other public authorities. They are subject to stringent regulation and enforcement as well as to harsh penalties including fines and remedial expenses. Organisations convicted of having engaged in government enforcement-related crimes also suffer adverse reputational damage due to negative publicity.

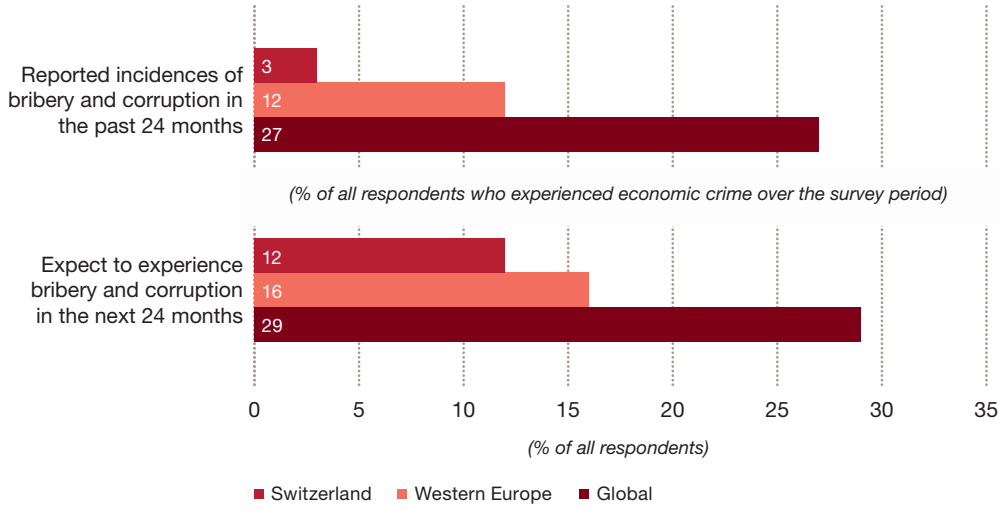
The impact of this type of crime has increased significantly in today's highly intertwined global economy. As organisations seek to gain new market shares and need to cope with intensified competition, they expand into high-risk territories where they are confronted with cultural differences and varying national customs. Therefore, they may be exposed to questionable business ethics and tempted to abide by them. In addition, organisations also have to consider the extraterritorial effects of their own national regulations in this regard.

Swiss companies and government enforcement-related crimes

When asked what type of economic crime their organisation has experienced in the previous 24 months, only 3% of Swiss respondents mentioned bribery and corruption. Even though that number appears to be in line with the perception of Switzerland as a country with low levels of bribery and corruption, we believe the incidence of this type of crime in Switzerland has been underreported and thus may not reflect reality. The risk perception of bribery is however higher, with 12% of all respondents believing it is likely that their organisation will experience this type of crime in the next 24 months. In contrast, at the global level a striking 27% of respondents affected by economic crime reported incidents of bribery and corruption over the same period of time and almost 29% expect to experience this crime in the future [Figure 8].

This significant difference is surprising in light of the fact that our survey shows that 76% of Swiss respondents already operate or expect to operate in territories where there is a high level of corruption risk, compared to 49% of respondents in Western Europe and 57% globally.

Figure 8: Incidences of bribery and corruption within the past 24 months and expectations for the next 24 months



Interestingly, our survey shows that even though almost three quarters of the Swiss financial services companies operate and/or plan to operate in territories with a high level of corruption risk, no respondent from that industry reported having been asked to pay a bribe or having lost an opportunity to a competitor who paid a questionable incentive over the past 24 months. Although bribery and corruption is widespread in different industrial sectors, this particular result comes as no surprise. However, as our findings suggest, an increasing number of Swiss financial services companies are involved or plan to get involved in business operations in high-risk markets. Going forward, this may leave them exposed to the risk of bribery and corruption, indicating that no industry is immune.

In terms of money laundering (13%) and anti-competitive practices (6%), our survey indicates that Swiss companies are currently more affected by these types of fraud than by bribery and corruption. Globally, the levels of money laundering and anti-competitive behaviour appear to be quite similar, with 11% of the fraud affected respondents having experienced money laundering and 5% reporting anti-competitive behaviour in the past 24 months. When asked about their future expectations in terms of money laundering, 14% of the Swiss respondents believe it is likely that their organisation will experience this type of crime and 11% believe the same for anti-competitive behaviour, which is in line with the trend observed globally.

The Swiss perception of government enforcement-related crimes – how risky are they?

We asked our respondents, which of the government enforcement-related crimes they perceived as posing the highest risk to their organisation in doing business on a worldwide scale. More than one-third of the Swiss respondents (37%) ranked bribery and corruption as the highest risk to their organisation, closely followed by money laundering (35%). This is considerably less compared to the global results, where more than half of the respondents (53%) consider bribery and corruption to be the highest risk [Figure 9].

This suggests that, even though Swiss respondents have been less affected by bribery and corruption in the past 24 months, they are becoming more aware of the risks that this economic crime may pose to their organisation and business activities, albeit far less so than their global counterparts.

Figure 9: The highest risk in doing business globally in terms of government enforcement-related crimes

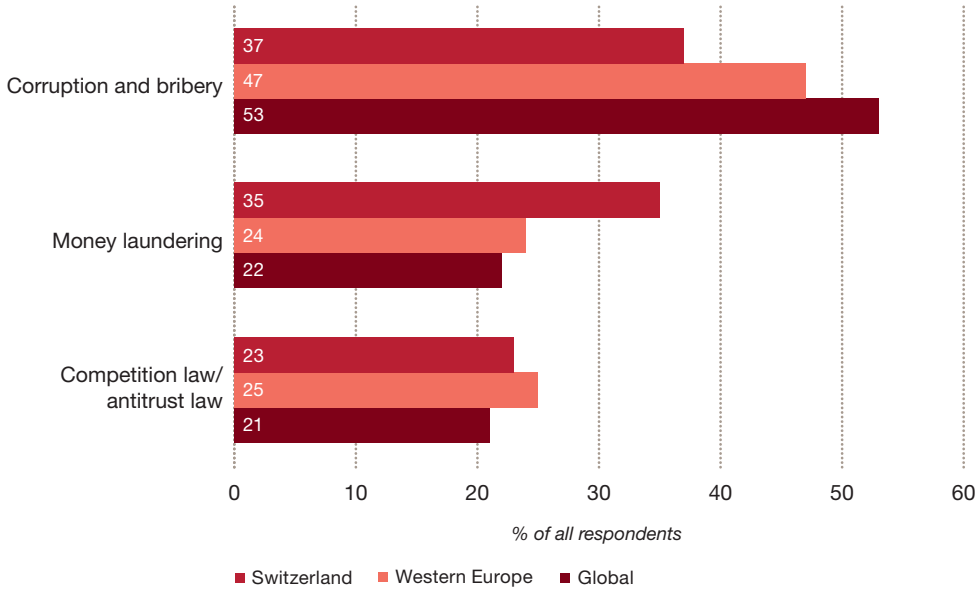
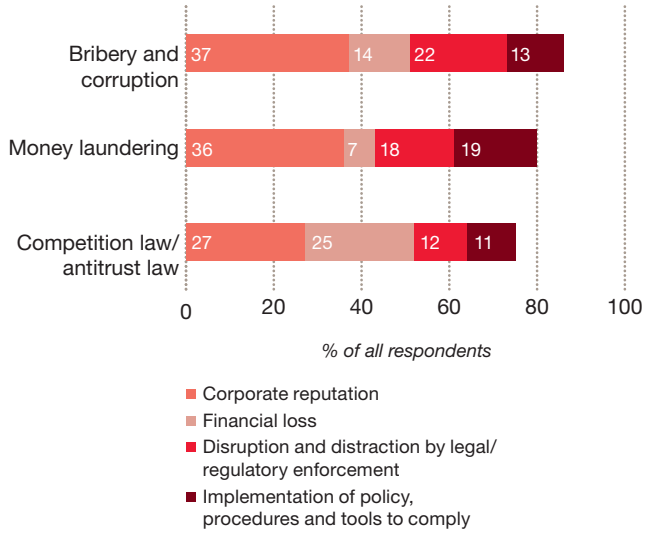


Figure 10: Perceived most severe impact of government enforcement-related crimes

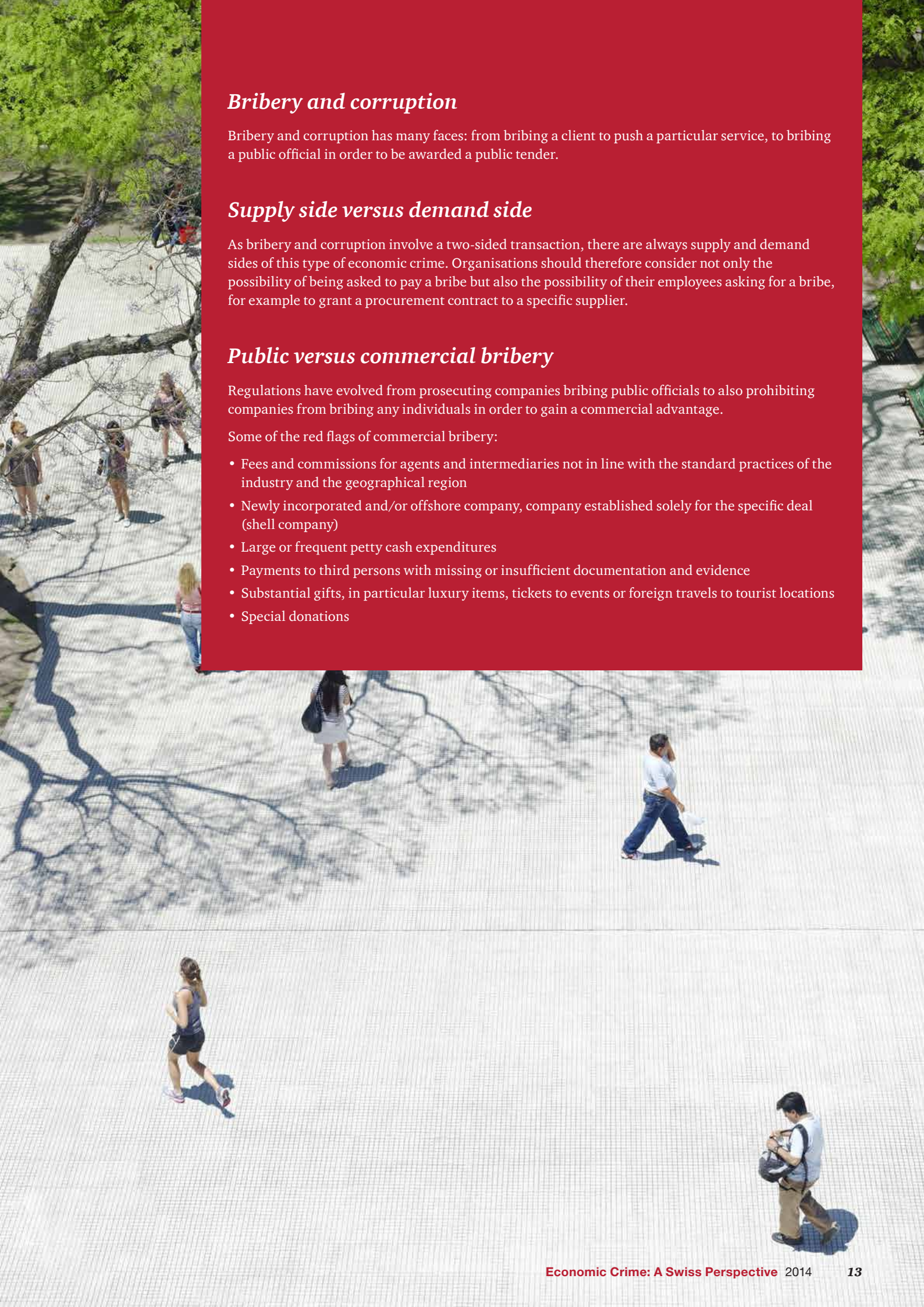


The associated costs

We also asked Swiss companies what they perceived to be the most severe impact of government enforcement-related crimes on their organisation. More than a third of the respondents indicated that money laundering as well as bribery and corruption have the greatest negative impact on corporate reputation. About one-fifth of the participants also mentioned the disruption and distraction caused by legal/regulatory actions in connection with government enforcement-related crimes [Figure 10].

With respect to anti-competitive behaviour, 27% of the respondents also mentioned corporate reputation. However, almost as many respondents (25%) said financial loss represented the most severe impact. This is not surprising, given the number of severe penalties imposed on organisations for anti-competitive behaviour. It is interesting to note that financial loss is also worsened by a decrease in profits when anti-competitive practices are ceased as a result of antitrust investigations.

This demonstrates that economic loss is not the only concern organisations have when combating fraud. Respondents clearly pointed at the damage to corporate reputation and additional regulatory burden on their business activities that result from government enforcement-related crimes. This trend appears to be very similar on a global level.



Bribery and corruption

Bribery and corruption has many faces: from bribing a client to push a particular service, to bribing a public official in order to be awarded a public tender.

Supply side versus demand side

As bribery and corruption involve a two-sided transaction, there are always supply and demand sides of this type of economic crime. Organisations should therefore consider not only the possibility of being asked to pay a bribe but also the possibility of their employees asking for a bribe, for example to grant a procurement contract to a specific supplier.

Public versus commercial bribery

Regulations have evolved from prosecuting companies bribing public officials to also prohibiting companies from bribing any individuals in order to gain a commercial advantage.

Some of the red flags of commercial bribery:

- Fees and commissions for agents and intermediaries not in line with the standard practices of the industry and the geographical region
- Newly incorporated and/or offshore company, company established solely for the specific deal (shell company)
- Large or frequent petty cash expenditures
- Payments to third persons with missing or insufficient documentation and evidence
- Substantial gifts, in particular luxury items, tickets to events or foreign travels to tourist locations
- Special donations

67% of our respondents stated that their perception of cybercrime risk increased during the last 24 months.

Cybercrime – here to stay

Cyber threat and Switzerland

It is generally accepted that today's ever-increasing dependency on technology has made the corporate landscape more complex and brought the threat of cybercrime progressively closer to our doorstep. Cybercrime was highlighted in our previous survey in 2011. As there are no borders in cyberspace, this allows fraudsters to use communication pathways created by the government and Internet service providers (ISPs) to exploit national infrastructure, our local businesses, and government entities. To date, there have been no disastrous cyber-attacks on Switzerland; however, our experience shows that cyber threats have reached our networks and thereby illustrate a basic truth: the precariousness of operating in a compromised digital environment.

Attacks on Swiss networks are not likely to peak in 2014 but instead will continue to evolve and increase in the years ahead – not because of any specific threat group or persistent vulnerability, but because of the unique Swiss corporate landscape mentioned earlier. Invading Swiss networks and stealing from Swiss financial institutions or corporations online is far less risky than committing the crime in person.

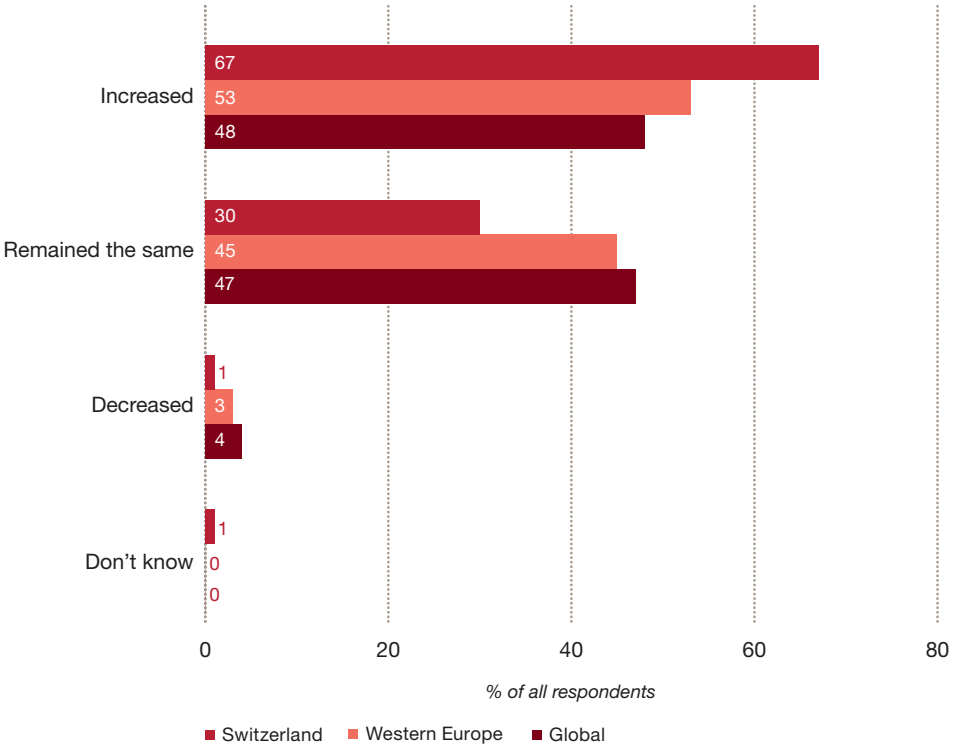
Although the risks in cyberspace can be managed, unfortunately they cannot be eliminated. Over the past 24 months, Swiss companies have started to understand that the goal is to mitigate rather than attempt to eliminate the damage and disruption that threats can do to the business. The Swiss findings of our current survey show an increase of awareness with regard to cyber risks. However, Switzerland still lags other major industrialised nations in addressing the risks cyber attacks pose to their companies.

Cybercrime – The costs we know of and those we don't

The 2011 report was the first in our series to highlight cybercrime as a high-level threat to organisations. This year's survey confirms the significant, continued impact of this crime on businesses, with one in four of all respondents that were affected by fraud, reporting they have experienced cybercrime as a type of economic crime in the past 24 months. On the other hand, the results also show that almost the same percentage of respondents (23%) are not actually aware of how much cybercrime has cost them during that time frame. In our estimation, this reflects the current state of awareness of cybercrime in Switzerland. As the degree of awareness increases in the coming years, the ability to quantify the financial impact will also increase.

In a sign that Swiss organisations are taking this threat more seriously, our survey indicates that the perception of cybercrime is increasing at a faster pace than that of reported actual occurrences. This year, 67% of our respondents said their perception of cybercrime risk increased in the survey period [Figure 11], in comparison to 52% in 2011.

Figure 11: Perception of cybercrime threats over the past 24 months



The risks of not knowing

While it is concerning enough that one-quarter of the respondents affected by economic crime reported cybercrime, we must also consider that a significant percentage of those who did not report cybercrime may have suffered such an event and not even known about it. And that is rather alarming. Further complicating the picture is that even when it is detected, cybercrime often goes unreported. Outside of breaches in regulated areas, such as identity theft, there are few regulatory conventions requiring disclosure. And often – such as in the case of theft of key intellectual property – there may be compelling competitive reasons for organisations to keep such losses confidential.

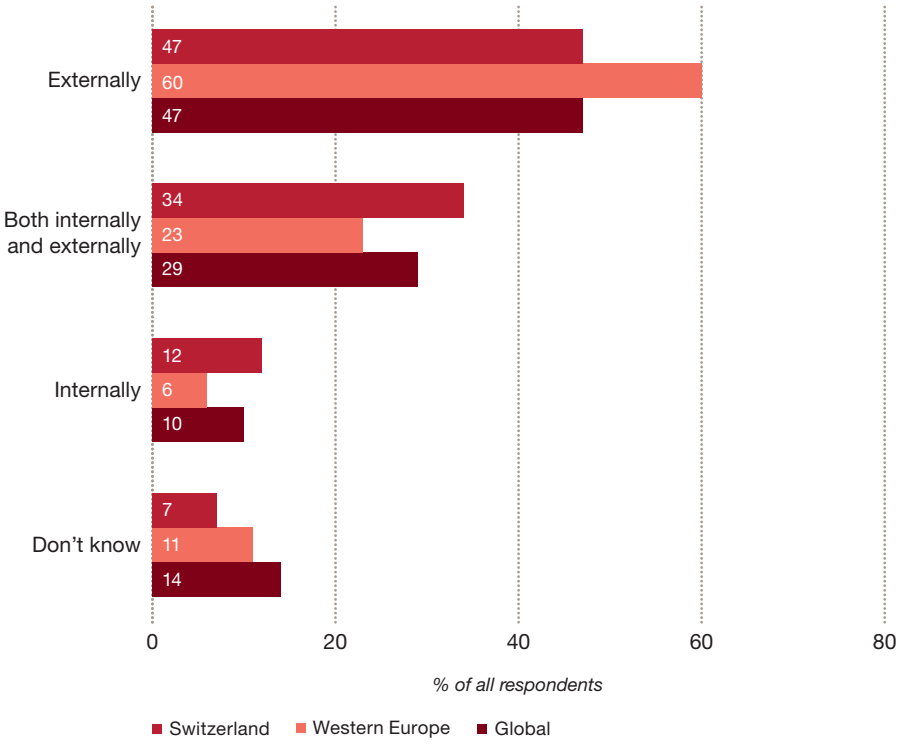
For example, if a confidential bid-planning document were accessed by cybercriminals and utilised by rivals to gain an advantage, would an organisation disclose the incident? Are organisations adequately defending themselves against such cybercrime breaches, and if they were discovered, how would they value the loss?

The bottom line is that much of the damage wrought by these types of attack is not disclosed, either because it is not known, difficult to quantify, or because it is not shared. Naturally, this kind of operational murkiness poses risks for a global business ecosystem that is increasingly reliant on both technology and intellectual property yet would benefit from such transparency.

Cyber threats from outside your network

When asked where the cyber threats will come from in the next 24 months, close to half of the Swiss respondents believe that they will come from outside their organisation, which reflects the trend globally. Compared to their global and Western European counterparts, Swiss respondents are also more sceptical with regard to cyber threats that come from within their organisation. However, this is to be expected, seeing as how the risk of data theft at Swiss financial institutions by internal perpetrators has been a hot topic in the past several years [Figure 12].

Figure 12: Source of cybercrime threat



Similar to the global findings, Switzerland has experienced an overall increase in concern that cyber threats will affect all areas of company, including reputational loss, financial loss, legal and investigation costs, regulation risks, intellectual property theft, and service disruption. In each of these categories, more than 60% of the respondents are either concerned or very concerned. The highest level of concern at Swiss companies pertains to reputational damage, closely followed by theft or loss of personal identifiable information (PII) [Figure 13].

Targeting the money

The financial services industry, with 43% of fraud-affected organisations noting cybercrime, is the clear leader in reported cybercrimes [Figure 14]. It is important to note that large, regulated financial institutions have higher levels of transparency and system safeguards, which may increase the chance of a breach being detected. Financial institutions also are an appealing target for cybercriminals because they provide large amounts of customer/financial information online that can potentially be accessed – and sold on illegal markets – by those with the right tools and skills.

Figure 13: Concerns about the effects of cybercrime on the organisation

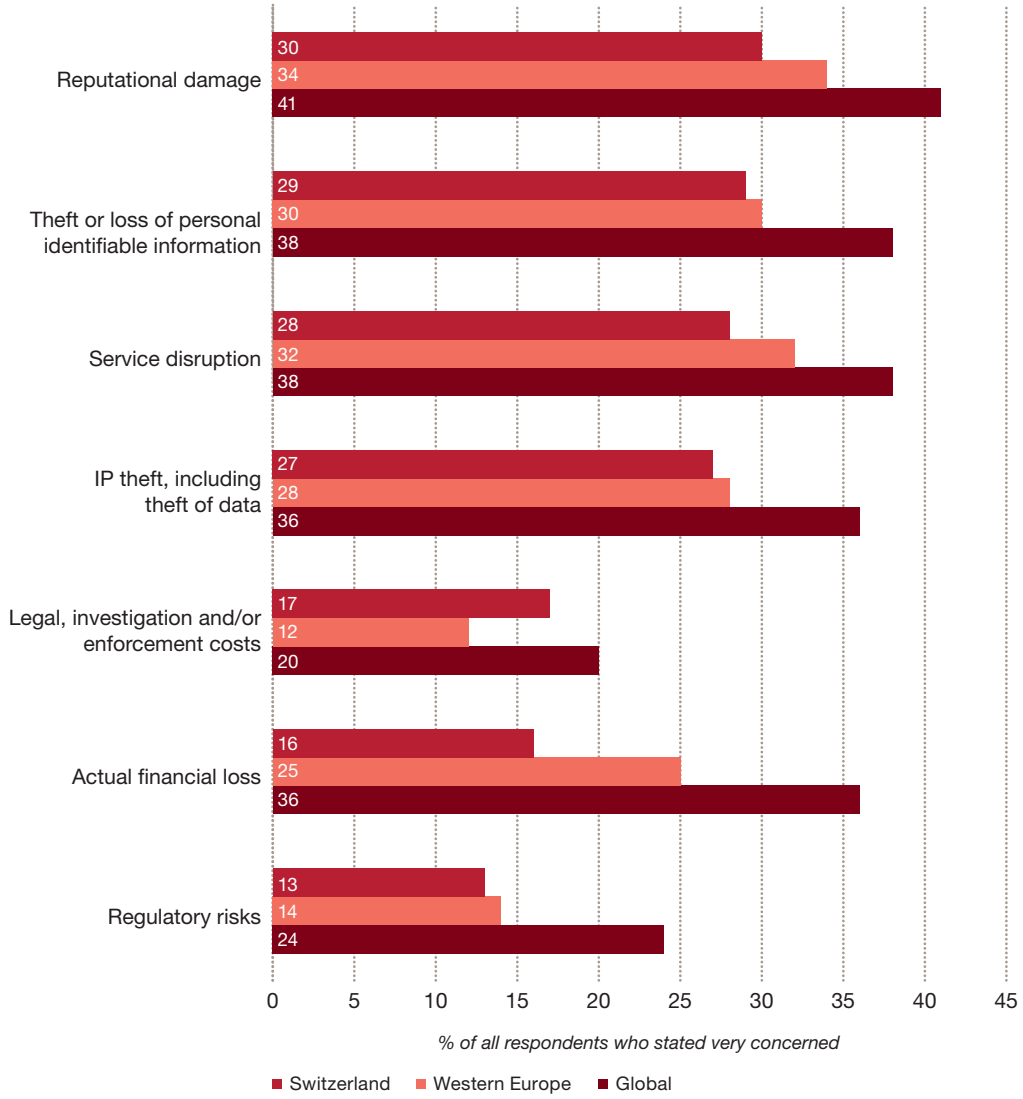
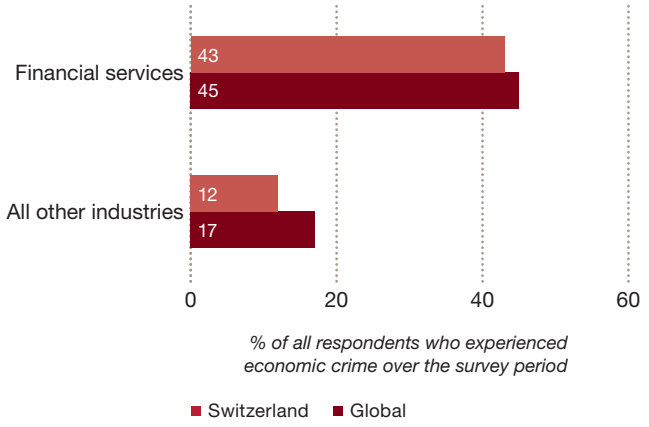


Figure 14: Cybercrime in the financial services industry and across the corporate landscape



The human element of technology problems

Even though organisations are generally aware of the types of cyber threats they face, many do not truly understand the capabilities of cyber criminals, what their targets might be and what the value of those targets are. While our 2014 Global CEO Survey reports that nearly half of the CEOs (47%) are concerned about cyber security threats (including lack of data security), cyber security is now trending lower on the scale of CEO concerns. Yet they continue to make their critical data available to management, employees, vendors, and clients on a multitude of platforms – including high-risk ones such as mobile and cloud – because the economic and competitive benefits appear to be so compelling.

While nobody expects those benefits to go away or for organisations to shrink their digital data footprint, with ever more data more accessible on an ever-growing number of platforms, it is clear that valuable data will remain under attack and that the cost of security breaches will continue to be steep. The truth is, in today's global digital domain the landscape is constantly changing and the sophisticated adversary takes advantage by attacking new vulnerabilities – which is why it is essential that organisations at least try to keep pace with the raiders who threaten them. Ultimately cybercrime is not truly a technology problem. It is a human problem – a strategy and process problem.

Cybercrime outlook for Switzerland

In every region surveyed, between a quarter and a third of the organisations told us they believe they will likely encounter cybercrime in the near future. It is interesting to contemplate whether these readings are grounded in a growing realisation on the part of organisations that they may be falling behind in detecting attacks, or whether they reflect a broader, well-founded sense of anxiety about cybercrime.

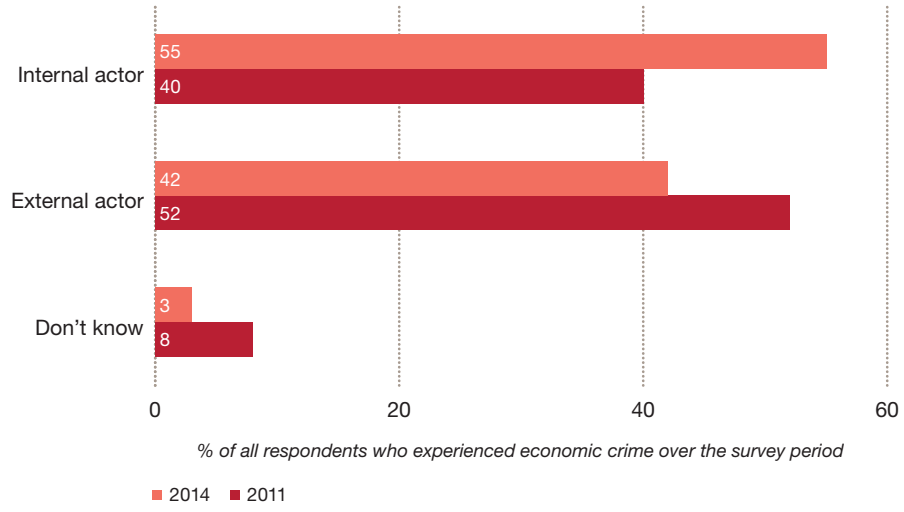
Each year Swiss organisations are becoming more aware of the cyber threat they face. Ironically, as Switzerland continues to prosper, these favourable conditions will attract cyber criminals whose intent is to exploit our domestic organisations and infrastructure.

55% of reported fraud incidents were committed by someone within the organisation.

The thief in our midst

One of the steps in protecting organisations against the possibility of fraud is to gather as much information as possible about the perpetrators. Knowing who they are and where they come from is essential in pinpointing weaknesses in the organisation's processes and internal controls. Of those Swiss organisations that experienced economic crime in the past 24 months, 55% said the fraud was committed by someone within the organisation [Figure 15], an increase from 40% in 2011. On a global scale, we are observing the same trend, with 56% of economic crimes perpetrated by an internal perpetrator.

Figure 15: The main perpetrator of the fraud

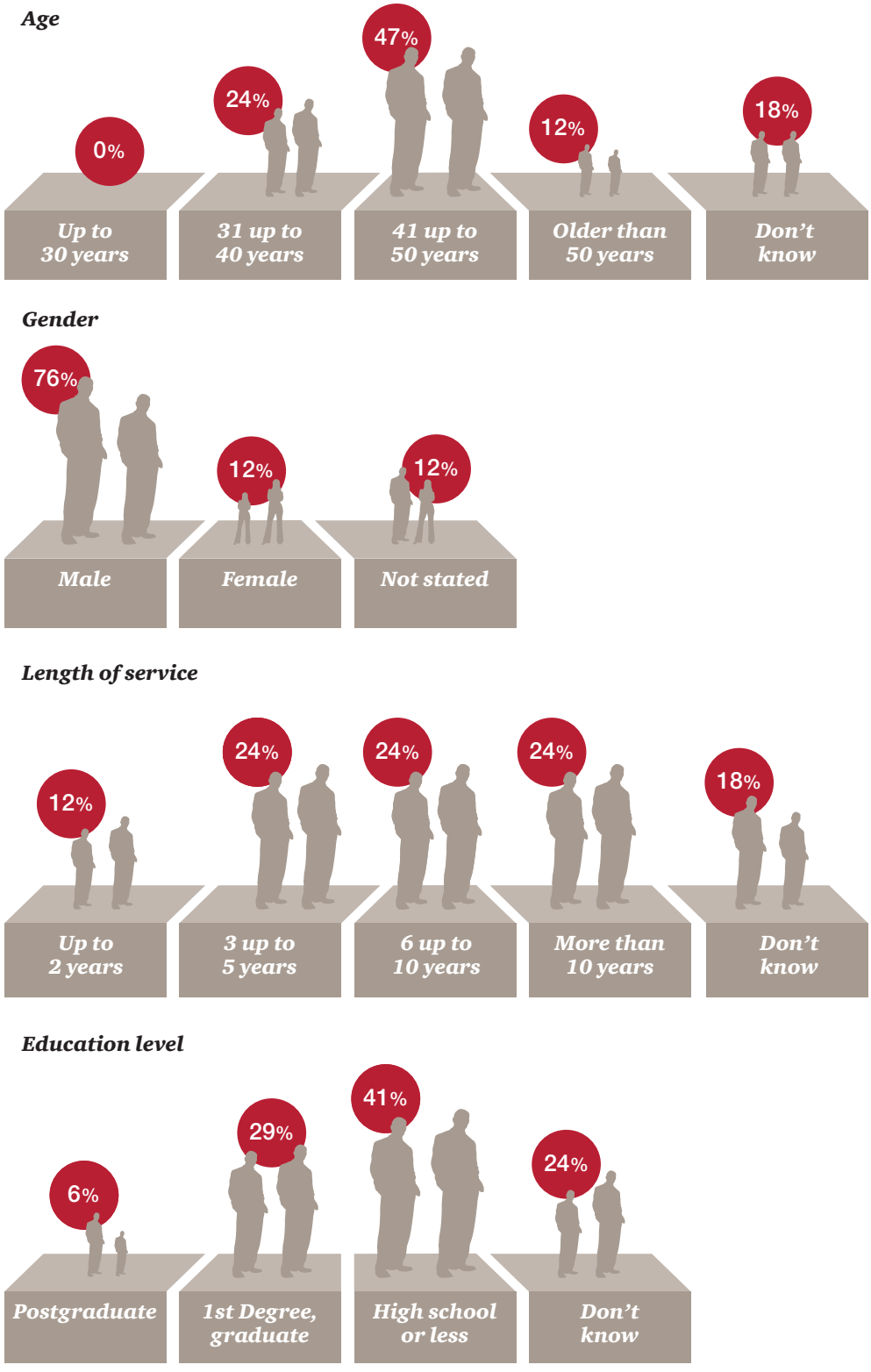


The fraudster profile

The internal fraudster

Asked about the internal perpetrator, 76% of the respondents said the culprit was a male, up from 50% in 2011. Interestingly, we note that the fraudster profile depicted by this year's survey is in line with the traditional profile encountered by anti-fraud practitioners – where the majority is male, has been with the company for several years, and is therefore familiar with the company's processes and controls [Figures 16–19].

Figure 16–19: Age, gender, length of service and education level of internal perpetrator



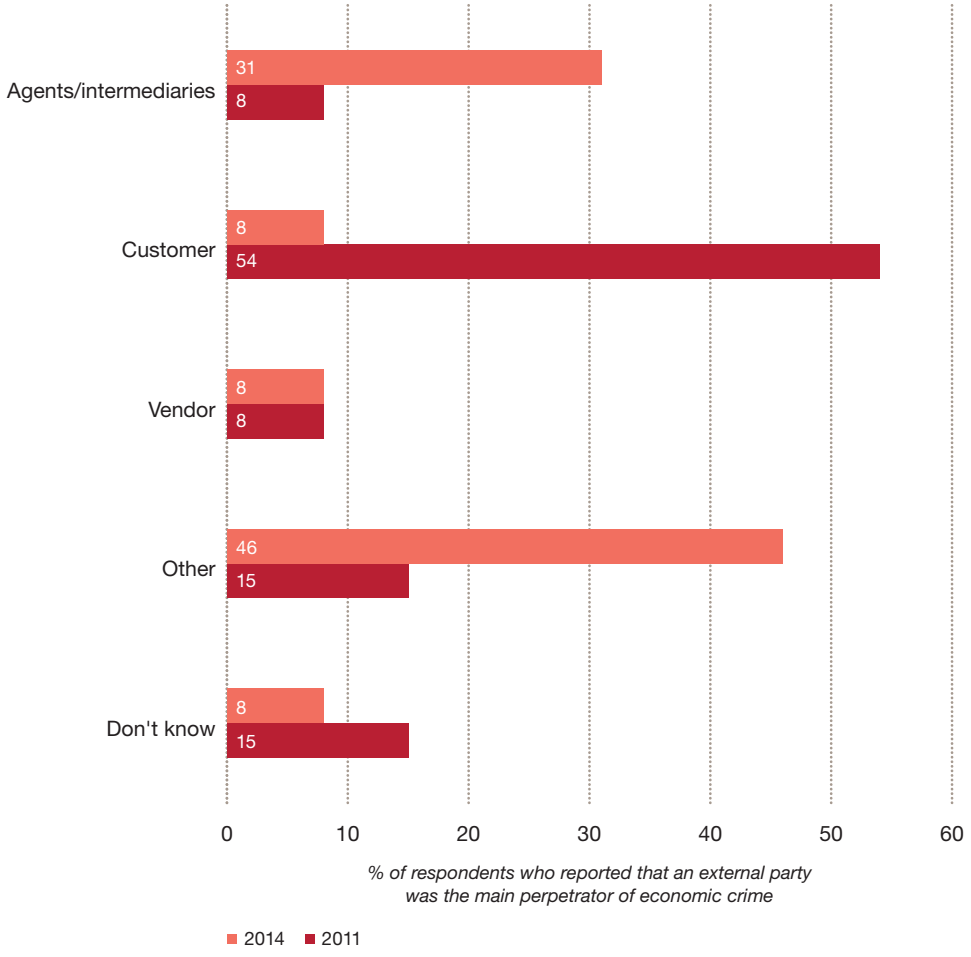
% respondents who reported that an internal party was the main perpetrator of economic crime

■ 2014

The external fraudster

In terms of the external fraud perpetrator, there have been significant changes since our previous survey. On one hand, the amount of fraud committed by agents and intermediaries has increased from 8% as reported in 2011 to 31% in the past 24 months and, on the other, fraud committed by the customer decreased from 54% to only 8%. Although organisations have become more effective in choosing their customers, they may have not applied the same methods when selecting their agents and intermediaries, which demonstrates the importance of third-party due diligence checks.

Figure 20: External fraudster

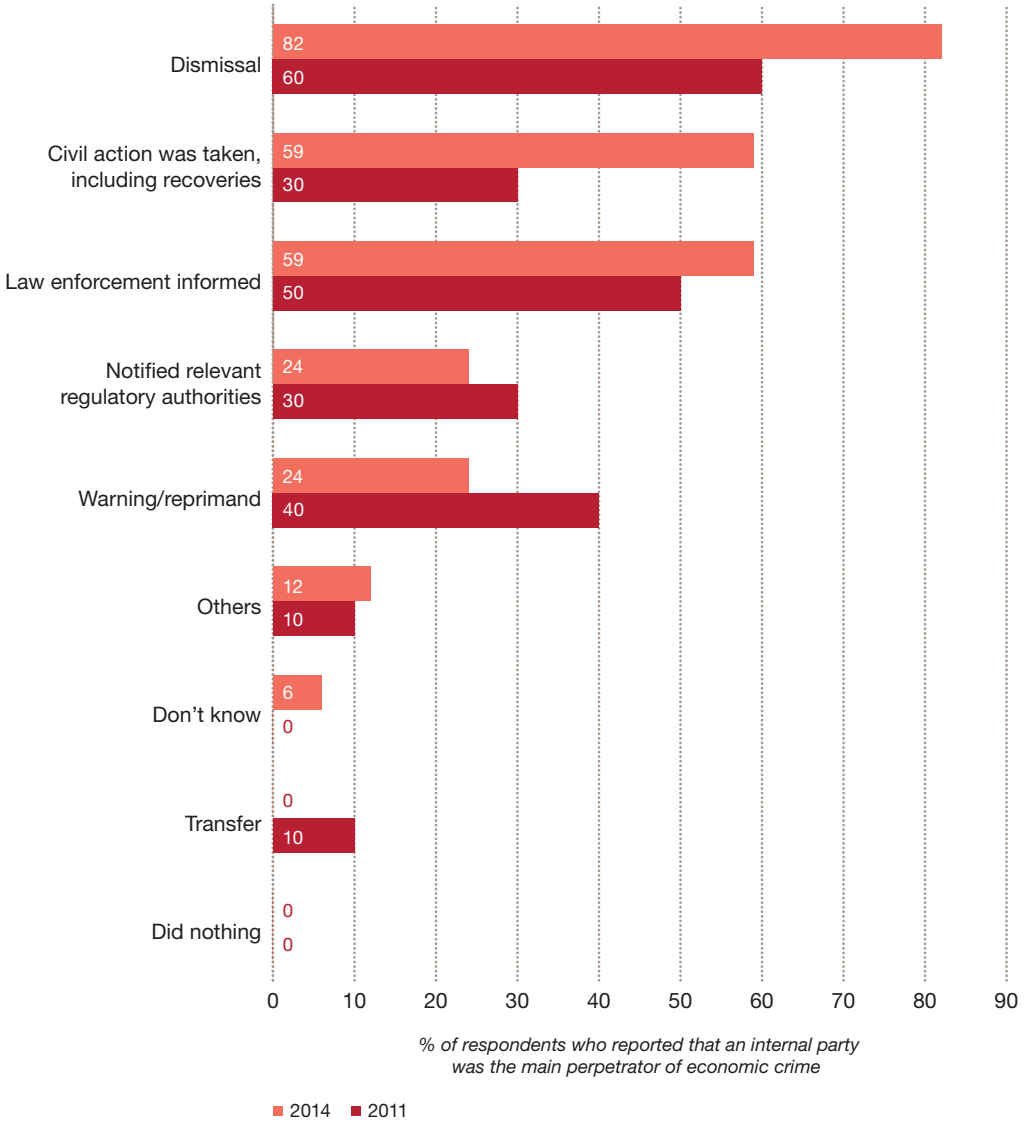


It is also interesting to note that a significant proportion of the external fraudsters in this year's survey do not fall into any of the main categories and were classified as "other" or "don't know" by our respondents. We believe that this trend may be related to the incidence of cybercrime, as 47% of respondents said the greatest risk related to this type of crime is posed by external parties.

Did the punishment fit the crime?

Organisations have several options on how to deal with fraudsters once they have been discovered. For internal infractions, disciplinary measures may start with a warning/reprimand and can, depending on the gravity of the crime committed, extend to dismissal. For external infractions, businesses may decide to cease the business relationship. Whilst in the previous survey the Swiss organisations appeared to have taken a more lenient stance in comparison to the global average when it came to disciplinary action, this year's survey suggests that they are taking a tougher stance. An increasing number of Swiss organisations take proactive measures aimed at protecting themselves against fraud and recovering damages, thereby going beyond a simple warning/reprimand or transfer of the fraudster within the organisation.

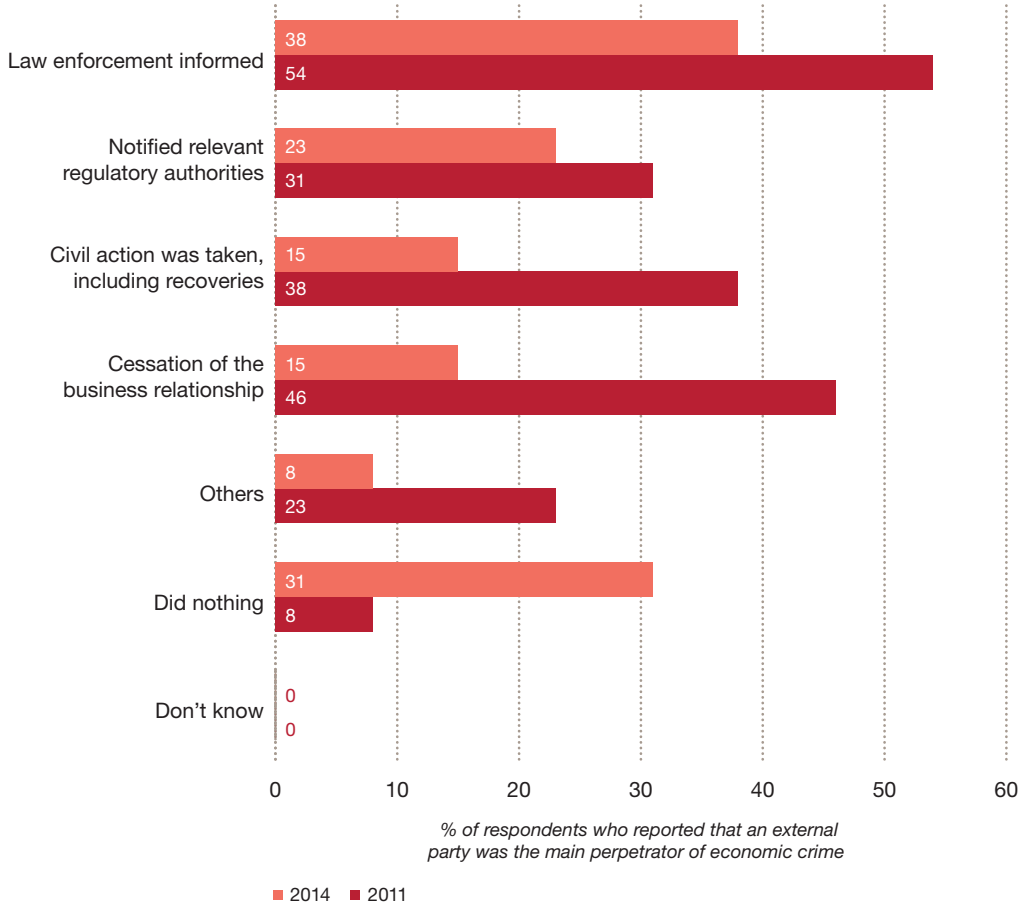
Figure 21: Actions taken against internal fraudsters



In fact 82% of the Swiss respondents chose to dismiss the individual involved in internal fraud and a further 59% took civil action against the perpetrator as well as sought to recover damages. This is more than a 20% increase for both of these measures compared to the 2011 readings. Furthermore, Swiss organisations are tougher on their perpetrators in comparison to respondents globally, where 79% of the companies dismissed the internal perpetrator and 44% initiated a civil action.

Surprisingly, this year's survey shows that Swiss organisations are less consistent when dealing with external perpetrators. Even though they appear to have improved their ability to identify external fraudsters, a striking 31% of the Swiss respondents who had been affected by external fraud took no action against the fraud perpetrator [Figure 22]. This is a significant increase in comparison to 2011, which may be explained by the recent rise of cybercrime in Switzerland where this type of fraud usually involves an unknown external party. Even though organisations are able to classify the type of perpetrator (for example a hacker), it would be difficult to uncover their identity, which makes taking specific measures against them rather challenging.

Figure 22: Actions taken against external fraudsters



Moreover, only 15% of the Swiss participants chose to cease the business relationship and a further 15% took civil action against the external perpetrator, a rate that is lower than the global average. In addition, 38% of the Swiss respondents reported having informed law enforcement authorities, which is also the measure most commonly taken by respondents globally (61%).

To catch a thief – methods of detection

There are many different ways to detect that an economic crime has occurred. The most straightforward method is to implement well-designed internal control mechanisms. The next step is to bolster the procedural detection system with a corporate environment that fosters zero fraud tolerance, given that a human element is essential in detecting fraud. However, we also recognise that fraud can be discovered by accident, perhaps by parties outside the realm of the organisation itself and beyond the influence of management.

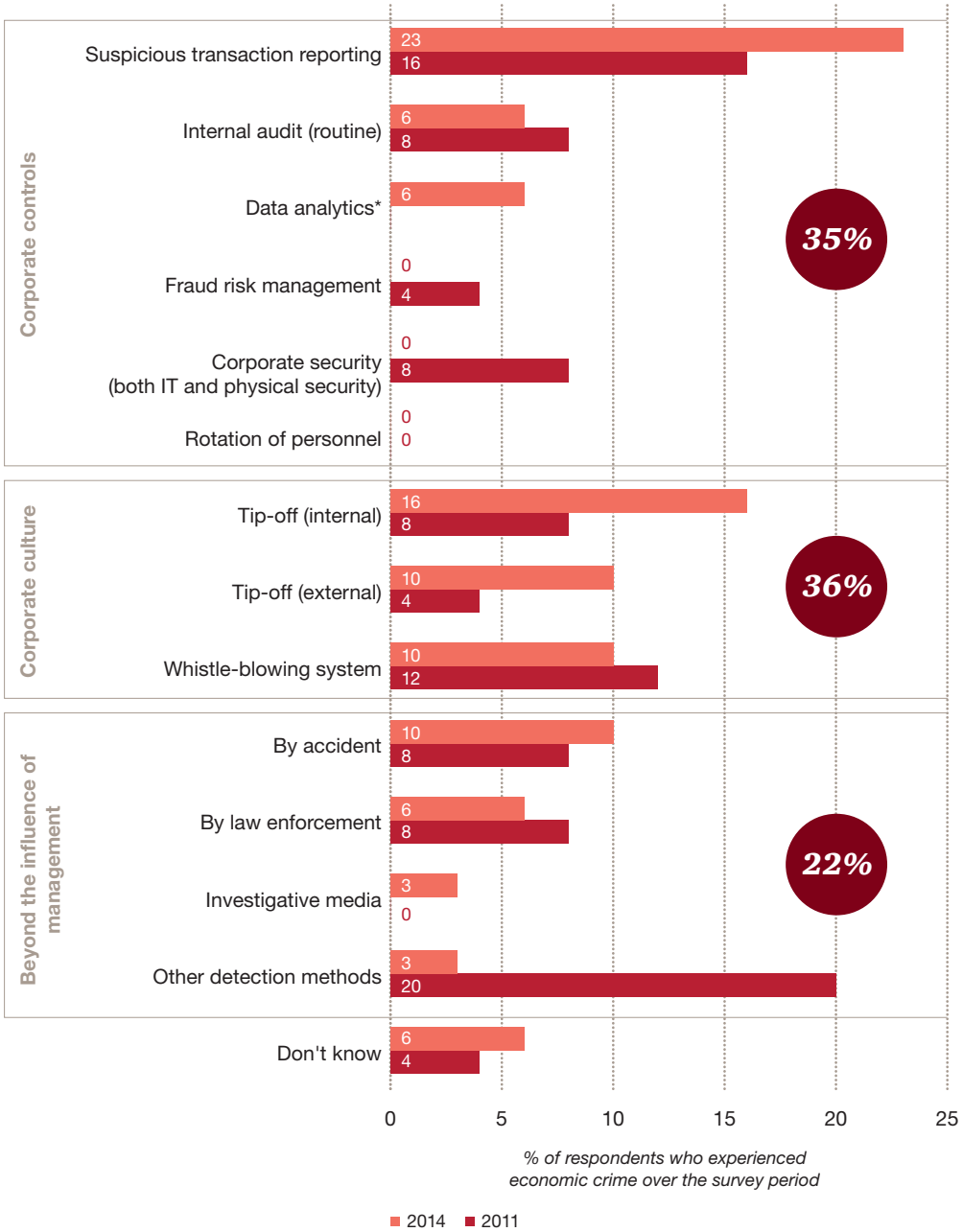
This year's survey shows that corporate controls as well as culture were more or less on a par in terms of their effectiveness, whereby more than one in three of the reported fraud incidents were detected by both of these methods independently. It is interesting to note that, whilst the overall effectiveness of corporate controls remained relatively unchanged during the survey period, we have observed an increase in fraud detected by corporate culture, i.e. from 24% in 2011 to 36% in the past 24 months [Figure 23].

In particular, there has been a significant rise in detection through data-driven fraud discovery methods and through tip-offs. In fact, 29% of the Swiss organisations affected by economic crime stated that the fraud was initially detected by suspicious transaction reporting or data analytics (data-driven fraud detection methods), compared to only 16% in 2011. A further 26% of the respondents mentioned external and internal tip-offs, a 14% increase over the 2011 figures.

The third key detection method in Switzerland is attributable to the whistle-blowing system with 10% of the respondents affected by fraud reported that it was initially detected through this method, compared to only 5% globally. Furthermore, over half of all Swiss respondents (52%) reported having a whistleblowing mechanism in their organisation, which is lower than then the global average (62%) and may suggest that Swiss companies have more sophisticated whistleblowing processes. Interestingly, our respondents' perception of the effectiveness of this process does not actually reflect reality as 51% of them rate their company's whistleblowing mechanism as only slightly effective or not effective at all.

Overall, the survey reveals that participating Swiss organisations may have increased the quality of their corporate controls and/or introduced new, more effective fraud-detection methods since the last survey. In particular, this year's survey demonstrates the progress made by Swiss companies in developing an anti-fraud corporate culture. This highlights the increased awareness of organisations of the need to improve the environment where anti-fraud controls operate, which starts by setting an appropriate tone at the top, fostering a "no tolerance for fraud" corporate culture, and heightening transparency within the company.

Figure 23: Methods of detection



* Data analytics was added as a new category in the 2014 Survey.

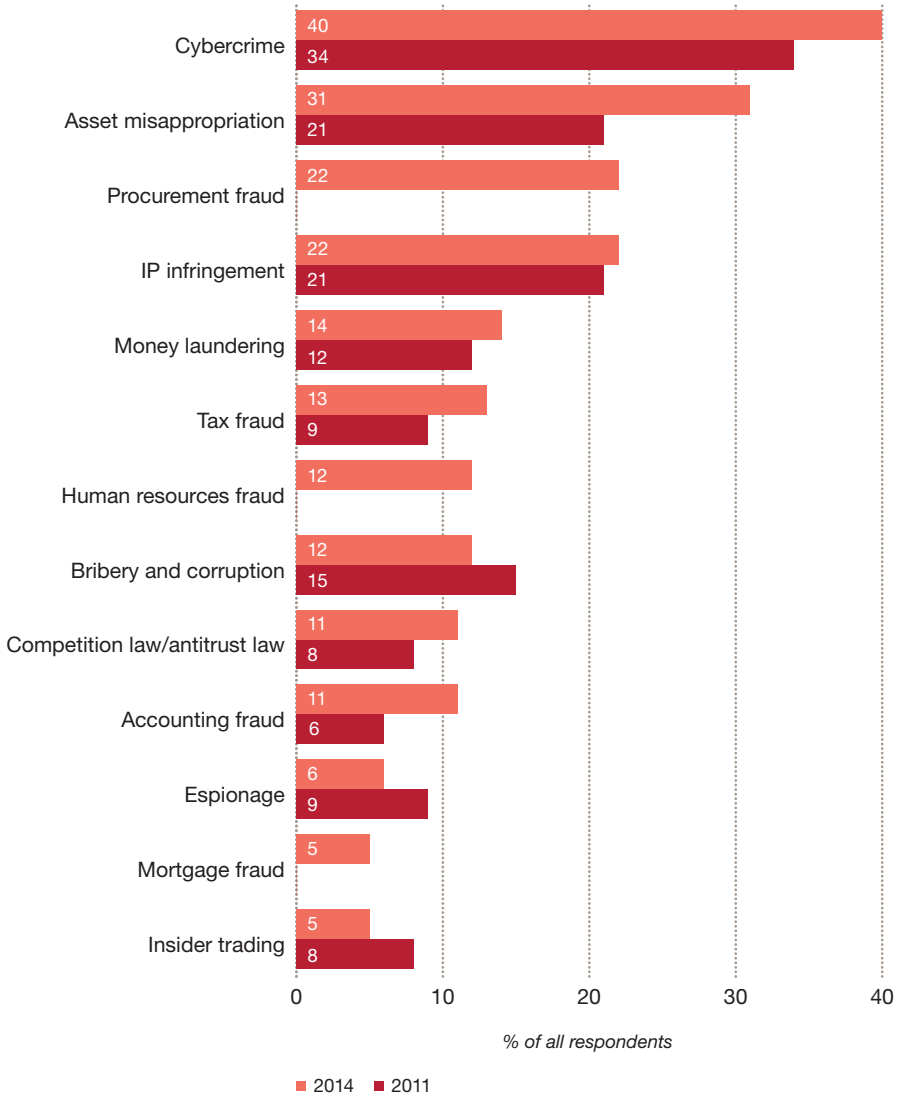
Swiss respondents expect cybercrime, asset misappropriation and procurement fraud to be the top three types of fraud affecting their organisation in the next 24 months.

The outlook – perception versus reality

It is quite clear that over half of the Swiss respondents are rather confident and believe that they will not fall victim to economic crime in the next 24 months. We do, however, note growing concern compared to 2011 especially with regard to cybercrime, where 40% of the respondents believe they will experience this type of crime in the future, a reading that exceeds even the easiest fraud to commit, i.e. asset misappropriation. We also note that respondents are concerned about procurement fraud. This type of fraud can be expected to remain amongst the top five economic crimes in the years to come [Figure 24].

In addition, due to growing concerns and despite the strengthening of corporate controls and corporate culture, it appears that Swiss companies took a less complaisant stance in terms of fighting fraud over the past 24 months.

Figure 24: Perception of future likelihood of economic crime



About the survey

The 2014 Global Economic Crime Survey was completed by 5,128 respondents (compared to 3,877 respondents in 2011) from 95 countries (compared to 78 countries in 2011). Of the total number of respondents, 50% were senior executives of their respective organisations, 35% represented listed companies and 54% represented organisations with more than 1,000 employees.

The Swiss survey was completed by 83 organisations, of which 42% are listed companies. Of the total number of respondents more than half were board members or senior executives within their organisations.

Terms and definitions can be found in the Global Economic Crime Survey.

Please note that due to rounding, the results as presented in this report may not add up to a 100% where applicable.

www.pwc.ch/crimesurvey

Contacts and contributors

Forensic Services in Switzerland

Gianfranco Mautone
Partner
Forensic Services
+41 58 792 17 60
gianfranco.mautone@ch.pwc.com

Ralf Baumberger
Director
Forensic Services
+41 58 792 17 63
ralf.baumberger@ch.pwc.com

Roman Gauch
Director
Forensic Services
+41 58 792 17 66
roman.gauch@ch.pwc.com

Thomas Koch
Director
OneSecurity
+41 58 792 29 54
thomas.koch@ch.pwc.com

Sebastian Ahrens
Senior Manager
Forensic Technology Services
+41 58 792 16 28
sebastian.ahrens@ch.pwc.com

Swiss survey team

Selma Krkić
Manager
Forensic Services
+41 58 792 20 86
selma.krkic@ch.pwc.com

Kevin Kirst
Manager
OneSecurity
+41 58 792 28 77
kevin.kirst@ch.pwc.com

Silvia Svihrová
Assistant Manager
Forensic Services
+41 58 792 46 82
silvia.svihrova@ch.pwc.com