www.pwc.ch/crimesurvey

Cybercrime in the spotlight

Swiss Economic Crime Survey 2011

140 organisations provide a Swiss picture of economic crime.

November 2011

pwc

Compared to the results of the 2009 survey, the number of Swiss organisations that have experienced crime within the last 12 months has increased slightly from 17% in 2009 to 18% in 2011.

Contents

Introduction

We are pleased to present the Swiss supplement to our Global Economic Crime Survey (GECS) 2011. This year, in addition to exploring the effects of traditional economic crime on organisations, the survey also examines the impact of cybercrime as an emerging threat to businesses. Respondents were asked a number of questions about cybercrime which enabled us to determine the level of concern and general trends in relation to cybercrime.

The survey is divided into two key sections: cybercrime and the current fraud environment. It examines the responses and views given by 140 executives and managers about their experiences in relation to these topics within their organisations.

Cybercrime in the spotlight

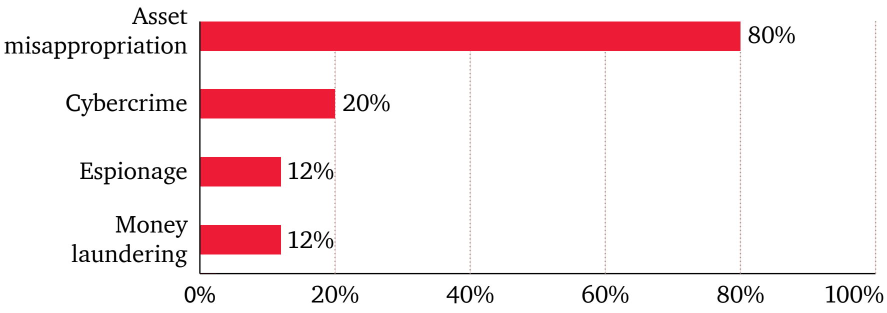
There is a considerable amount of ambiguity surrounding the definition of cybercrime as it is open to interpretation by many people; for example, is cybercrime the introduction of a Trojan horse or simply an employee misappropriating the assets of an organisation using a computer? However, for the purposes of our questionnaire, PwC has formally defined cybercrime as follows:

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

This year, cybercrime was ranked as the second most common economic crime suffered by Swiss organisations in the last 12 months (20%). When we asked respondents if they had experienced cybercrime in previous economic years the results were insignificant and were combined with 'other types of fraud'. This year we have introduced cybercrime as a separate category [Figure 1].

We are also seeing a considerable change in the perception of the risks associated with cybercrime amongst the Swiss respondents of which 52% reported that their perception of these risks had increased in the past 12 months. When asked the same questions, global respondents and those in Western Europe each reported a 39% increase.

Figure 1: Top three economic crimes as reported by Swiss respondents (% of reported frauds)



[1] As defined in GECS 2011 by PwC in conjunction with our survey academic partner, Professor Peter Sommer.

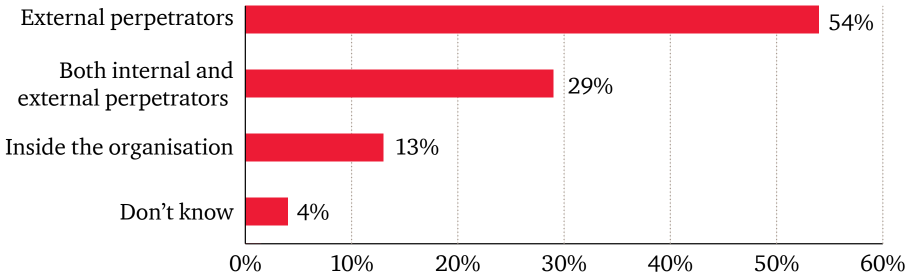
Cybercrime is on the rise and was the second most common crime reported by our respondents (20%)

Is cybercrime purely an external threat?

When asked where they saw the greatest threat of cybercrime could come from, 54% of the Swiss respondents thought that the threat was external to their organisation. Indeed, there are four major groups[2] of cyber criminals: foreign intelligence services, transnational criminal enterprises, corrupt competitors and 'lone wolf' criminals (often insiders), with the first three being external to the organisation.

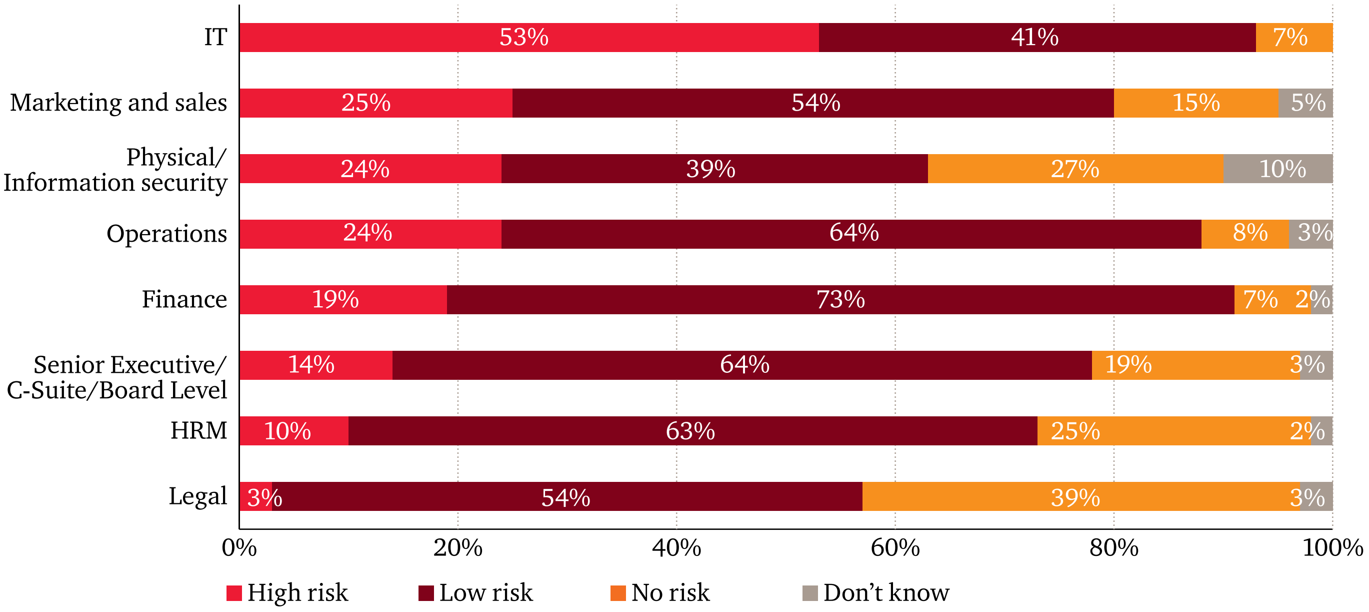
However, almost a third of the respondents thought that the greatest cybercrime threat could be external as well as internal (29%). This suggests that the perception of cybercrime is changing and that cybercrime is not only perceived as a crime committed by some distant anonymous organisation or person but can also come from within the organisation itself [Figure 2].

Figure 2: Greatest risk of cybercrime threat comes from (% of all respondents)



[2] PwC publication, 'Getting real about cyber threats: where are you headed?', June 2011

Figure 3: Perception of internal cybercrime threats (% of all respondents)

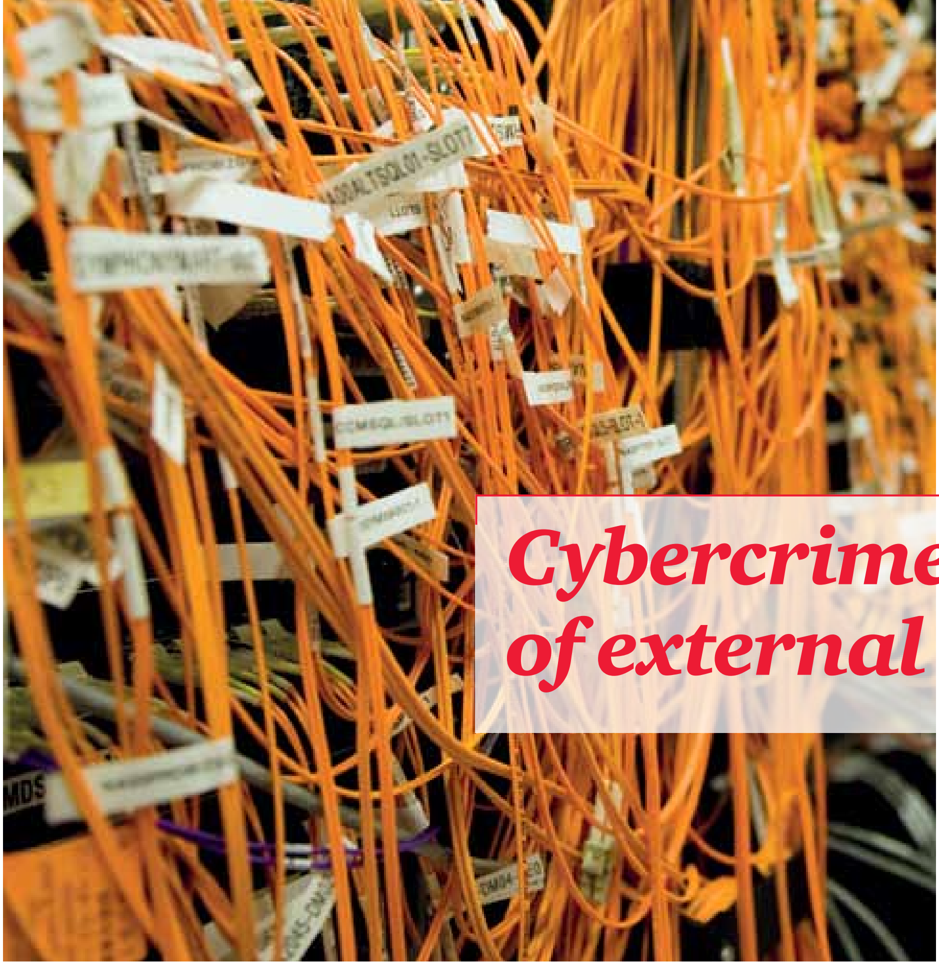


Unsurprisingly, 53% of those who perceived that the threat of cybercrime was internal to the organisation[3] thought that the greatest level of risk comes from within the information technology department which is the same globally. The second highest level of risk as perceived by the Swiss respondents comes from the marketing and sales department (25%) whilst globally it is thought to be the operations department (39%).

Almost three quarters of respondents perceived the finance department as the one posing the lowest risk (73%) [Figure 3]. This is quite surprising as IT infrastructure is integral to the operations of the finance department where all financial transactions of the organisation are recorded. This seems to indicate that there is a misconception of the level of risk that is posed by individual departments other than the IT department. In our experience, economic crime often involves the falsification of accounting records to either disguise criminal action or extract money from the organisation. It could be a costly mistake to exclude the finance department from strengthened IT controls that would reduce the risk of cybercrime in these areas.

54% of respondents think the threat of cybercrime is external to the organisation.

[3] This question was asked to all respondents who indicated that the greatest threat of cybercrime was internal to the organisation, or both internal and external.



Cybercrime – source of external threats

When asked where they saw the greatest external threat of cybercrime coming from in geographic terms, half of the Swiss respondents (50%) stated both from within and outside their country of operations. Furthermore, 39% of Swiss participants saw the greatest external risk of cybercrime as coming solely from outside their country of operations. Only a small proportion of respondents (5%) saw the external threat as coming from within Switzerland alone. On a global level, participants had a similar view as more than half (51%) saw the largest external threat concerning cybercrime coming from both within the country as well as outside.

For those respondents who indicated that cybercrime was a threat which came from outside the country[4], the following top five countries were **perceived** as the sources where cybercrime originated: Hong Kong and China, Nigeria, Romania, Russia, and the United States.

[4] This question was asked to all respondents who indicated that cybercrime risk was coming from outside the country or from both within and outside their country of operations.

There is a heightened level of awareness of the effects of cybercrime on organisations, with most respondents being concerned about reputational damage and loss of data.

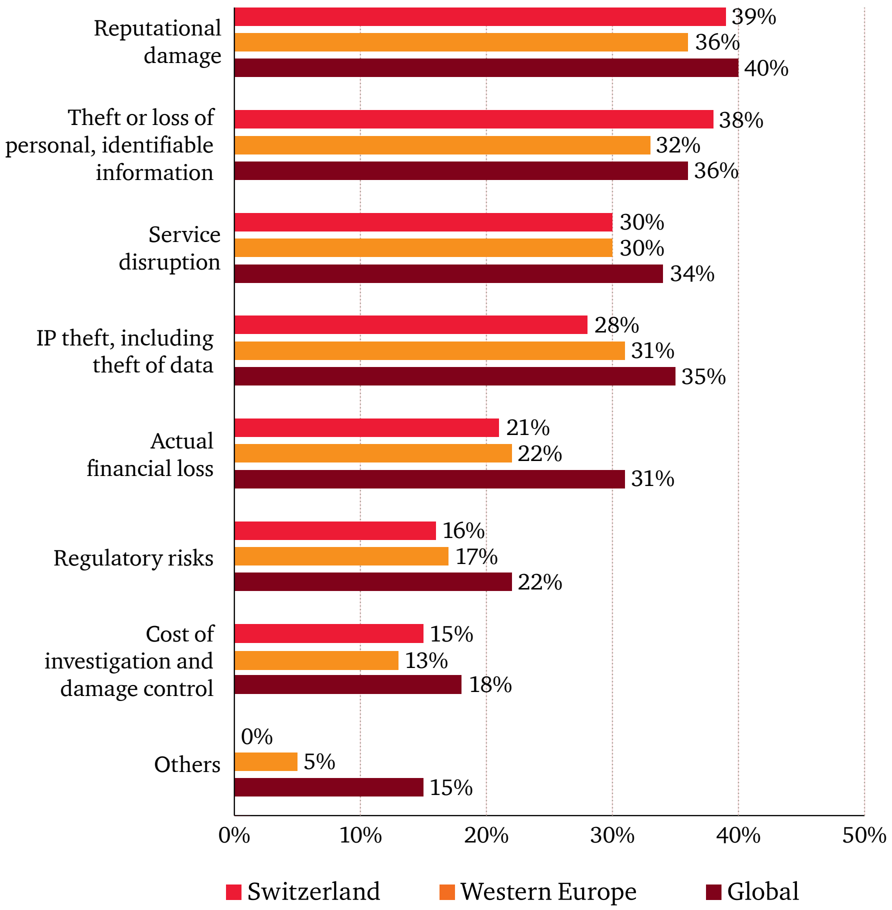
Effects of cybercrime on organisations

The true effect of cybercrime stretches far beyond mere data loss and service disruption. It may also result in regulatory sanctions, reputational damage, financial losses, intellectual property theft and diminished shareholder value. In fact, when Swiss respondents were asked how concerned they felt about the effects of cybercrime activity on their organisations, the top three concerns were reputational loss (39%), theft or loss of personal, identifiable information (38%) and service disruption (30%). Globally as well as compared to the results from Western Europe the trends appear to be similar [Figure 4].

It may be said that, generally, there is a very high level of fear of cybercrime although Swiss respondents believe they have adequate in-house capabilities to fight cybercrime, as shall be examined in the next section. However, this level of fear is not unusual as the backdrop for cybercrime is complex and continually evolving, and it shows a growing awareness of what cybercrime entails.

Regardless of the level of concern, organisations cannot afford to ignore the potential collateral damage that may be suffered as a result of cybercrime. By addressing these concerns and remedying them, organisations may be able to gain a competitive advantage if they are viewed as a secure business in the market.

Figure 4: Concerns about the effects of cybercrime on the organisation (% of respondents who stated very concerned)



Organisations appear to be largely unprepared when dealing with cybercrime incidents – despite heightened fears.

Is your organisation prepared?

There is a heightened awareness of cybercrime threats: 52% of our respondents perceived that the risk of cybercrime to their organisation had increased in the last 12 months compared to 39% of respondents globally. Although our respondents are aware of the risks they appear to be doing little to counter them.

This means that organisations still have a long way to go in implementing sufficient measures to effectively deal with cybercrime incidents. As a first line of defence, they should strengthen their preventative controls to reduce the risk of cybercrime occurrences. Secondly, organisations should have a sound infrastructure that allows them to have unequivocal know-how, including access to external investigators, to effectively and efficiently deal with incidents of cybercrime once they occur.

Our survey shows:

- **36%** of all Swiss respondents do not have or are not aware of whether their organisation has **in-house capabilities to prevent and detect cybercrime;**
- **56%** do not have or are not aware of whether their organisation has the **in-house capability to investigate cybercrime;**
- **69%** do not have or are not aware of whether their organisation has **access to forensic technology[5] investigators;**
- **55%** do not have or are not aware of whether their organisation has a **media and public relations management plan** prepared for cases of cybercrime;
- **41%** do not have or are not aware of whether their organisation has **controlled emergency network shut down procedures** in the event of a cybercrime occurrence.

[5] Forensic technology is the application of computer investigation techniques to gather, preserve and analyse digital evidence.

How do Swiss organisations manage cybercrime risks?

Organisations in Switzerland and globally are more reactive than proactive: 52% of the Swiss respondents and 48% of the global respondents only engage external experts after a cybercrime incident has occurred. A further 5% of the Swiss respondents are not aware at what stage their organisation would enlist the assistance of external experts. In common with reactions to other forms of economic crime, there appears to be a tendency for organisations to focus on investigating and evaluating what has gone wrong rather than investing proactively to prevent losses in the first place. In addition, delays in instigating an investigation, potentially compounded by lengthy appointment processes for specialised support and a shortage of specialised Forensic Technology Service ("FTS") experts on the market, could impede the quality of any investigation and the likelihood of recovering any losses.

In dealing with incidents of cybercrime a large number of organisations are reactive, rather than proactive.

Once an incident occurs 77% of Swiss respondents engage external experts; this figure is 12% higher than that for global counterparts. A high number of respondents would also consult with internal staff (74%). This indicates that although organisations are confident about the internal skill base they seek additional advice from external experts to complement the skills of their employees. In addition, Swiss organisations are more likely to inform law enforcement bodies (63%) than respondents globally(51%).

Ultimate responsibility for managing cybercrime within the organisation

Swiss respondents were asked where the overall ownership and responsibility for preventing cybercrime risks resides within their organisation. More than half (56%) reported that the overall responsibility for cybercrime related matters lies in the hands of the Chief Information Officer (CIO) or Chief Security Officer. Only 26% reported that the Senior Executives or the Board should have the overall responsibility in regard to cybercrime risks within their organisation. This also corresponds to the global respondents where only 20% perceived that the overall responsibility in cybercrime prevention should lie with the Board [Figure 5].

Only 26% of respondents believe that the Board should have the ultimate responsibility for cybercrime related matters in the organisation.

We believe there is a misconception of the level of responsibility that the CIO should have when it comes to matters of cybercrime. The role of the CIO should be in advising the Board and the Senior Executives of the threats of cybercrime to the organisation, and amongst others, to design appropriate safeguards which could mitigate these risks. Ultimately, it is the Board together with the Senior Executives that have the overall ownership and responsibility in this matter. Organisations should set up a cybercrime incident emergency plan in order to avoid any uncertainty regarding responsibilities, and to avoid delays, mistakes and inefficient and costly actions in the case of an occurrence.

Swiss respondents were also asked how often Senior Executives and Board members review the risks that cybercrime presents to their organisation. Less than a third (31%) conduct a review once a year and about a fifth (19%) engage in reviewing their organisation's exposure to cybercrime only on an ad-hoc basis. This shows a significant level of complacency of the leadership teams when it comes to cybercrime as they should be more involved and proactive due to the evolving nature of cybercrime. Even more surprisingly, a substantial part of the leadership team (11%) still does not consider cybercrime risk reviews to be necessary at all. Almost a fifth (19%) have no knowledge how often such a review takes place. This is worrying insofar as the perception of cybercrime risks has increased [Figure 6].

Figure 5: Perception of ownership and responsibility by department (% of all respondents)

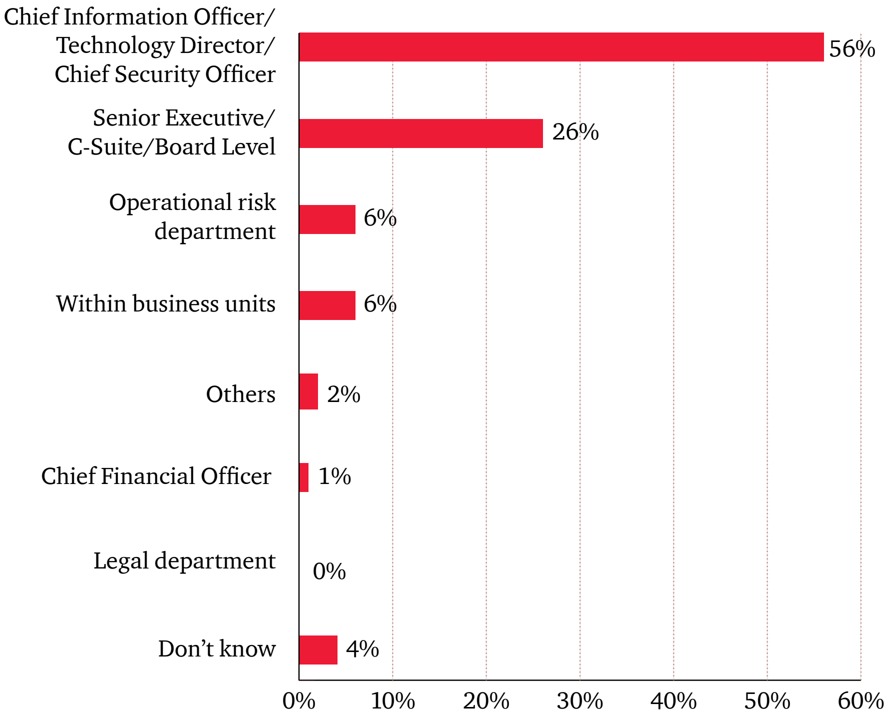
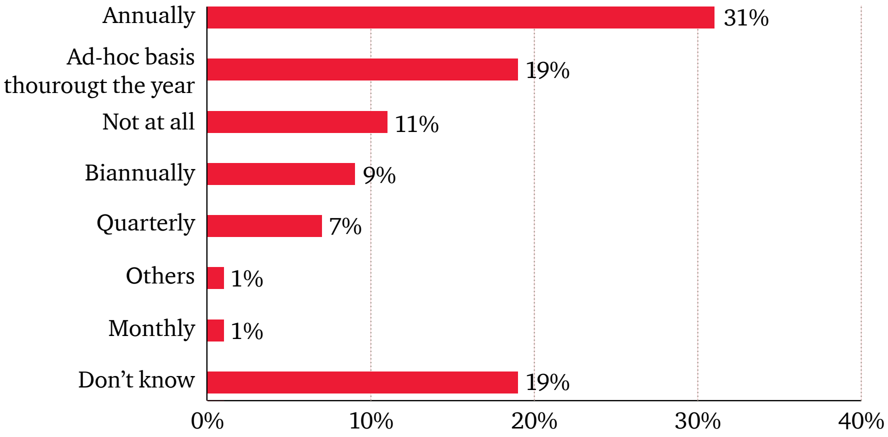
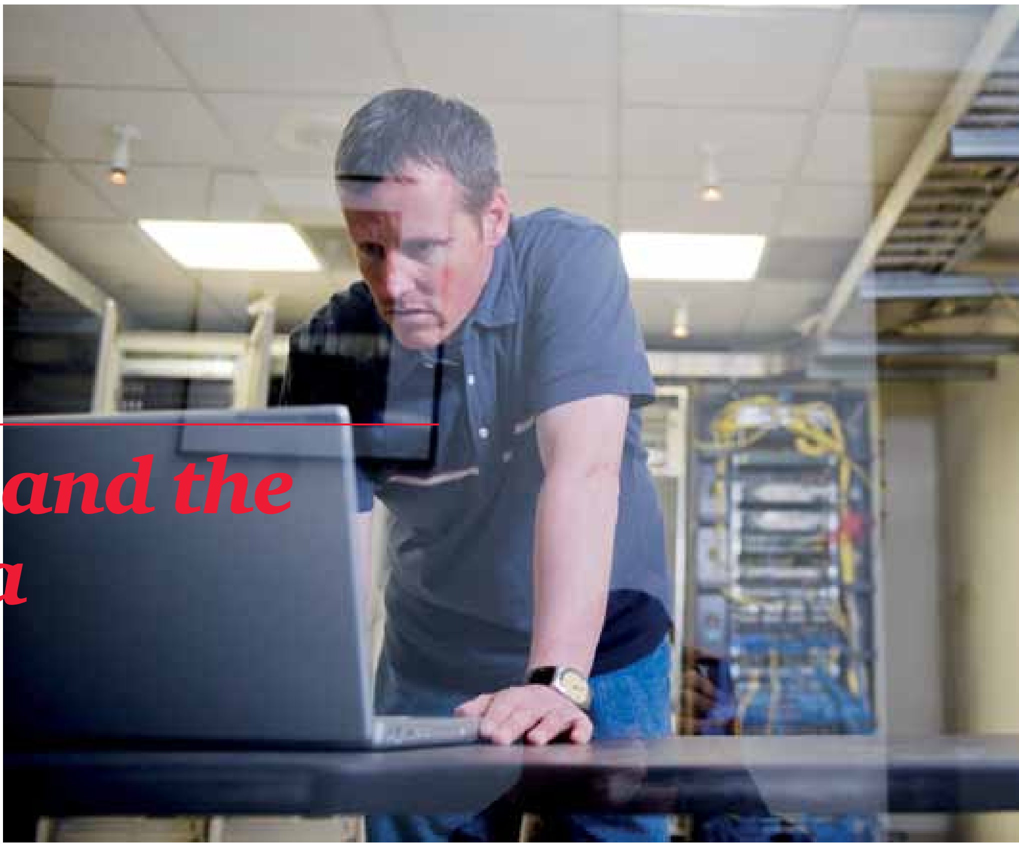


Figure 6: Review of cybercrime risk by the CEO and the Board (% of all respondents)



Cybercrime and the social media



Although they have already accepted the use of social networking sites by their employees, many organisations are still not aware of the risks that social media sites, such as Facebook, Twitter and LinkedIn, can pose to their organisations. Whilst social media is not a direct source of cybercrime itself, it can be used for social engineering attacks, such as phishing, or to spread viruses and malware which can expose organisations to theft of sensitive data and reputational loss.

Our survey shows that 49% of the Swiss respondents reported that their organisation did not monitor the use of social media sites or that they were not aware if their organisation monitors usage of such sites at all in comparison with 60% of respondents surveyed globally. This indicates that a large number of organisations are not aware of the risks that social networking sites can pose to their businesses.

The organisations that do monitor social media usage largely monitor external and internal electronic traffic including web-based activity (82%). This is followed by further safeguards in employee contracts which stipulate proper usage of internal documentation and information by employees (76%).

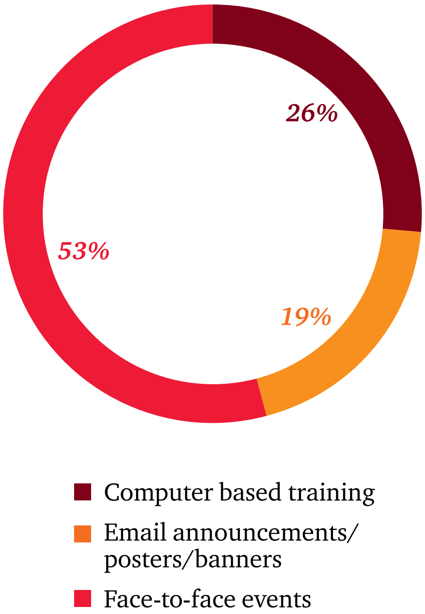
41% of respondents received no cybercrime related training in the last 12 months.

Cyber security training in Swiss organisations

Swiss participants were asked what types of cyber security related awareness training – if any – they had received over the past 12 months. For those who had received some type of training, the top three methods were email announcements (41%), face-to-face events, such as presentations or workshops (24%), and computer-based training (18%).

However, the most worrying finding is that a large number of participants (41%) did not receive any form of cyber security related awareness training at all. In the light of the increased perception of cybercrime risks by organisations these results are quite unexpected.

Figure 7: Perception of cybercrime training effectiveness by type (most effective, % of all respondents)



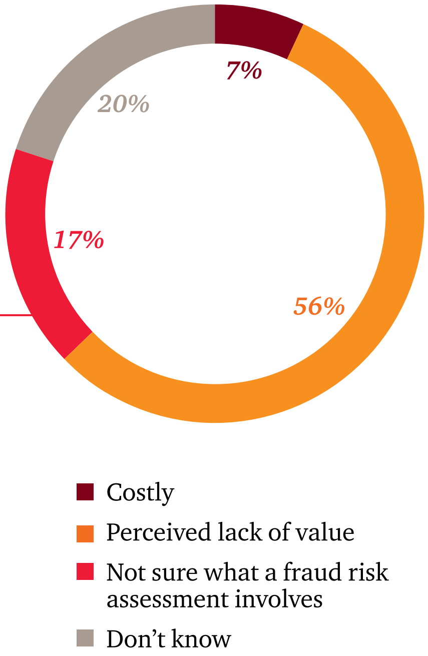
Our respondents were also asked which type of training they found most effective: 53% found face-to-face training to be the most effective type of cyber security awareness training although only 24% actually received this type of training. Face-to-face training is often costly to conduct and since organisations are still undergoing budgetary cuts this result is not unusual.

Moreover, only 19% of Swiss respondents perceived email announcements to be the most effective type of cyber security awareness training despite the fact that email announcements were the most frequently received type of training [Figure 7].

We believe that Swiss employees are not receiving enough, if any, training and where training is given it is not perceived to be very effective or meeting the requirements of employees. Organisations should, therefore, increase and adapt their training offerings which in turn could help mitigate the risks of cybercrime.

Section II: The current fraud environment

Figure 9: Reasons for not performing any fraud risk assessments in the last 12 months

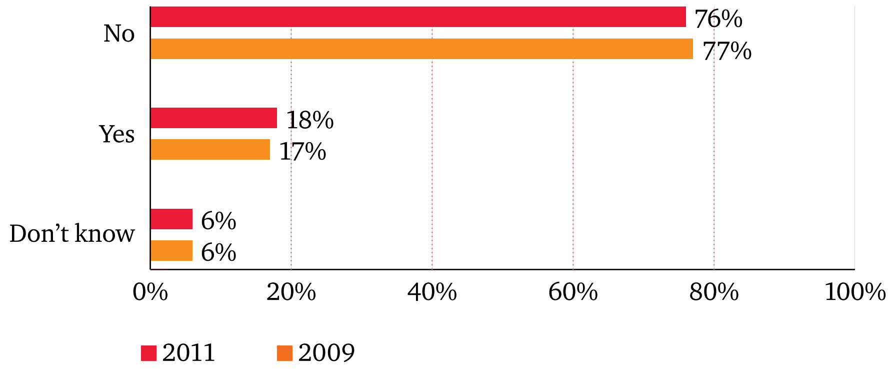


How did Swiss organisations fare in comparison to 2009?

Compared to the results of the 2009 survey, the number of Swiss organisations that have experienced crime within the last 12 months has increased slightly from 17% in 2009 to 18% in 2011. These results are surprising as our general expectation in the previous survey was that in the light of turbulent economic markets this number would significantly increase [Figure 8].

However, we still believe that a large number of economic crimes in Swiss organisations go undetected, especially when compared to organisations surveyed globally of which a total of 34% experienced an incident of economic crime in the last 12 months.

Figure 8: Incidents of economic crime: 2009 and 2011 (% of all respondents)



One factor that might have impacted the result this year is that organisations are still finding themselves in the midst of an unrelenting economic downturn and are thus continually making budgetary cuts not only in the area of internal audit and compliance but across the board. This makes detecting and preventing crime even harder.

Another factor that could have influenced the results is that organisations do not conduct regular fraud risk assessments. 29% of the organisations surveyed had not performed a fraud risk assessment in the last 12 months and of those 56% stated that there was a perceived lack of value in doing so. A further 37% were not sure what a fraud risk assessment actually involves or did not know whether their organisation actually performs such an assessment [Figure 9].

This demonstrates worrying educational and awareness issues and organisations need to dedicate more time in educating their employees about the benefits of performing regular risk assessments. Risk assessments are an essential tool for identifying critical gaps where organisations may be exposed to fraud.

Organisations are not aware of the benefits of fraud risk assessments.

Types of economic crime

Figure 10 shows the different types of economic crimes experienced by the Swiss respondents in the last 12 months. Asset misappropriation (80%), followed by cybercrime[6] (20%), espionage (12%) and money laundering (12%) were the most common types of fraudulent activity [Figure 10].

Asset misappropriation clearly stands out this year, showing a 16% increase in comparison to 2009. As it is the easiest crime to commit, and can also be committed by anyone in the organisation regardless of their rank, this result is not unusual. Globally, the situation appears similar with 72% of respondents experiencing economic crime in this category.

This year's survey shows a significant drop in accounting fraud since 2009, decreasing by 19%. This trend appears to be the same on a global level. In contrast to asset misappropriation, this type of fraud is more difficult to commit as it centres on the manipulation of accounting records and requires the perpetrator to have extensive knowledge of the internal controls surrounding the financial reporting system. The loss suffered is also often greater for the organisation when compared to asset misappropriation. There may be various reasons for this shift, and some of the factors that could have contributed to this are:

1. Our 2009 results showed that management was much more concerned with the survival of the business in the wake of the economic crisis and has, therefore, felt the pressure to manipulate financial results. In fact, as reported in our 2009 GECS, 49% of the global respondents felt that this was a factor that could have contributed towards creating more opportunities to commit fraud.
2. It may also simply be that organisations have now implemented tighter accounting controls, which are more difficult to circumvent.
3. Many organisations have reduced the headcount in recent years which could make detecting crime more difficult. If cuts were made in departments that were traditionally responsible for fraud management the extent of possible review may now be limited by fewer resources.
4. As there is a considerable amount of ambiguity about what cybercrime is, some respondents may have re-classified certain incidents of accounting fraud as cybercrime because it was committed using computers or other electronic devices.

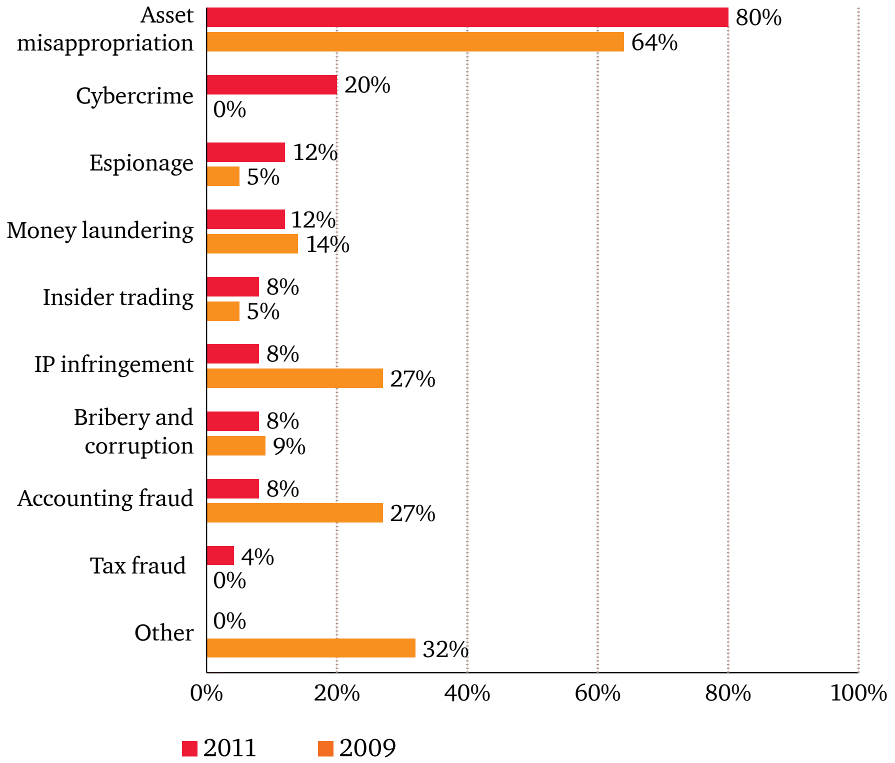
[6] As explained earlier, cybercrime is a new category included in the current survey which, due to low response levels, was included in the 'other types of fraud' category in our previous surveys. It is our belief that as organisations become more cyber savvy we will see an increase in the detection of this type of fraud in the future.

With 80%, asset misappropriation is the highest ranking economic crime.

This year, we have also introduced sustainability fraud as another emerging crime into the questionnaire; however, our respondents experienced no such incidents in the last 12 months. Given the recent cases of sustainability fraud reported in the Swiss media these results are surprising. This trend is also evident globally, representing only 1% of reported frauds.

While all industries are affected by economic crime, some suffered more than others. 44% of the reported fraud incidents occurred in the financial services sector, followed by insurance, pharmaceuticals and life sciences, retail and consumer, and transportation and logistics with 8% reported cases in each industry.

Figure 10: Types of economic crime in the last 12 months compared to 2009 (% of reported frauds)



Swiss respondents think fraud is predominantly an external threat.

Who are the fraudsters?

40% of the Swiss respondents who suffered economic crime in the last 12 months said that the fraud was committed by someone within the organisation. A further 52% reported the main perpetrator to be external to the organisation. These results are in contrast to the global results where 56% of the economic crimes were committed internally and 40% externally.

Furthermore, 8% of the participants stated that they were unaware of who the perpetrator was. This is worrying as an important element in fraud prevention is knowing where fraud is likely to come from. Organisations therefore should gather as much information as possible about internal perpetrators in order to close any gaps in the anti-fraud internal control environment and thus be more prepared for future attacks.

The fraudster profile

When asked about the staff level of the internal perpetrators, Swiss respondents reported that 20% were from senior management, 10% from middle management and 70% were other employees [Figure 11].

Figure 11: Internal fraudsters (% of reported frauds)

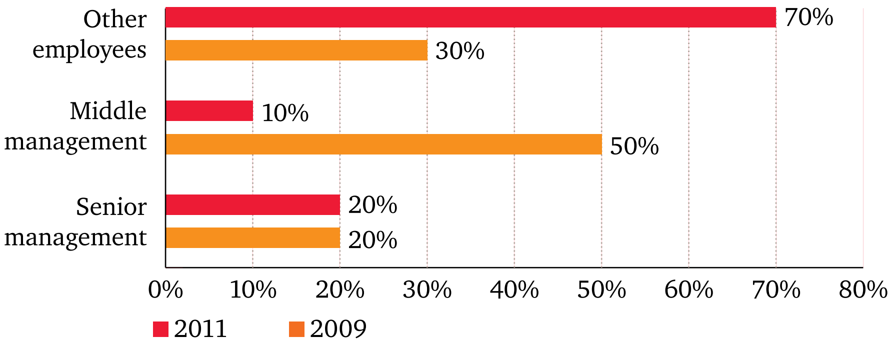
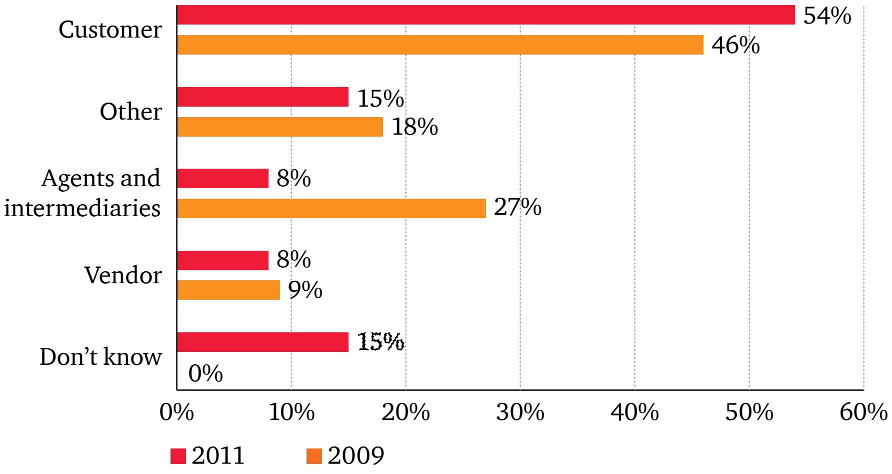


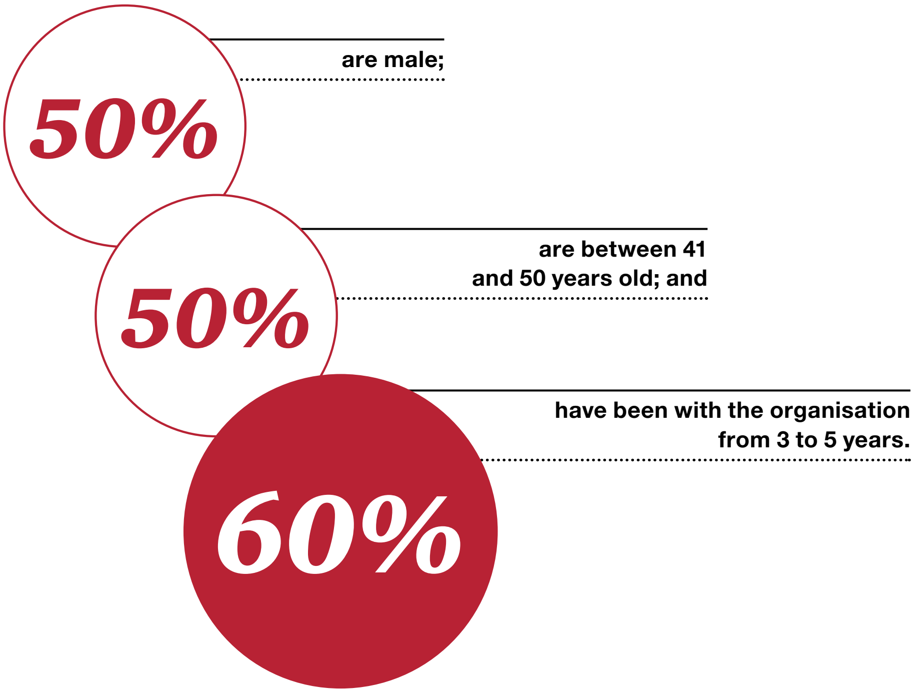
Figure 12: External fraudsters (% of reported frauds)



Compared to 2009, the percentage of internal fraudsters from senior management remained unchanged while there has been a strong shift from middle management (–40%) to other employees (+40%).

54% of those respondents who experienced economic crime committed by an external party stated that the crime was committed by the customer. The level of frauds committed by the customer has increased by 8% in comparison to 2009. There has also been a sharp increase in the 'don't knows' [Figure 12]. Whilst we appreciate that conducting extensive checks on customers and agents may not always be commercially viable, it is worrying that some organisations are not at all aware who the external perpetrators are.

The profile of the typical internal fraudster is as follows:



50% are male;

50% are between 41 and 50 years old; and

60% have been with the organisation from 3 to 5 years.

Only 46% of respondents ended the business relationship with the external fraudster.

Only 60% of internal fraudsters were dismissed in the last 12 months.

What actions do organisations take against fraudsters?

This year, the top three disciplinary actions taken to deal with internal perpetrators were dismissal (60%), notifying law enforcement bodies (50%) and issuing warnings (40%) [Figure 13]. This suggests that organisations are still taking a complacent stance when it comes to disciplinary action. They appear content with the fact that a large number of employees who commit fraud will remain within the organisation, having only received a warning, and seem to ignore the risk that they may commit such crimes again. This sends the message that organisations are lenient when it comes to incidents of fraud when they should be demonstrating zero tolerance for such behaviour.

When dealing with external fraudsters, the majority of Swiss organisations chose to inform law enforcement bodies (54%), followed by ending the business relationship (46%) and taking civil action against the external party (38%) [Figure 14].

Figure 13: Actions taken against internal fraudsters (% of all respondents)

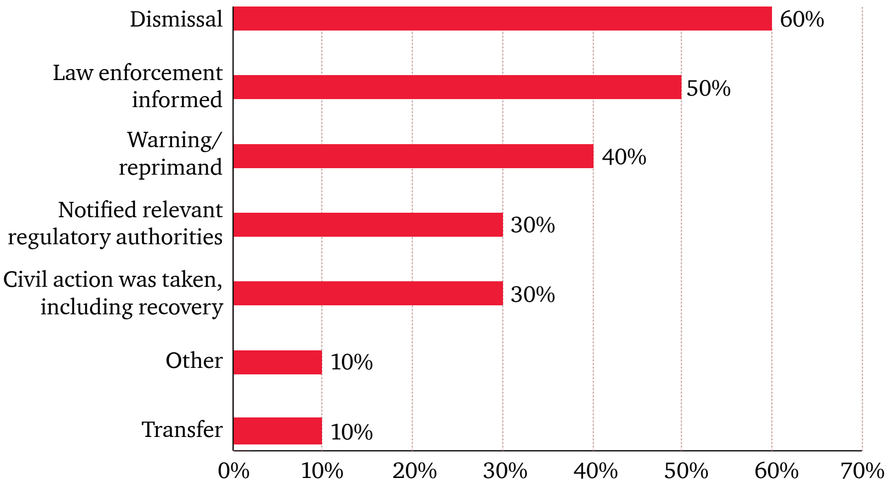
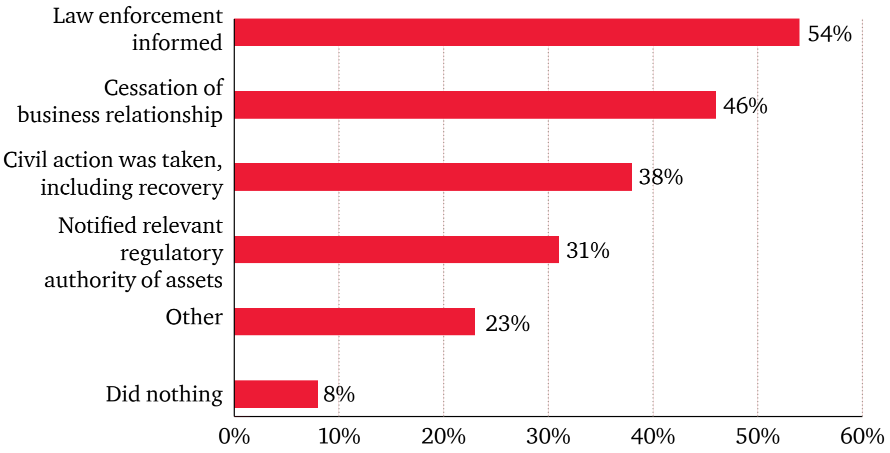


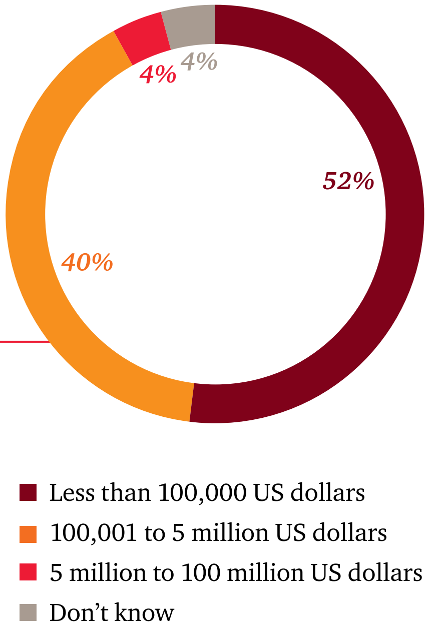
Figure 14: Actions taken against external fraudsters (% of all respondents)



The costs of economic crime

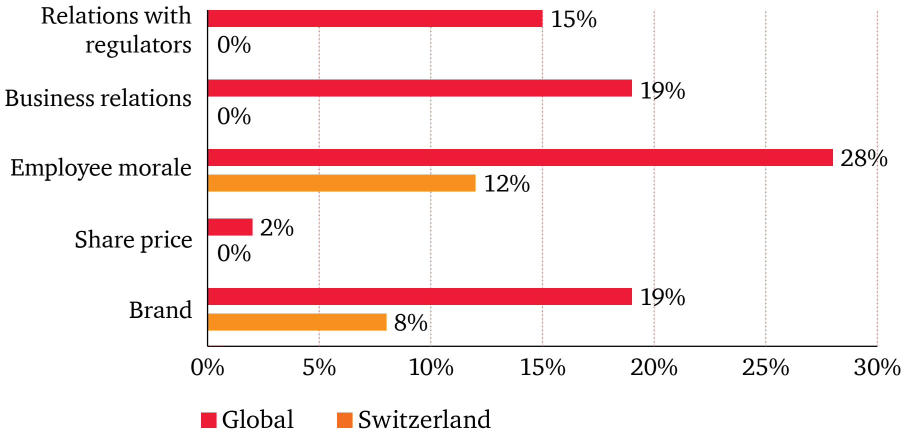
More than half of the respondents (52%) who experienced economic crime during the last 12 months reported the direct costs of fraud as being less than 100,000 USD. Compared to 2009, this is a 29% increase in this category [Figure 15]. The increase may be related to the emergence of asset misappropriation as the most prevalent source of economic crime in this year's results and the shift in the importance of employees rather than management as the main perpetrators. As employees typically have limited authority in comparison to management, they may not be able to commit the same magnitude of fraud in financial terms. Organisations may also be underestimating the fall-out that results from incidents of fraud, such as reputational damage or decreased employee morale and focusing only on the financial impact.

Figure 15: Costs of economic crime (% of reported frauds)



An organisation may potentially suffer additional indirect costs or collateral damage through incidences of fraud. When asked about the additional impact of fraud on the organisation, Swiss respondents seem to consider their organisations to be more resilient to incidences of economic crime than their global counterparts [Figure 16]. Only 12% of respondents reported that economic crime had a significant impact on employee morale and even less reported a significant impact on their brand or reputation (8%).

Figure 16: Perception of significance of collateral damage caused by economic crime (% of all respondents)



Detection

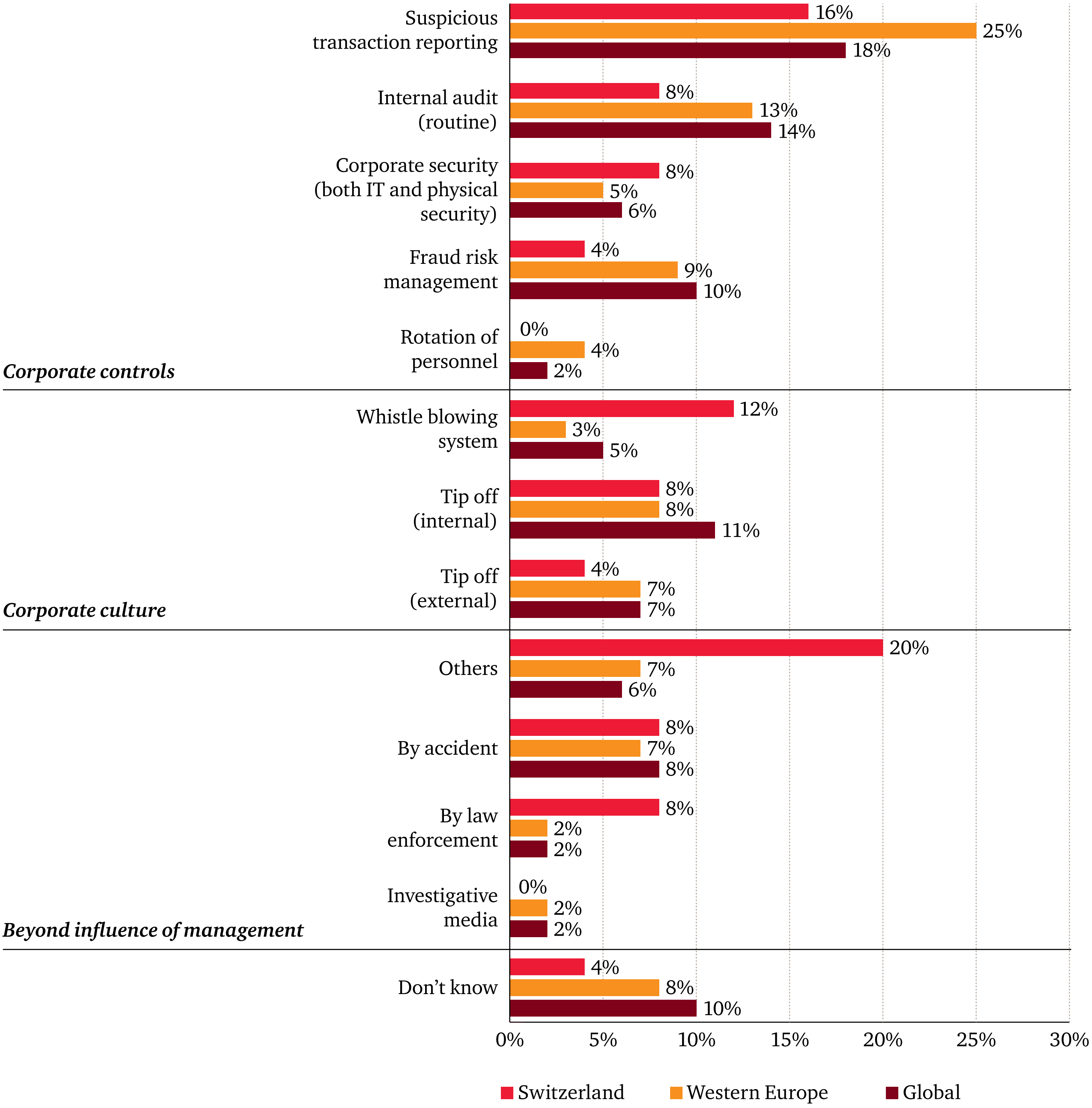
Respondents were asked how the incidents of economic crime were initially discovered. There has been a major decrease in crime detection by way of internal audit; from 36% in 2009 to 8% in 2011. On the other hand, there has been an increase in detecting crime with methods beyond management's control; from 0% in 2009 to 20% in 2011. This is rather concerning, especially when considered alongside the Swiss respondents' perception of a lack of value from conducting fraud risk assessments (see Figure 9), as it suggests that Swiss organisations may have relaxed efforts to uncover fraud by internal mechanisms and controls.

Furthermore, there is a decrease in detecting crime through fraud risk management controls; from 5% in 2009 to 4% in 2011. Switzerland is also lagging behind in this area when compared to organisations surveyed globally (10%) and in Western Europe (9%).

More incidents of crime were found by suspicious transaction reporting; this increased from 5% in 2009 to 16% in 2011. There has also been an increase in crimes reported through the organisation's formal whistle blowing system; from 0% in 2009 to 12% in 2011. Even though there is still no legal requirement for Swiss organisations to have formal whistle blowing systems in place this indicates that some organisations are taking steps in the right direction in order to combat fraud [Figure 17].

There has been a major decrease in crime detection by way of internal audit.

Figure 17: Methods of detection 2011 (% of all respondents)



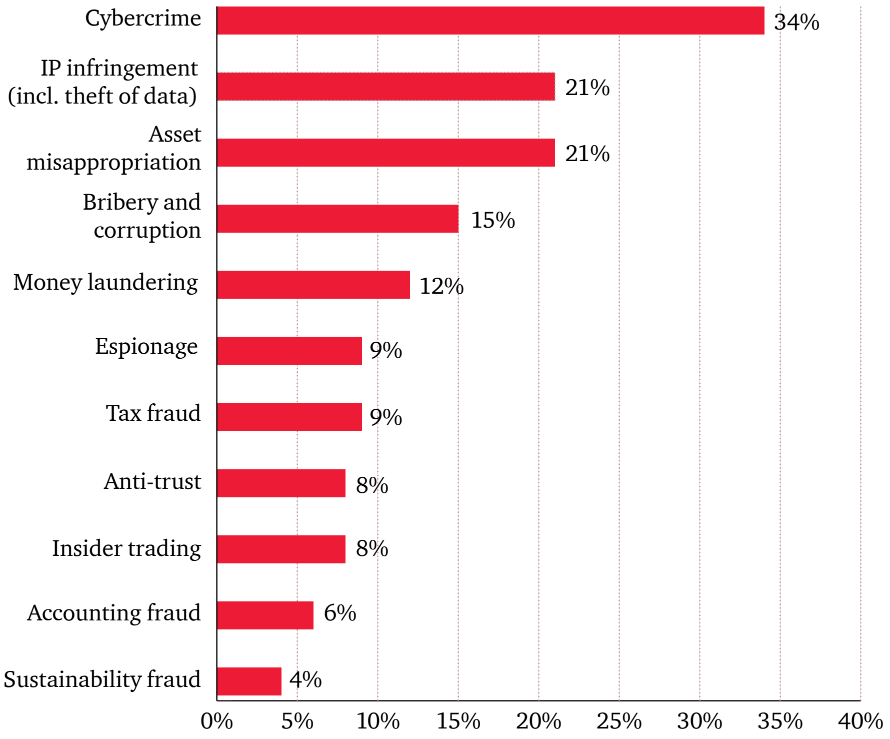
What lies ahead?

As in previous years, our respondents were asked to think about which types of crimes they thought most likely to occur in their organisations in the next 12 months. Unsurprisingly, cybercrime was on top of their list of concerns at 34%, followed by asset misappropriation (21%) and IP infringement (21%). They were least worried about accounting fraud (6%) and sustainability fraud (4%) [Figure 18].

While overall the figures suggest that Swiss respondents do not think that incidents of crime are very likely, we know from experience that the perception of fraud and the number of actual occurrences often differ greatly. It appears respondents consistently underestimate the risks and are far too optimistic in appreciating the seriousness of these matters. In addition, the responses here are inconsistent with earlier answers, when for example Swiss respondents stated that they think the risk of cybercrime has increased (52%).

Notwithstanding the current perception, the threat of economic crime is unrelenting and organisations must persist in their vigilance by strengthening anti-fraud controls and educating staff of its dangers.

Figure 18: Perception of how likely organisations are to experience fraud in the next 12 months (% of all respondents)



Survey demographics

The 2011 Global Economic Crime Survey is based on information supplied by 3,877 respondents in 72 countries who completed our Web based questionnaire. More than half of the respondents were chief officers or board members within their organisation. The survey coverage provides us with a broad and deep assessment of economic crime around the world.

The Swiss survey included 140 organisations, 34% of which are listed on a stock exchange.

Terms and definitions can be found in the Global Economic Crime Survey 2011.

Please note: due to rounding the results as presented in the report as well as the figures may not add up to 100% where applicable.

Contacts

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

Ivo Hoppler
Partner, Forensic Services, Switzerland
Tel. +41 58 792 17 00
ivo.hoppler@ch.pwc.com

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

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

Ian Hasson
Director
Tel. +41 58 792 17 30
ian.hasson@ch.pwc.com

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

www.pwc.ch/crimesurvey