www.pwc.com/crimesurvey/fs

Fighting Economic Crime in the Financial Services sector

Financial Services sector analysis of our sixth Global Economic Crime Survey

pwc

Contents

About the report

45% of Financial Services organisations have suffered frauds in the last 12 months

We are pleased to present the Financial Services[1] ("FS") sector report from the results of PwC's sixth Global Economic Crime Survey, one of the most comprehensive studies of economic crime in the business world. The focus of our current survey is the growing threat of cybercrime, considering the significance and impact of this form of economic crime and the way in which it affects organisations globally.

The last two years have continued to be characterised by economic uncertainty. Our survey examines the current fraud landscape against this background, taking a closer look at what new frauds are emerging and who is committing them.

"People are highly motivated by fear of losing economic and social status relative to others (and sometimes in absolute terms too). Therefore, when times become harder, those who do not have strong ethical standards or fear being shamed, are more likely to commit frauds" – The Australian Institute of Criminology.

Furthermore, in this report we turn the spotlight onto the global trend of increased regulatory interest in fighting economic crime and associated pressures on FS organisations to have robust preventative and detective controls in place.

Our survey data of 3,877 responses spanning across 78 countries allows us to dig deeper and analyse the results by industry. The FS sector represented 23% of our overall survey population with 878 respondents from 56 countries. Respondents were asked a number of 'core' questions on economic crime in general, to enable us to detect long term trends, as well as questions specifically relating to cybercrime. Our findings provide some action points for those FS organisations who may no longer be achieving best practice.

1 Financial Services: Including retail and investment banking, insurance, investment management, stock broking and private equity.

Key highlights

The Facts:

- The FS industry continues to be the fraudsters' target of choice, primarily for asset misappropriation[2]
- 45% of FS organisations have suffered frauds in the last 12 months compared to 30% in other industries
- Cybercrime is the 2nd most commonly reported type of economic crime for FS organisations
- Nearly a third of staff in FS organisations have not received any cyber security related training
- External fraud remains the principle threat for FS organisations, but internal fraud is catching up
- The percentage of frauds where senior management are involved has seen a 50% increase in the last 2 years
- 1 in 5 of FS organisations failed to carry out a fraud risk assessment in the last 12 months
- Whistleblowing mechanisms are underused and under promoted by FS organisations

How to protect your organisation against economic crime:

- Cyber security should be embedded into the business and the risks fully defined and understood
- A fully defined cyber crisis response plan to protect against financial and non-financial loss should be in place
- Senior management need to proactively lead in the fight against economic crime
- More regular fraud risk assessments should be conducted to identify ever changing economic crime risks
- Whistleblowing mechanisms should be promoted and supported

2 Asset misappropriation (including embezzlement/deception by employees): The theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

Cybercrime – protecting against the growing threat

Cybercrime is a growing threat in a world where most individuals and organisations rely upon the Internet and connected technologies, opening themselves up to the risk of attack from global criminals from anywhere in the world. Against a background of rising incidents of data losses and theft, pharming, phishing, computer viruses and hacking, our survey scrutinised the significance and impact of this type of economic crime and the way in which it affects organisations worldwide.

Perhaps the biggest challenge when assessing cybercrime risks is the lack of any globally agreed definition; the same event might be categorised as "industrial espionage", "IP theft" as well as "cybercrime". For the purposes of this survey we have defined cybercrime as:

"An economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank details. It's only a cybercrime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one."[3]

Whilst cybercrime isn't that new for the FS sector, it is a particularly prevalent issue for FS respondents in comparison to other industry sectors and one that puts its customers, brand and reputation at significant risk. Regulators are increasingly viewing cybercrime as a key area of focus. FS organisations are expected to have appropriate systems and controls in place to fight the growing threat of cybercrime. For example, in the UK the Financial Services Authority ("FSA") has included "Data Security" within its top economic crime risks for some time. At a recent conference in China[4], Premier Wen Jiabao stated that the nation needed to put more emphasis on the fight against cybercrime.

38%

Cybercrime accounted for of economic crime incidents for Financial Services organisations.

3 As defined in our 2011 Global Economic Crime Survey (PwC in conjunction with our survey academic partner, Professor Peter Sommer.)

4 The Fourth National Conference on Financial Work held in Beijing, January 2012.

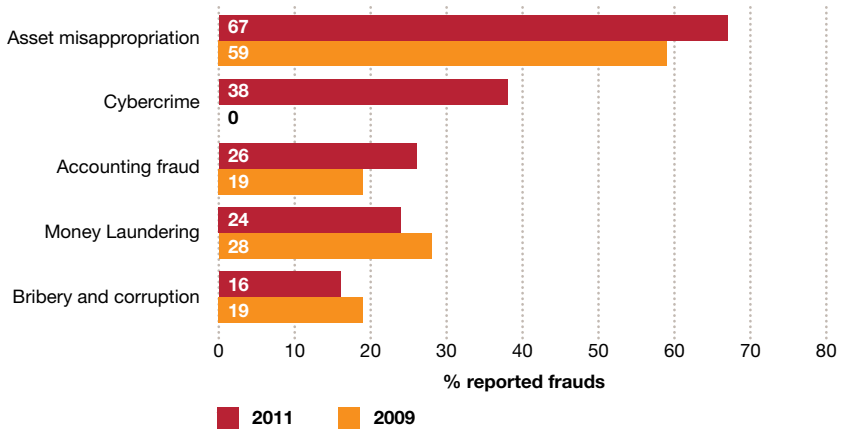
FS respondents reported cybercrime as the second most common type of economic crime experienced by their organisations in the last 12 months, after asset misappropriation (see figure 1). Cybercrime accounted for 38% of economic crime incidents for FS organisations, compared to 16% for other industries. This is not wholly surprising as the FS sector holds large volumes of the type of data cyber criminals are interested in and there is an established underground economy servicing the needs of the market for stolen and compromised data.

Whilst FS organisations have historically taken significant steps to control their customers' data (e.g. call centre protocols, disabling computer ports, two factor identification for internet access etc) they are nevertheless concerned about the growing threat. Half of FS respondents perceive the risk of cybercrime to have increased in the last 12 months, compared with 36% for other industries. Some of the developing technologies such as using 'Apps' to access banking services and mobile phones to make payments are likely to increase, rather than decrease these risks.

Where is the threat of cybercrime coming from?

FS respondents predominantly see cybercrime as an external threat, although historically FS organisations have reported that staff have been targeted by criminal gangs seeking data and that 'sleepers' have been placed by criminal gangs into organisations to gain access to data. The perception of cybercrime therefore continues to evolve and many organisations also recognise the threat of internal cybercrime.

Figure 1: Top 5 types of economic crime experienced in the last 12 months in the FS sector



FS respondents believe that the risk of cybercrime is lowest within the HR (13%) and legal departments (7%), which is consistent with our Global survey results (see the "Other Industries" column in figure 2). However, the sensitive information held within HR systems can be of interest to fraudsters as well as customer data. FS organisations should recognise that the internal threat can come from anywhere within the organisation and should not be considered as solely an IT risk.

FS organisations need to consider who is responsible for tackling cybercrime, assess where the growing and evolving threat is coming from and respond appropriately to any cybercrime incidents. They need to have a holistic and integrated response. Seeing this as an IT risk and not a financial crime risk is likely to lead to an inefficient and incomplete response to the risk.

Figure 2: Internal departments perceived to present the biggest cybercrime risk

Department	FS	Other industries
1. IT	63%	49%
2. Operations	47%	37%
3. Finance	39%	30%
4. Sales and Marketing	33%	34%
5. Physical/information security	31%	23%
6. Senior exec/board level	19%	16%
7. HR	13%	15%
8. Legal	7%	8%

What concerns do organisations have about cybercrime?

We asked organisations what aspects of cybercrime they were most concerned about. Figure 3 shows that FS respondents have a greater concern around all of the categories of collateral damage listed when compared to other industries. This is not unexpected given the higher risks within the FS sector. The greatest concern raised by FS respondents was around reputational damage, with more than half expressing concern. This is understandable given the impact that negative media can have on the perception of a brand.

How prepared are organisations in responding to incidents of cybercrime?

When a cybercrime incident occurs, the first few hours are crucial. It is particularly important to react quickly and decisively, as the consequences of not doing so can be severe in terms of both financial and non-financial damage.

We expected most FS organisations to have cybercrime incident response mechanisms in place. To our surprise, only 18% of FS respondents said that they had in place all five measures specified in our survey (see figure 4 for details on these measures).

It appears that some FS organisations are complacent about the risks that cybercrime poses, in spite of serious concerns about potential damage arising from cyber threats. However, our survey results highlight that the FS sector is slightly better placed when compared to other industries. Figure 4 shows that over half of FS respondents have a media and PR management plan in place, nearly two thirds have shut down procedures in place, and over two thirds have an in-house capability to prevent and detect cybercrime.

Figure 3: Collateral damage concerns

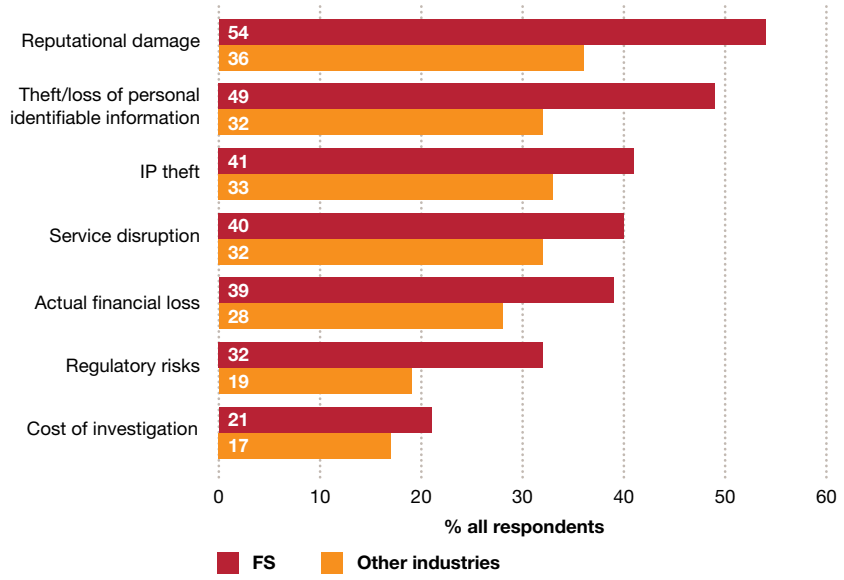
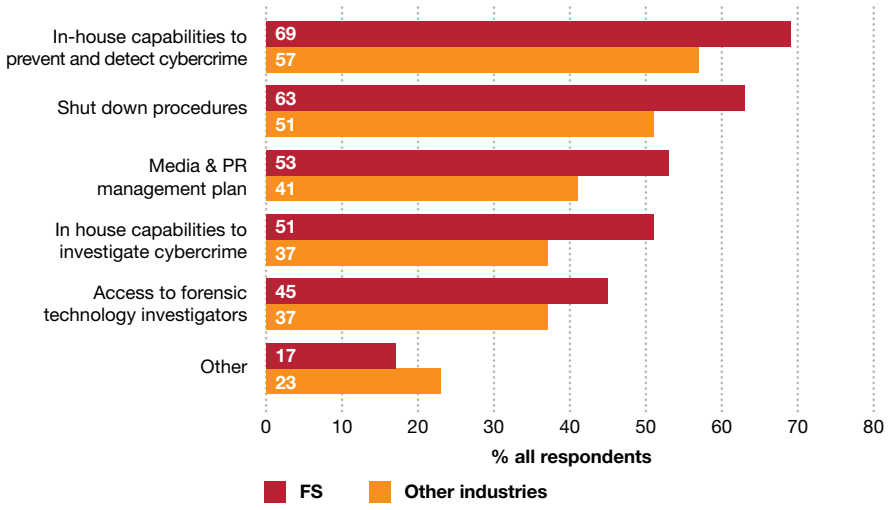


Figure 4: Cybercrime incident response mechanisms

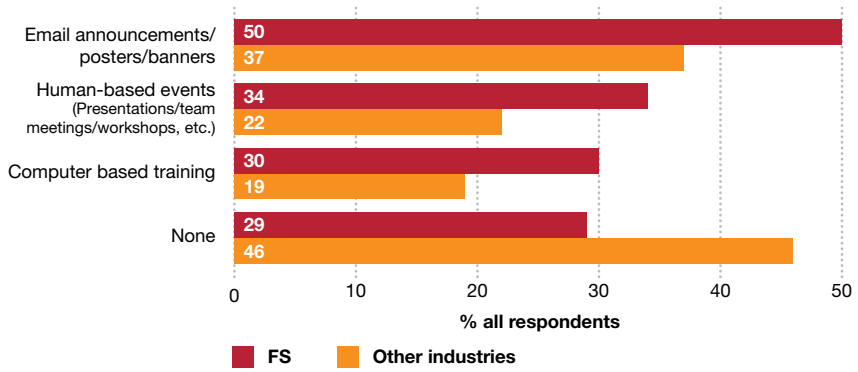


Who should be taking ownership for preventing cybercrime?

Our survey results show that FS respondents see cybercrime as predominantly an IT issue. This mirrors the results for other industries. In our view, overall responsibility for managing cybercrime risks rests with senior management. It is therefore essential that senior management understand the potential risks and opportunities that the cyber world can present and ensure that there is clear accountability and responsibility within the organisation for dealing with these risks and opportunities. It is also essential that the responsibilities go across business lines and operations so that cybercrime is seen as a holistic corporate responsibility and not just an 'IT' problem.

FS organisations have placed significant emphasis on cyber security related training and awareness programmes. Only 29% of FS respondents didn't receive cyber security training compared to 46% for other industries (see figure 5). This statistic is encouraging and suggests that FS organisations are being proactive. However, a lot more could be done. That nearly a third of staff in FS organisations have not received any cyber security related training is a significant concern. This is heightened by the ambiguity around the definition of cybercrime and general lack of clarity around responsibilities for managing cybercrime risks. It is important for FS organisations to ensure that staff and senior management understand cybercrime concerns and are equipped to tackle day-to-day cyber security as well as any crises.

Figure 5: Cyber security awareness training received



Fraud – avoiding complacency

The FS sector has always been a target for fraudsters. It continues to remain very attractive due to the significant amount of cash, assets and sensitive client data that is available to them as well as the nature of the industry. 45% of FS respondents suffered frauds in the last 12 months. This is a much higher figure compared to the fraud levels reported by other industries (30%). This may be because the FS industry has extensive controls for identifying external frauds perpetrated against it, as well as enhanced second and third line testing. This may also be due to having defined and extensive internal controls which mitigate the risks and assist in detection.

What are Financial Services organisations' experiences of economic crime?

Figure 1 (page 4) shows the top 5 types of economic crime experienced by FS respondents in the last 12 months. Asset misappropriation and accounting fraud continue to rise in the FS sector. As highlighted earlier in this report, cybercrime has emerged as the second most common type of economic crime reported.

The rise in accounting fraud from 19% in 2009 to 26% in 2011 differs to other industries where it fell significantly from 38% in 2009 to 22% in 2011. The decline could be explained by stricter controls being implemented by organisations, stricter penalties being faced by staff, and greater opportunities for fraud to go undetected and therefore unreported. The FS sector's increase in accounting fraud may be partly due to greater incentives for staff to hit targets, together with other factors such as personal pride in being seen as a success and meeting a myriad of stakeholders' expectations.

The Financial Services sector remains the fraudsters' target of choice.

Money laundering remains a significant economic crime for the FS sector at 24% (3% for other industries) and bribery and corruption remains in the top 5 types of economic crime for the FS sector at 16% (27% for other industries). Interestingly, both money laundering and bribery and corruption as types of reported economic crime have decreased slightly since our 2009 survey. This could be due to stronger preventative controls being in place.

FS organisations have historically needed to maintain strong systems and controls in order to prevent money laundering. Whilst the slight decline in money laundering and bribery and corruption could be attributed to organisations following regulatory requirements and implementing suitable systems and controls, it is clear that both types of economic crime remain significant risks for the FS sector.

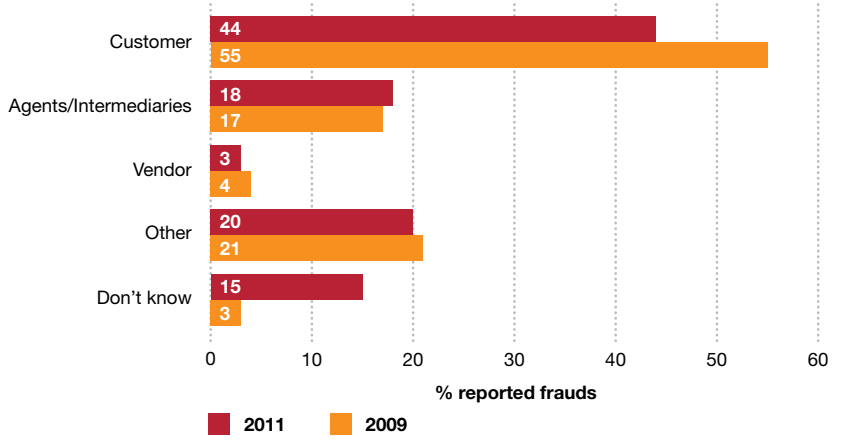
"The risks arising from any abuse of the financial system for money laundering purposes apply equally if criminals seek to embroil it in the financing of terrorism or in acts of fraud. It is therefore especially important that financial institutions do their utmost to combat and prevent such crimes" – BaFin, the German Financial Services regulator.

Should Anti-Bribery and Corruption be a key concern?

There is a general misconception that the FS sector has been less impacted by bribery and corruption. Our survey shows that this is not the case. Bribery and corruption is in the top 5 types of economic crime experienced in the last 12 months. The plethora of global bribery and corruption laws, including the US Foreign Corrupt Practices Act ("FCPA"), UK's Bribery Act and Canadian Corruption of Foreign Public Officials Act means that FS organisations need to consider how they could be impacted by bribery and corruption and how they can mitigate their risks.

Regulatory interest is increasing and there are likely to be more regulatory penalties for anti-bribery and corruption failings. Recent examples include FCPA settlements with Siemens (USD 800m) and Daimler (USD 185m), and two fines by the UK's FSA against Willis Limited (£7m) and Aon (£5m). However, it needs to be recognised that enforcement levels of bribery and corruption laws will vary by jurisdiction.

Figure 6: Main perpetrators of external fraud in last 12 months for FS organisations



Who's committing fraud?

The FS sector is typically seen to be targeted by external fraudsters and our survey results substantiate this. However, there has been a significant reduction from 71% to 60% in externally perpetrated frauds since our 2009 survey. This shift suggests that better controls may be in place or that different types of external fraud are not being detected.

There has been a 50% increase in senior management fraud in FS organisations (12% in 2009 to 18% in 2011). This suggests that the "tone at the top" and overall senior management attitude to fighting fraud is worsening, and presents an increasing challenge for Non Executive Board members. This could have a detrimental impact on an organisation's ongoing ability to prevent and detect fraud.

Figure 6 shows that the main perpetrators of external fraud over the last 12 months are still considered to be an organisation's customers (44%). This has fallen significantly since our 2009 survey (55%), with a corresponding rise in FS respondents stating 'other' or 'don't know'. This may be a result of the increase in cybercrime, where the crime is not usually perpetrated by the customer against the FS organisation, but rather by a criminal against the customer and the FS organisation. This could be either through account takeover, siphoning off money, or by stealing the customer's data and using it to impersonate the customer, or selling the data so that others may impersonate the customer. It also suggests that organisations might not be conducting thorough investigations to actually identify the perpetrators of fraud.

There has been a 50% increase in senior management fraud in FS organisations.

How do organisations detect economic crime?

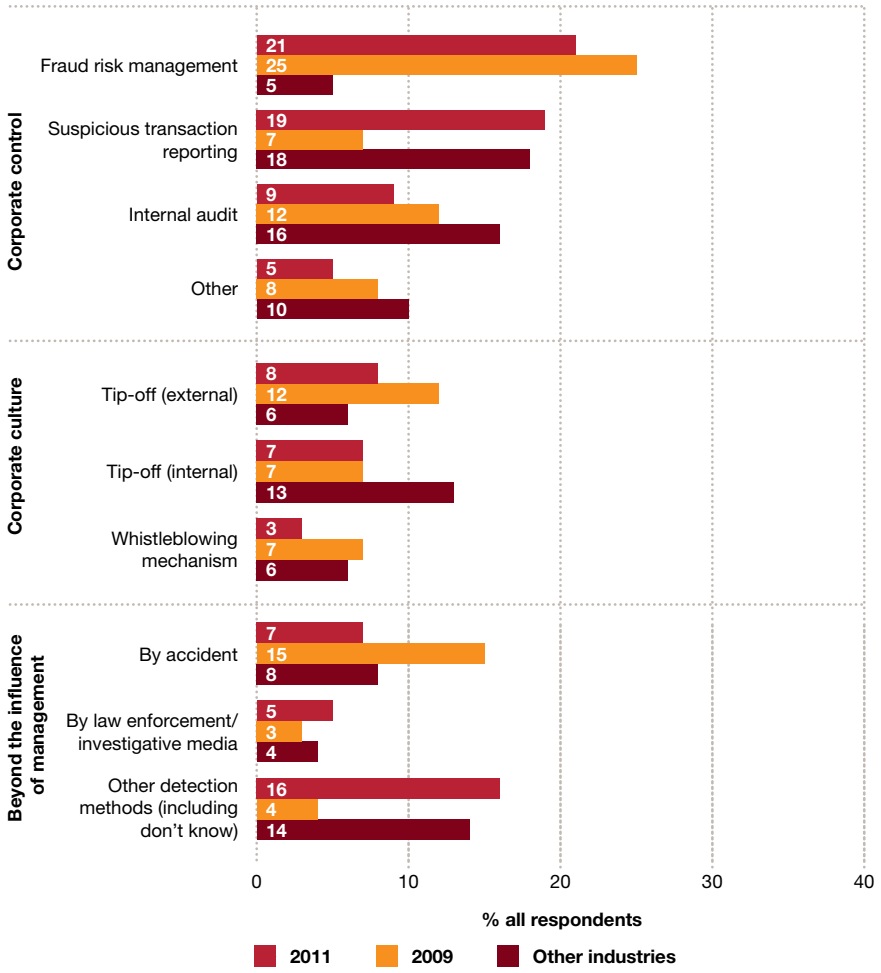
We have seen a correlation between the frequency of fraud risk assessments ("FRAs") and the extent of reported frauds across all industries. This indicates that organisations which perform FRAs at least once or more a year are able to detect more frauds and therefore report more economic crime. Our survey shows that the most effective detection method in the FS sector was fraud risk management. 21% of all frauds reported by FS respondents were detected by fraud risk management (see figure 7), of which FRAs are a key activity. This clearly shows the importance of FRAs in fighting fraud.

Our survey also shows that FS organisations have performed FRAs more often when compared with other industries. This could explain why the FS sector has reported higher levels of fraud (45% compared to 30% for other industries). One other possible reason for the high levels of fraud being reported by the FS sector is that a proper risk assessment process was in place during the last 12 months, which enabled more fraud to be detected. However, 1 in 5 FS respondents hadn't performed an FRA during the last 12 months. If they had done so we could have seen a much higher level of economic crime.

When asked why no FRA was performed, 36% of FS respondents weren't sure what a FRA actually involved (compared with 29% of other industry respondents). This lack of awareness is of real concern, particularly as the FS sector has traditionally been seen as stronger than other industries in carrying out FRAs. It is clear that a number of FS organisations need to raise their game when it comes to assessing and identifying the risks and costs associated with economic crime.

The second most effective detection method reported by FS respondents was suspicious transaction reporting, which has increased significantly as a detection method from 7% in 2009 to 19% in 2011. Whilst this is consistent with other industries it is a little surprising that the figures were so low in 2009. FS organisations have used suspicious transaction reporting for many years, primarily for money laundering reporting purposes. Reports are usually made to external authorities without knowing what actual crime has been committed and FS organisations tend to use the reporting framework to comply with regulatory reporting requirements. Organisations should invest in their systems and ensure that the parameters they set for detecting potential suspicious activity are appropriate. This will help ensure that staff resources are effectively utilised and results quickly analysed.

Figure 7: Detection methods of economic crime



"Recent statistics show that financial institutions are particularly vulnerable from within, when criminals use existing channels and systems to defraud these institutions, or use them to launder the proceeds of crime. Effective controls such as transaction monitoring can help institutions to protect themselves and their customers against such activities. However, this also places an obligation on regulators to ensure that the necessary controls have been put in place to limit these risks" – Murray Michell, Director of the South African Financial Intelligence Centre.

Is whistleblowing underrated as a detection method?

Figure 7 (page 9) shows that whistleblowing mechanisms have been generally ineffective in detecting economic crime. Some FS organisations dislike the term "whistleblowing" preferring to refer to a "Speak Up" procedure. We appreciate that there are sensitivities in this complex area but have used the term whistleblowing to cover all procedures of this type. Many FS organisations have whistleblowing mechanisms in place, but our survey results tell us that they have had limited success as a key detection mechanism and deterrent to fraud. Is this because:

- Whistleblowing procedures are in place but have not been made effective via training and awareness programmes?
- There is a "tone at the top" issue where senior management fail to show that they promote and respond to the use of whistleblower mechanisms?
- In the past a whistleblower's interests have not been protected, leading to a general lack of faith in the process?
- There is a cultural resistance to 'shopping' a work colleague?

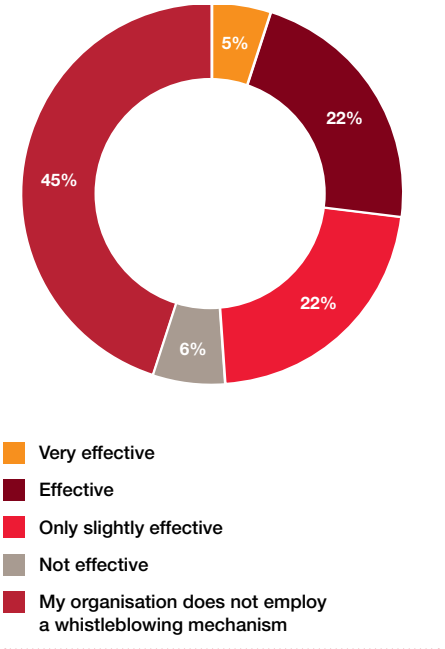
One of the surprising facts of our survey is that 45% of FS respondents stated that their organisation did not employ a whistleblowing mechanism and 28% of FS respondents said their whistleblowing mechanism was either not effective or only slightly effective (see figure 8).

There appears to be a lack of awareness amongst FS organisations in the potential effectiveness of whistleblowing mechanisms. Organisations could do a lot more in promoting, supporting and more effectively utilising them. This will need senior management commitment in order to be successful and reiterates the importance of having a strong "tone at the top" in the fight against economic crime. Even the best designed whistleblowing arrangements will not be effective unless they can be embedded within the wider culture of the organisation.

Whistleblowing mechanisms should be an important tool in detecting many types of economic crime. Attitudes to whistleblowing will vary significantly between countries; hence management of global FS organisations must not assume that "one size fits all". Five key milestones should be followed when developing an effective whistleblowing mechanism as follows:

1. Gaining top level commitment;
2. Developing a whistleblowing policy;
3. Designing whistleblowing reporting mechanisms;
4. Embedding a whistleblowing programme; and
5. Reporting, monitoring and evaluating the whistleblowing arrangements.

Figure 8: Effectiveness of a whistleblowing mechanism for FS organisations



Conclusion

The FS sector continues to be a hugely attractive target for fraudsters. Our survey shows that traditional types of economic crime remain prevalent, however, it is significant that cybercrime has become the second most common type of economic crime reported. FS organisations are very concerned about the reputational damage that could arise from a cybercrime incident, but could do a lot more in being prepared. With the rapid changes in the delivery of banking and other financial services and the ever increasing reliance on technology for the delivery of those services, cyber security and cybercrime are risks that cannot be ignored. Having cyber security effectively embedded in your routine procedures and a cyber crisis response plan in place is vital.

Whistleblowing appears underused as a detection method, which may be symptomatic of a wider "tone at the top" issue. The support and promotion of whistleblowing mechanisms must increase. This will also provide senior management with an opportunity to demonstrate their overall dedication to the fight against economic crime.

FS organisations should consider the following 5 ways to protect their organisation against economic crime:

1. Ensure that cyber security is embedded into the business and that the risks are fully defined and understood, and the impact of changing technologies in the market place are fully addressed and planned for.
2. Ensure there is a fully defined cyber crisis response plan to protect against financial and non-financial loss and to mitigate the reputational risks associated with an incident.
3. Ensure that senior management proactively take the lead in the fight against economic crime.
4. Conduct more regular fraud risk assessments to identify ever changing economic crime risks.
5. Promote and support the embedding of whistleblowing mechanisms.

Senior management must be proactive in taking the lead in the fight against economic crime. The rapidly changing market place and delivery mechanisms, as well as the global regulatory environment and tougher enforcement actions makes this essential. Senior management need to focus on both preventative and detective economic crime controls. They should ensure that fraud risk assessments regularly take place and that the approach taken addresses the risks. Making sure that there is a holistic approach across the FS organisation that is fully embedded and operating in business as usual processes is key. Economic crime and cyber security are not just a compliance or IT issue but are an important business issue that must be addressed.

For those interested in the detailed methodology used in our survey, or the Global results, these can be found at: www.pwc.com/crimesurvey

Contacts

If you would like to find out more about the information contained within this report, or to discuss any issues around economic crime and how our team can help you, please contact us:

Andrew P Clark
Partner, Europe, Middle East & Africa
+44 (0) 20 7804 5761
andrew.p.clark@uk.pwc.com

Christopher Cowin
Survey Project Manager, UK
+44 (0) 20 7212 6185
christopher.b.cowin@uk.pwc.com

Steve Ingram
Partner, Asia Pacific
+61 (3) 8603 3676
steve.ingram@au.pwc.com

Jeff Lavine
Partner, Americas
+1 (703) 918 1379
jeff.lavine@us.pwc.com

Forensic Services

The PwC forensic services network is comprised of forensic accountants, economists, statisticians, former regulators and law enforcement, fraud examiners, and forensic technologists. We help organisations tackle the major financial and reputational risks associated with economic crime. We identify financial irregularities, analyse complex business issues, and mitigate the future risk of fraud.

Design & Media – The Studio 21050 (03/12)