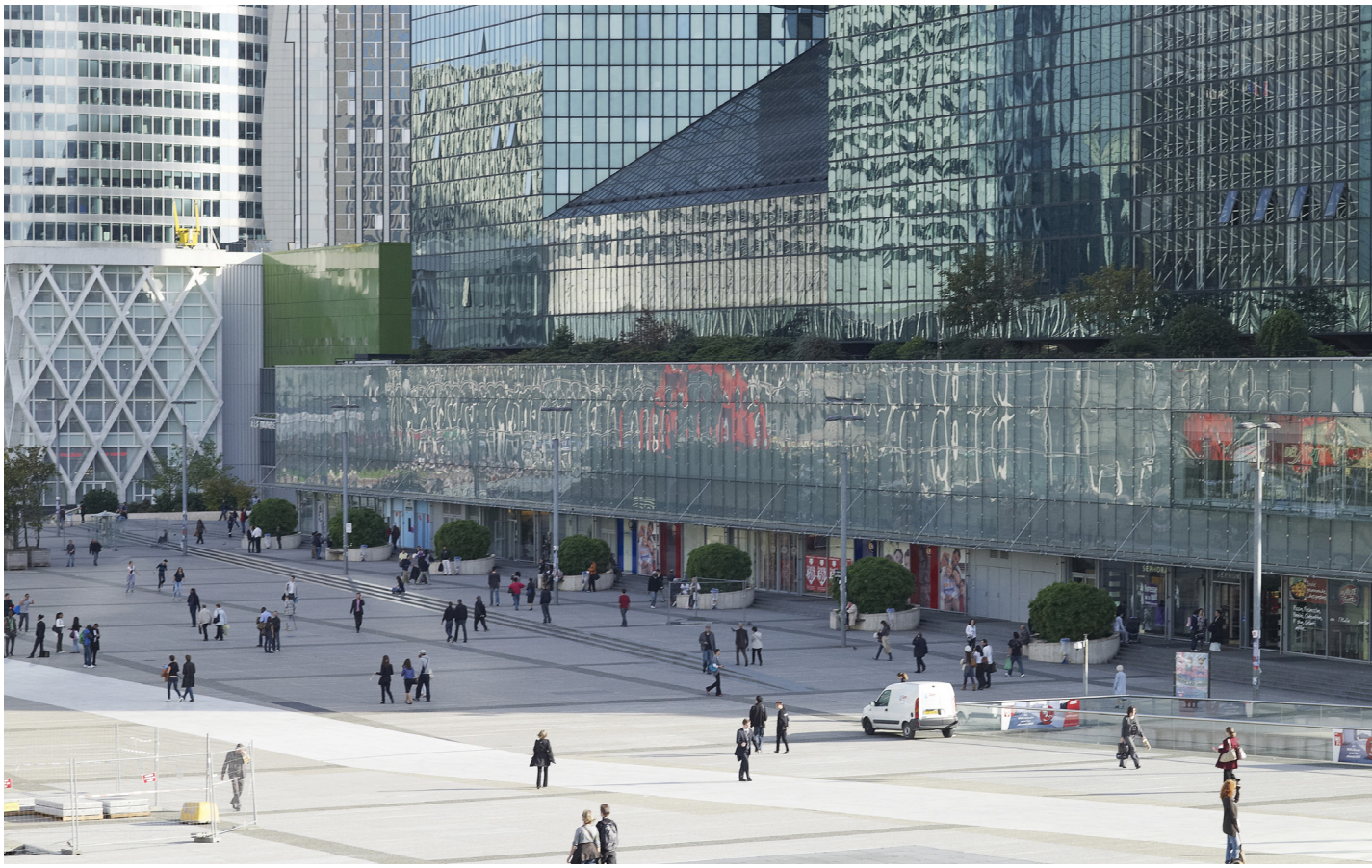
Financial Services sector analysis of PwC's 2014 Global Economic Crime Survey

Threats to the Financial Services sector



pwc

www.pwc.com/crimesurvey

Contents

Key highlights
FS sector survey responses

An attractive target… 45% have suffered economic crime during the survey period compared to only 34% across all other industries.

More than one way to lose… The sector remains a key target for criminals and asset misappropriation is still the primary type of reported economic crime. Cybercrime, bribery and corruption appear to be increasingly common in the sector.

Tone from the top… 1 in 5 internally-perpetrated frauds still involve senior management, though the majority of such fraud tends to be committed by junior staff or middle management.

Delusions of security… Cybercrime risk appears to be increasing – however, risk awareness can differ greatly depending on an individual's role and function.

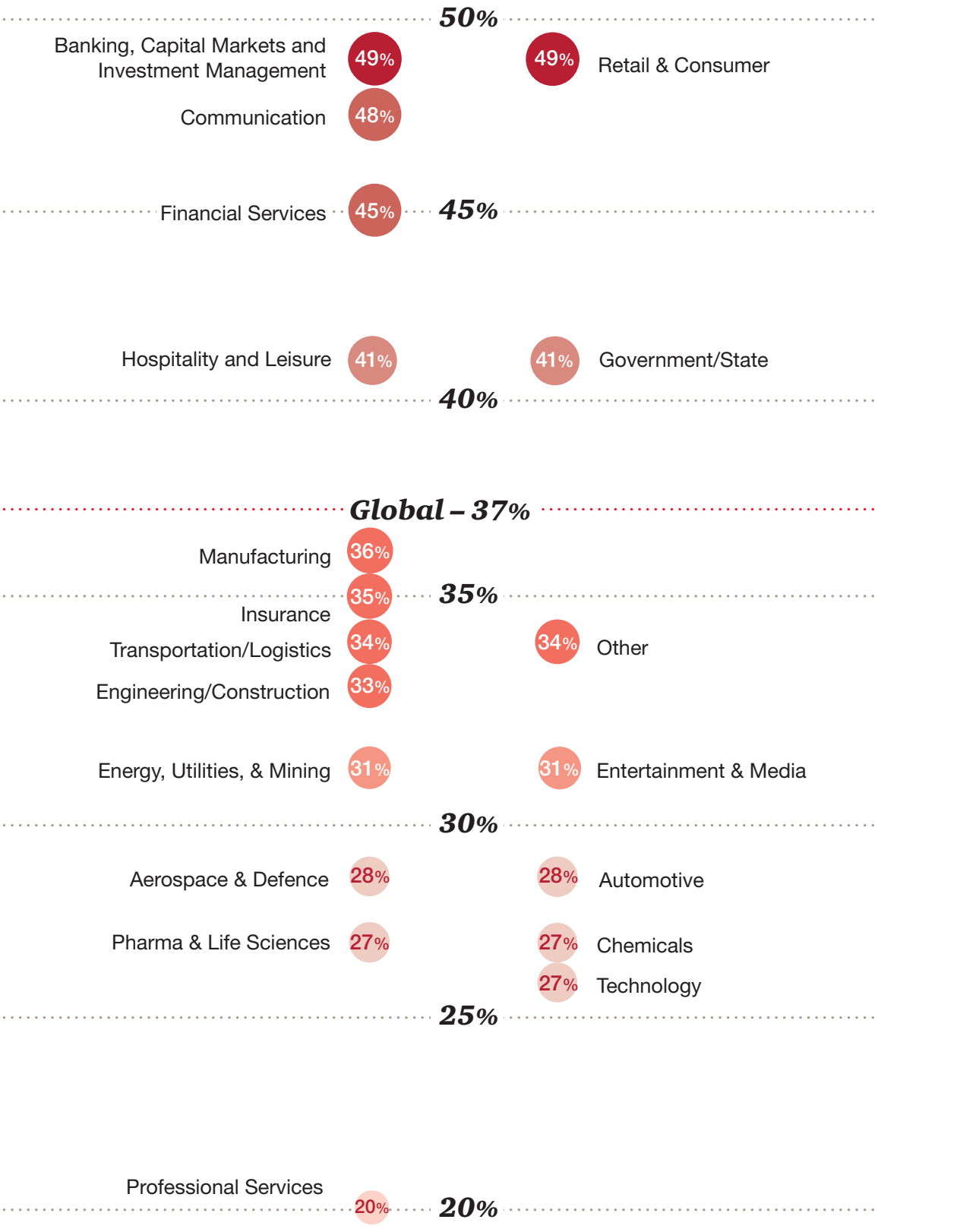
Where the money's at… Money laundering remains a hot topic in the FS sector, where it is almost five times more likely to occur than in other industries.

Named and shamed… FS organisations fear the fallout of being caught up in money laundering – almost 30% believed that the most severe impact is reputational.

Telling… Whistleblowing mechanisms appear to be more prevalent than before, however doubts remain over their effectiveness.

Underestimating the risk… 1 in 4 FS respondents failed to conduct annual fraud risk assessments. Over half of those who have not conducted any at all during the survey period are unaware of what these assessments involve or fail to see value in them.

Fig 1 Economic crime percentage reported by industry



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

The rate of economic crime reported by FS respondents is exceeded only by that in the Retail & Consumer and Communications sectors. Note that the proportion of Insurance-specific respondents who reported economic crime in our survey is lower than that of other Financial Services respondents – this is not unexpected given that other FS organisations such as banks are perceived to be where the money is and therefore more attractive for fraudsters.

Introduction

45% of Financial Services organisations have suffered economic crime during the survey period, compared to only 34% across all other industries.

The Financial Services ("FS")[1] sector results from PwC's seventh Global Economic Crime Survey are the most comprehensive and intriguing to date.

There were 1,330 responses from the FS sector alone – 26% of the 5,128 responses received from all sectors.[2] FS respondents hailed from 79 different countries – making this FS sector report truly global[3] and representative of views on economic crime in its many guises, from fraud and cybercrime to money laundering and bribery and corruption.

Our survey questions were designed to assess corporate attitudes to economic crime in the current economic environment, the types of fraud encountered during the survey period, whether cybercrime is becoming more prevalent, and the extent of bribery andcorruption, money laundering and anti-competition experienced.

The FS sector results are intriguing because they often depart from the trends observed in other industries' results. In some areas they also continue to defy what might be expected of a sector that is heavily scrutinised and regulated globally. In this report, we shine the spotlight on the correlation between economic crime, corporate culture and individual behaviour in the FS sector and explain how the FS sector results demonstrate that many FS organisations need to improve their understanding of integrity and conduct risk threats.

The key message from our survey results is this: whilst the FS sector may be ahead of many industries in terms of prevention and detection of economic crime, more can and should be done by FS organisations. Of particular concern are the clear weaknesses in some organisations' fraud risk assessments, whistleblowing (or equivalent 'Speak up/Speak out') mechanisms and awareness of the pervasive and sustained threat of cybercrime.

Our survey findings are accompanied by action points for FS organisations if they wish to achieve or sustain 'best in class' practice.

1 Financial Services: Including retail and investment banking, insurance, investment management, stockbroking and private equity. The survey allowed respondents to identify as being from the "Insurance" sector separately from the "Financial Services" sector (as seen in Fig. 1). For this report, 'Financial Services' or FS shall refer to the combination of these respondents.

2 This compares to 3,877 responses in the 2011 survey – of which 878 (23%) were from the FS sector.

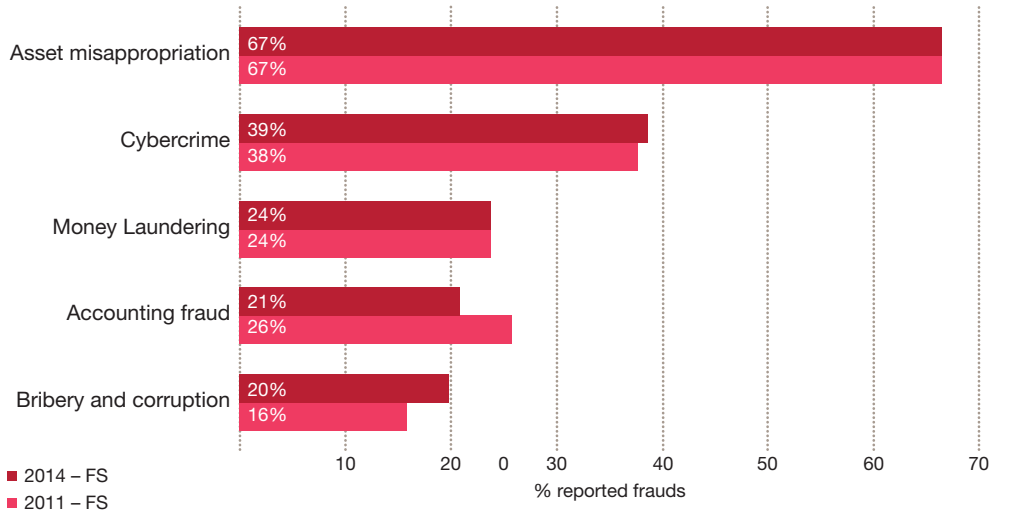
3 There were 79 countries represented in the FS sector responses – a significant (nearly 41%) increase from 56 countries in the 2011 survey.

Section 1 – FS economic crime today
Occurrences and value

Around half of the FS respondents who have experienced economic crime during the survey period report an increase in the number of occurrences and the financial value of economic crime during the period (more so than other industries' respondents). There are regional variations – in Asia Pacific at least half of FS respondents reported an increase; in contrast, nearly 40% of FS respondents from South & Central America reported a decrease.

The key threats

Fig 2: Top 5 types of economic crime experienced by the FS sector during the survey period



Asset misappropriation remains the primary type of economic crime reported by FS organisations (67%) – not unexpected for a sector which processes money, and given the low cost of conversion for fraudsters. This is followed by cybercrime which is becoming more common, as is bribery and corruption. Only 1 in 5 experienced accounting fraud (compared to 1 in 4 previously) – we believe this is explained by improvements in corporate controls.[4]

Definitions of fraud vary, but mostly relate to obtaining financial or personal gain through wrongful deception. The key threats to the FS sector within the broad spectrum of economic crime range from more 'conventional' fraud (e.g. asset misappropriation) to money laundering by third parties.

4 Corporate controls: the suite of activities such as internal audit, fraud risk management, rotation of personnel and physical and IT security procedures undertaken in an organisation to monitor and address risks

Internal vs External

External fraudsters are still the main perpetrators of economic crime for the majority of FS organisations (57% in 2014 and 60% in 2011).

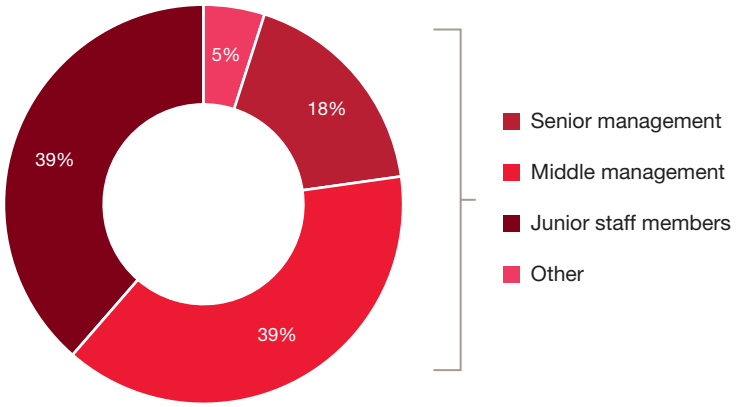
FS organisations are prime targets for external fraud given the amount of money fraudsters could potentially obtain and also the importance and sensitivity of data held by organisations (e.g. credit card and personal identity details). We note – and our FS respondents expect – that cybercrime is most often externally perpetrated and not just for monetary gain but also for valuable information about individuals. For instance, insurers may hold sensitive information and high-profile individuals' security details.

The FS sector also tends to be more strictly regulated and as a result many business processes and functions have corporate controls in place. This makes it more difficult for frauds to be internally perpetrated without discovery. To illustrate this – of the FS respondents who knew how the economic crime in their organisation had been detected, 61% attributed the detection to corporate controls in place compared to 56% in other industries.

Rank and profile

After the economic downturn began in 2008, we saw in previous survey results that the involvement of senior management (whose primary motivation when committing fraud may be to alter performance and stock prices for their own bonus and other benefits) in FS economic crime increased by 50% from 12% in 2009 to 18% in 2011. The involvement of senior management remained at the same levels in 2014 (18%), suggesting that the response by regulators and governments to the financial crisis of imposing more rules and regulations has not sufficiently managed integrity or conduct risk i.e. the risk that people are not doing the right thing when no one is looking.

Fig 3: Seniority of internal fraudsters in FS



That said, most FS internal frauds are still committed by junior staff and middle management. In other industries, 64% of internal frauds are committed by middle or senior management, compared to 57% in the FS sector. Internal fraudsters in FS are also more likely to hold at least a university degree qualification than in other sectors, a reflection of the entry requirements of recruitment in the sector.

Our survey results suggest that the average FS internal fraudster is able to carry out fraud from quite a junior level in the organisation. This may be due to the fact that FS products are on the whole more complex by design and function, and consequently more difficult to 'police' (despite the corporate controls and monitoring in place).

Rather than accept these finding as 'status quo', FS organisations should explore what it means for their approach to fighting fraud:

- Is there sufficient emphasis on personal integrity and ethical behaviour?
- Are employees routinely encouraged to advance corporate and personal gain without regard to the impact of their behaviour on others?
- Is there evidence of how policies and procedures are actually deployed in day-to-day operations?
- Are ethical behaviours celebrated and poor behaviours penalised in a consistent, open and transparent way?
- Are employees encouraged to question the behaviour of others or ask questions in an open forum?

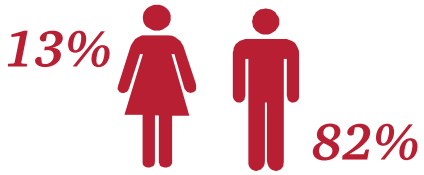
The sector is known for emphasising processes, rules and compliance – yet all too often, conformity can lead to wrongdoing if employees lack the training, incentives and support to question it.

Workforce diversity

FS respondents reported that the typical internal fraudster is likely to bebetween 31-50 years old.

When asked about the most significant internal fraud experienced during the survey period, FS respondents reported that 82% were perpetrated by male fraudsters (an increase from 75% in 2011). The proportion perpetrated by female internal fraudsters has dropped (from 20% to 13%) in contrast to other industries which reported no material change in the proportion of internal frauds perpetrated by females. The remaining 5% of FS respondents did not confirm the gender of the fraudster.

Some studies on female representation suggest that the number of women in FS is in decline. The FS sector is less diverse than some other industries in terms of gender representation, and we see that reflected to some extent in the profile of the average internal fraudster.



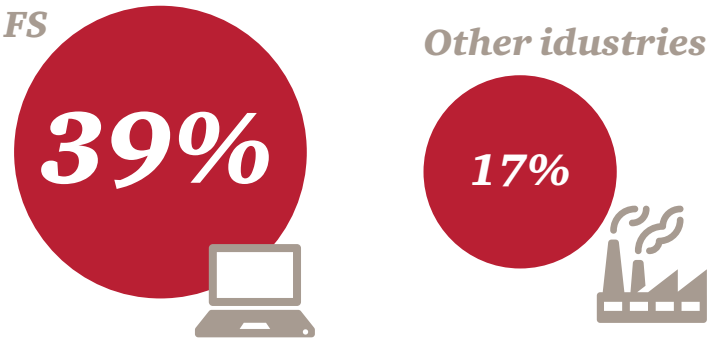
What can you do?

- Define the organisation's strategic aspiration for ethical business conduct – ensure that a clear vision is set and that it is effectively communicated to all in the organisation.
- Assess the organisation's current integrity risk exposure (e.g. by conducting a gap analysis for misalignment between intended, expressed and actual behaviour) and define the risk tolerance level.
- Identify and address the drivers of undesirable behaviours within the organisation. For instance, review the organisation's recruitment policy and 'ethos', communication round risk and reward and other behavioural triggers.

Section 2 – Cybercrime
Not just an IT risk

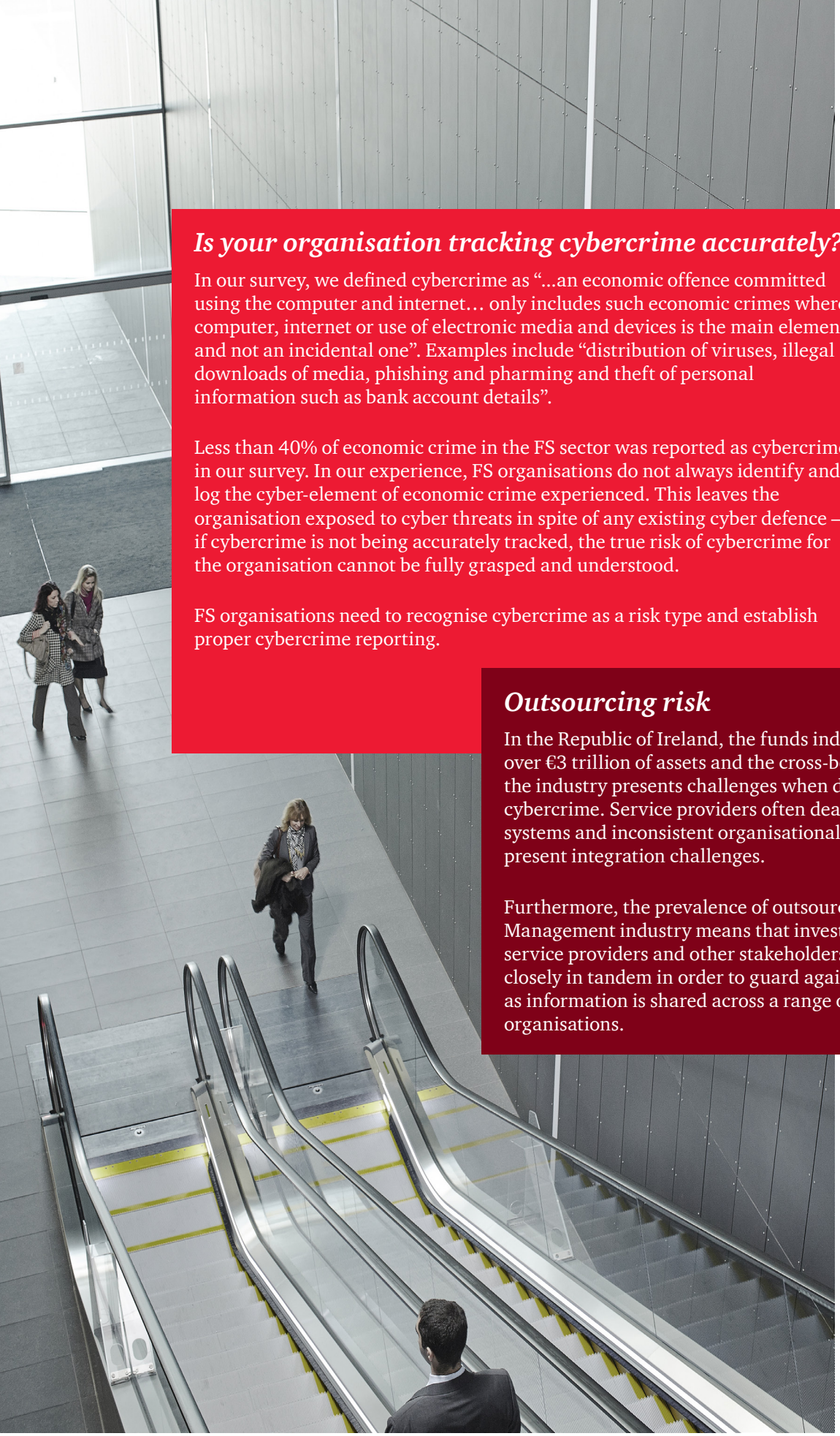
The FS sector was one of the first to be targeted by cybercrime – little wonder, as there have always been significant potential financial gains to be had from subverting computerised processes and corporate controls in banks.

Our survey shows that cybercrime is still the second most common type of economic crime reported by FS respondents (after asset misappropriation) – 38% in 2011 vs 39% in 2014 (this compares to only 16% in 2011 vs 17% in 2014 in other industries). However, we view this percentage of respondents as alarmingly low – our experience has shown that a clear majority of FS organisations (especially retail banks) suffered cybercrime during the survey period.



Similarly, only 41% of FS respondents believe it is likely that they will experience cybercrime in the next 24 months (including some 45% in Africa and36 % in Asia Pacific). This compares to 26% in other industries. A further 19% of FS respondents are unsure whether they are likely or unlikely to experience cybercrime.

FS respondents perceive a greater increase in the risk of cybercrime compared to counterparts in other industries (57% in FS vs 45% in other industries). In 2011, only half of FS respondents felt that the risk was increasing. Clearly, FS organisations believe that cybercrime is becoming a greater threat than ever before, and yet many do not believe that it will actually happen to them.



Is your organisation tracking cybercrime accurately?

In our survey, we defined cybercrime as "...an economic offence committed using the computer and internet… only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one". Examples include "distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details".

Less than 40% of economic crime in the FS sector was reported as cybercrime in our survey. In our experience, FS organisations do not always identify and log the cyber-element of economic crime experienced. This leaves the organisation exposed to cyber threats in spite of any existing cyber defence – if cybercrime is not being accurately tracked, the true risk of cybercrime for the organisation cannot be fully grasped and understood.

FS organisations need to recognise cybercrime as a risk type and establish proper cybercrime reporting.

Outsourcing risk

In the Republic of Ireland, the funds industry services over €3 trillion of assets and the cross-border nature of the industry presents challenges when dealing with cybercrime. Service providers often deal with multiple IT systems and inconsistent organisational processes, which present integration challenges.

Furthermore, the prevalence of outsourcing in the Asset Management industry means that investment managers, service providers and other stakeholders must work closely in tandem in order to guard against cybercrime, as information is shared across a range of systems and organisations.

Old tricks, new methods

On one hand, certain cyber threats do ebb and flow – for instance, the Middle Eastern cyber attacks that targeted several large U.S. banks in 2012/13 appear to have receded. Overall some 5% of FS respondents said that their risk perception (of cybercrime) had decreased, and this could be due to the cessation of such previous high-profile incidents.

On the other hand, cybercrime is growing and the methods are constantly evolving – we see no abatement in attacks on banks' infrastructure. Some recent attacks have installed hardware in bank branch systems to enable transactions to be manipulated via mobile networks. The U.S. has seen dramatic increases in FS economic crime – from outages created by Distributed Denial of Service (DDOS) attacks to massive ATM withdrawals effected by organised criminal groups. Credit card fraud has become more pervasive as the U.S. has yet to embrace the Chip and PIN system. In Japan, phishing scams have targeted bank customers' personal computers via virus, using fake pop-up windows or e-mails masquerading as legitimate internet banking interfaces to trick customers into inputting their personal information.

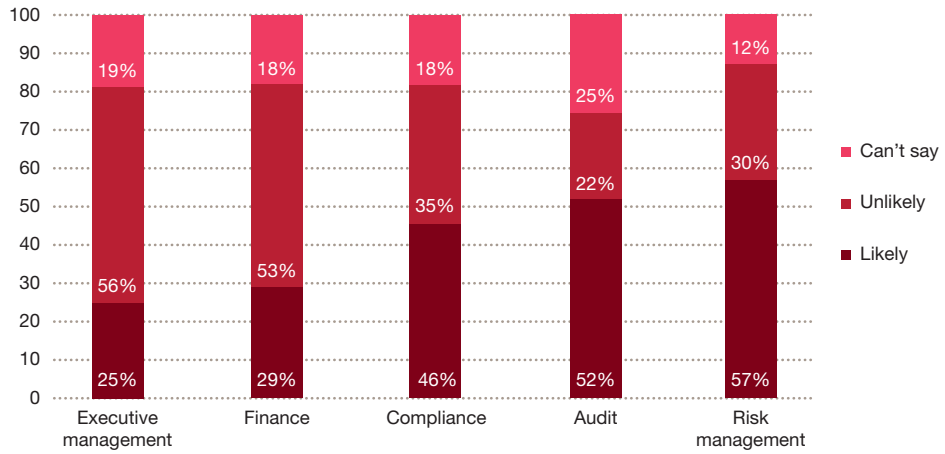
The landscape of cybercrime is also changing in a literal sense. For instance, our cybersecurity experts have perceived a rise in cybercrime from Africa, which correlates with big government initiatives to roll out broadband in that region. Industry sources also indicate that cybercriminals are relocating to South Africa from Europe (due to increased co-operation between law enforcement agencies in the EU).

Varying awareness of cybercrime

It is concerning that 40%of all FS respondents believe that it is unlikely their organisations will experience cybercrime in the next 24 months. When we delved into the responses by respondent roles, an alarming 54% of CEO (or equivalent) and 49% of CFO (or equivalent) respondents declared that it is unlikely. 1 in 5 CEOs were unable to conclude whether it was likely or unlikely. And yet, cyber insecurity is seen as a key threat by CEOs – results from PwC's 17th Global CEO Survey show that more than 70% of Banking & Capital Markets CEOs see cyber insecurity as a threat to growth, more than any other sector.

There is a stark disconnect in the perception of cybercrime risk within FS organisations.FS respondents from the internal audit, compliance and risk functions thought it was more likely than unlikely that their organisations would experience cybercrime whilst the opposite was true for finance and executive management FS respondents.

Fig 4: "Is your FS organisation likely to experience cybercrime in the next 2 years?"



Clearly there is a mix of views amongst C-suite respondents, with CEOs and CFOs on the whole appearing less aware of the likelihood of cybercrime occurring in their organisation. It may be that within some FS organisations, cybercrime has not been materially reported to C-suite attention.

While the more risk-focussed functions like internal audit, compliance and risk management show greater awareness of the risk, a worrying percentage of respondents from those functions still conclude that cybercrime is unlikely.

It is widely recognised that the FS sector is very much at the forefront of fighting cybercrime. However, our survey results suggest that complacency still exists heavily within FS organisations – perhaps management feel comfortable that their organisations have better cybersecurity defences than ever before, without realising that threats are usually one step ahead. Or perhaps certain functions (including finance) still tend to perceive cybersecurity as more of an IT issue (rather than a significant business risk).

> ***"Today's incidents, yesterday's strategies – As the digital channel in financial services continues to evolve, cybersecurity has become a business risk, rather than simply a technical risk"***
>
> The Global State of Information Security® Survey (an annual, worldwide study by PwC, CIO magazine, and CSO magazine)

FS respondents should be aware that their organisations are increasingly likely to suffer cyber attacks regardless of whether proper defences are in place. When the findings above are linked up with survey results around fraud risk assessment (see further below), there is a sense that FS organisations still fail to see the importance of establishing fundamental IT security objectives and linking those with business objectives and risks.

Regulators fight back

Meanwhile, regulators around the world are waking up to the fact that cybercrime poses systemic danger, especially when retail and commercial banks are concerned. FS organisations are custodians of monetary assets and sensitive information for companies and individuals in other industries, meaning the effects of cybercrime in the FS sector are seldom contained to FS organisations alone.

Regulatory pressure on cyber threats

In the UK, the Bank of England has declared cybercrime a major risk to the FS sector and, along with other FS regulators in the UK, co-ordinated a major cyber attack in November 2013 to 'stress test' UK banks in an exercise known as 'Waking Shark II'. The Bank's report on this exercise cited a need both for greater co-ordination within the sector and for educating firms about the need to report major incidents to regulators. In the same month, the New York State Department announced that it would require the banks under its regulation to answer questions in a real-time online test in order to assess their cybersecurity policies and processes.

Additionally in the U.S., regulators have increased the visibility of cybercrime by requiring cyber incidents which have had material impact to be disclosed in registered public company filings. Several large FS organisations have thus been prompted to disclose within their 10K filings with the SEC that they have been targeted by cyber attacks.

Even in Lebanon, where online banking activities are less developed and banks therefore do not perceive the cybercrime risk as material, significant losses from cybercrime in the FS sector have emerged. The Banking Control Commission of Lebanon has initiated reviews of IT security in banks with a view to strengthening cyber defences.

Knowledge is power – FS organisations have been co-ordinating to share threat intelligence for years. Collaborating to share cyber threat data helps organisations deal quickly and proactively with cybercrime. In Luxembourg, where the FS sector is dominant, such collaboration is of strategic importance to the economy at large.

The largest FS organisations are also catching on to the need to deter (rather than just detect) cybercrime. At least one large global bank has established a zero-tolerance policy to combat all online banking fraud, regardless of materiality.

What can you do?

- Educate employees at all levels (from C-suite to junior management) about cyber threats – cybercrime is not just the domain of the IT/network security function. There are different types of cybercrime, from hacktivism to data theft, which affect different functions of the bank in varying ways.
- Understand the potential culprits and their motivations to engage in a cyber attack on the organisation.
- Ensure that key fundamental safeguards for effective cyber security are in place – including ongoing monitoring, up-to-date personal or sensitive data inventory, a back-up policy and business continuity plans.
- Continue to engage with regulators to understand what other peer organisations are doing to counter cybercrime and adopt 'best in class' practices.
- Separate out the gross and net financial loss due to cybercrime for the FS organisation and report to executive management as meaningful indicators of activity and recovery levels.

Section 3 – Fraud
More than one way to lose

The FS sector is particularly exposed to certain types of economic crime (such as money laundering) and faces unique regulatory challenges as a result.

Money laundering

Money laundering continues to be a hot topic in the FS sector. It is also distinct from other types of economic crime in that an FS organisation does not suffer direct financial loss through money laundering – instead, the effects are felt through a loss of reputation (in the eyes of both the public and the regulator), and increasingly compounded by colossal regulatory fines. At least 50% of FS respondents in Western Europe and Africa selected money laundering as their highest risk in doing business globally, compared to bribery andcorruption and anti-competition law.

Our survey showed that money laundering ranked next behind asset misappropriation and cybercrime in the types of economic crime experienced by FS organisations. It is almost five times as likely to occur in the FS sector compared to other industries.

FS organisations reported feeling particularly concerned about the impact of money laundering on their reputation (more so than operational disruptions or financial loss). Their focus on corporate reputation is in line with expectations given that many banks have had adverse press coverage regarding their Anti-Money Laundering ("AML") breaches.

of FS respondents felt that the most severe impact of money laundering is on their organisation's reputation

In the past few years, enforcement action across the globe has crystallised regulatory expectations in the AML space. The challenge for global FS organisations is how best to utilise Know Your Customer (KYC) information across the organisation, particularly in relation to customers that have multiple touch points with the organisation across more than one business unit and several jurisdictions. Regulators have made it clear that they expect institutions to have a consolidated picture of the client relationship, regardless of limitations presented by legacy IT systems and complexities of cross-border data privacy legislation.

There is a growing realisation that FS organisations need to invest in AML technologies in order to ensure they are operating as expected. The Financial Action Task Force (the inter-governmental body which sets AML standards) has recently indicated that its focus is shifting away from whether FS organisations can demonstrate compliance with AML requirements, to whether the AML arrangements in place are actually effective.

AML on the back foot

Many banks continue to struggle with AML remediation due to the size and complexity of their operations and customer base. Regulatory authorities – including central banks from Ireland to Israel – continue to push for greater accountability, creating challenges ahead.

Regulators ranging from the UK's Financial Conduct Authority ("FCA") to Malaysia's Bank Negara Malaysia have recently published thematic reviews on financial institutions' AML systems and controls. The FCA's thematic review TR13/9 for Asset Management and Platform Firms sets out examples of 'good' and 'poor' practice, and also made the following comment on senior management oversight:

"We identified examples of recurring issues being reported to management committees, with no clear ownership for the closure and resolution of those issues, leading to a 'reactive' approach in managing money laundering and bribery and corruption risks. Some firms' senior management could not clearly articulate their money laundering and bribery and corruption risk management arrangements."

In South Africa, financial intelligence units were first established in the 1980s to identify and combat the laundering of illegal drug trade proceeds. Today, a much broader effort is under way – the Financial Intelligence Centre (FIC) monitors activity by globalised criminal syndicates operating in and through the country, large scale corruption and the influence of Politically Exposed Persons in the private sector, amongst other things. The FIC is increasingly confronted with the challenge of "big data" analysis and will need further investment in technology systems capable of handling massive data volumes and analytical functions.

What can you do?

- Ensure that 'Know Your Customer' (KYC) procedures and Anti-Money Laundering processes are operating effectively across a 'single customer view' – making sure all relevant systems and records are joined up for consistency of data.
- Resolve legacy IT issues in order to keep pace with regulatory requirements and new tactics of money laundering syndicates.

Dealing with bribery and corruption abroad

Of the FS organisations surveyed, 47% currently have operations in a market with high corruption risk.[5] At the same time, for each associated economic crime like bribery and corruption, money laundering and anti-competition law, around 40% of FS respondents were unable to provide an estimate of the financial loss suffered as a result.

Our survey results show that such risks remain hard to quantify in terms of financial loss. The results also indicate that FS organisations have not fully come to grips with the risks of operating in such territories. Regulators continue to take a strict view on money laundering, bribery and corruption – focusing on the corporate as well as the individual. In the UK, the Bribery Act emphasises personal liability ofboard members, while the 2013 Financial Services Act places the burden of proof on the individual (to demonstrate that reasonable steps have been taken to avoid bribery and corruption).

A number of forward-thinking FS organisations are seeking to get ahead of the pack.

We recently worked with a global investment bank and with the cooperation of several peer organisations (competitors) sought to benchmark their anti-bribery, corruption and fraud management. This gave the FS organisation an external, objective view of their organisational structure and how roles, resources and areas of responsibility were geared towards dealing with such risks and incidents.

FS organisations need to remain wary of who they are "getting into bed with" in emerging markets. In June 2013, the U.S. Department of Justice announced that it had arrested the managing partner of a U.S. broker-dealer on felony charges arising from a conspiracy to pay bribes to a senior official in a South American state-owned economic development bank. More recently, certain global banks have come under investigation from UK and U.S. regulators for potential bribery and corruption due to their practice of making high-profile government-linked hires in Asia. While such occurrences are common among local entities, many foreign regulators may have a different view on such matters. It is far better for FS organisations to take a circumspect and informed approach to operating in emerging markets than to fall foul of regulators after the event – especially as recent regulatory releases and press reports seem to suggest that the FS sector is beginning to experience increased regulatory scrutiny with regards to the U.S. Foreign Corrupt Practices Act (FCPA) and other similar areas of compliance.

What can you do?

- Carry out risk assessments for fraud, bribery and corruption in order to identify ways of improving the effectiveness of fraud detection mechanisms as well as to mitigate the risk of regulatory breach when operating in a territory with heightened corruption risk.
- Implement comprehensive due diligence programmes on third parties which would help to highlight potential "red flags" indicating vulnerability to bribery or corruption. These red flags may include issues such as engagement with Politically Exposed Persons, negative references in media or involvement in litigation.

5 Territory with high corruption risk is defined as one with a 2012 CPI score below 50 http://www.transparency.org/cpi2012/results

Whistleblowing – improving but underused and underrated

Whistleblowing mechanisms remain underused in the FS sector. We attribute this in part to the greater dependencies placed on process-type detection methods in the industry – which may encourage complacency and diminish the perceived need for personal integrity and responsibility to come to the fore.Alternatively, it could be because whistleblowing does tend to be a 'last resort' option for employees to report concerns and issues.

Our survey shows significant improvement in some areas – only 19% of the FS respondents confirmed a complete lack of whistleblowing mechanism in place at their organisations (compared to 45% of the FS sector in 2011). Of those who do have a whistleblowing mechanism in place, over 1 in 2 (53%) reported effective or very effective whistleblowing mechanisms according to respondents – compared to 27% in 2011. However, doubts over the effectiveness of whistleblowing policies still remain – 16% still don't know whether their whistleblowing mechanism is effective or not. And a further 7% of FS respondents believe it is ineffective – including 10% from Western Europe and 6% from Asia Pacific and Africa.

In fact, tip-offs and whistleblowing helped to uncover only 16% of the most significant economic crime detected, compared to corporate controls which accounted for 57%. In other industries, tip-offs and whistleblowing helped to uncover 26% of economic crime.

A cautionary tale

The LIBOR scandal has highlighted competition law violations that also saw individual employees from different banks implicated in wrongdoing, putting in the spotlight the need for whistleblowers to 'lift the lid' on malpractice and fraudulent behaviour.

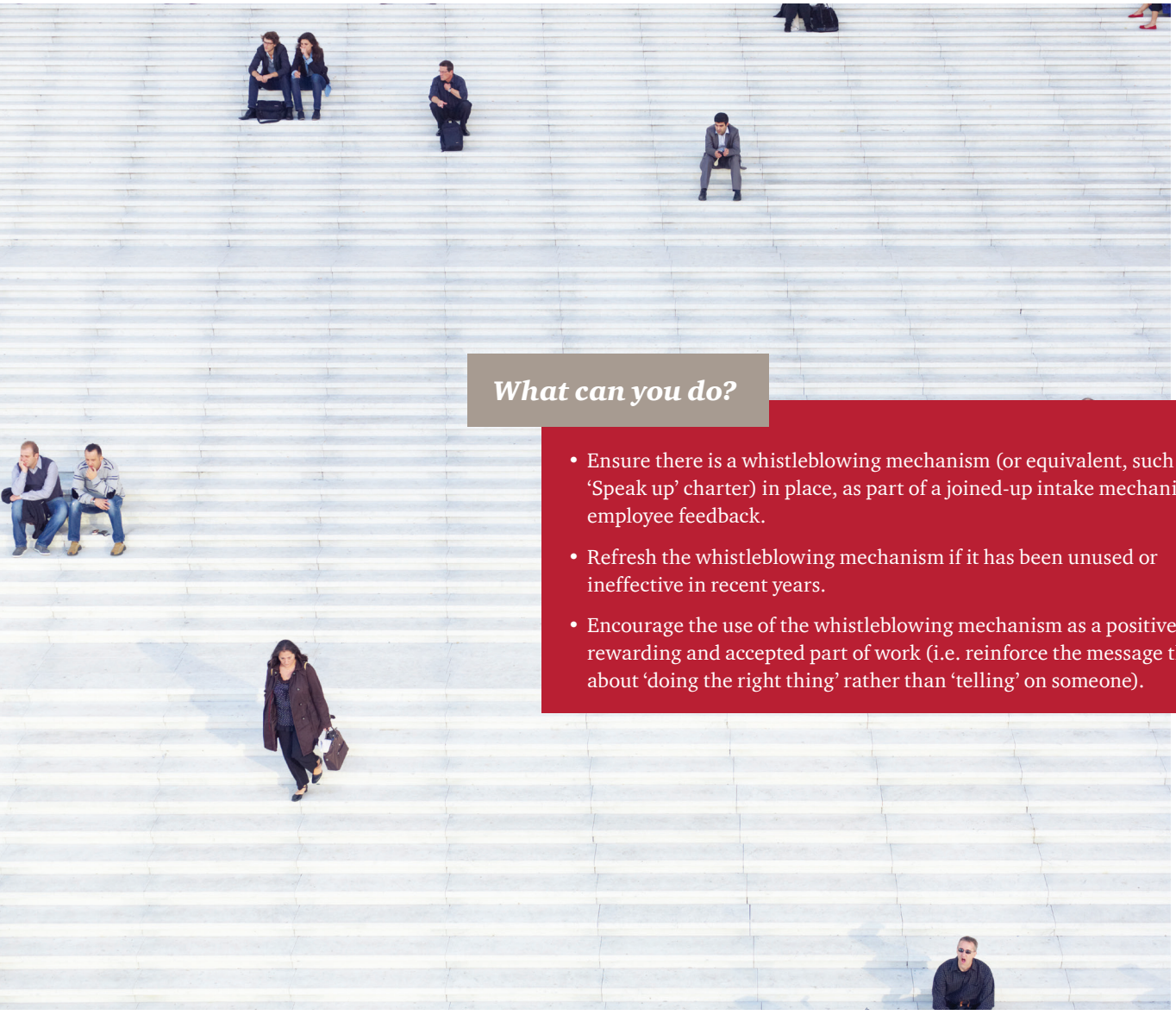
It is not enough to encourage the use of the whistleblowing mechanism if, as in the LIBOR case, employees are not encouraged to also challenge social conformity. It appears that many employees had not even realised or acknowledged that LIBOR manipulation equated to wrongdoing. A change in tone-from-the-top needs to take place in some FS organisations. Many banks have seen their reputation and public trust eroded in recent years; there needs to be a stronger culture of 'doing the right thing'.

Senior management need to lead from the front in this area, especially as accountability is now more heavily scrutinised by the regulators and potential criminal sanctions could be imposed if accountability is established.

Some FS regulators have taken significant measures to encourage whistleblowing. For example, people who provide original information that leads to a successful SEC enforcement action could be rewarded with a share of any sanction collected over $1m and a share of proceeds from any related regulatory action. In 2012, a former UBS banker was paid $104m by the U.S. Internal Revenue Service for revealing a tax evasion scheme. And in Germany, it has become a formal legal requirement for financial institutions to have an appropriate whistleblowing process (the effectiveness and appropriateness of which is subject to annual audit).

The magnitude of financial rewards available is being called into question by those worried about its distortionary effects on employee behaviour. It remains to be seen whether whistleblowing mechanisms will be abused as a result. Furthermore, whistleblowing is not seen as positive behaviour in certain territories for historical and cultural reasons. FS organisations may need to reflect on how whistleblowing concerns and outcomes are fed back into the business, as well as on the visibility of any such output, and ensure that the whistleblowing mechanism is sufficiently joined up with other feedback processes in the organisation.

On the whole, FS regulators are emphasising recognition of positive whistleblowing behaviour. A balanced approach is required - financial incentives and positive recognition need to be coupled with penalties for clear misuse of the whistleblowing mechanism. Moreover, employees should be empowered to identify and report issues before matters escalate to a stage where whistleblowing remains the only way forward.



What can you do?

- Ensure there is a whistleblowing mechanism (or equivalent, such as a 'Speak up' charter) in place, as part of a joined-up intake mechanism for employee feedback.
- Refresh the whistleblowing mechanism if it has been unused or ineffective in recent years.
- Encourage the use of the whistleblowing mechanism as a positive, rewarding and accepted part of work (i.e. reinforce the message that it is about 'doing the right thing' rather than 'telling' on someone).

Fraud risk assessment

In certain jurisdictions, FS regulatory requirements exist for risk areas like money laundering and fraud. Our survey asked about fraud risk assessments ("FRAs") and the results reveal a surprising number of FS organisations still do not carry any out. It is possible that if FRAs took place more regularly additional economic crime would have been detected. Other economic crime areas such as bribery, corruption and money laundering also benefit from thorough enterprise-wide risk assessments.

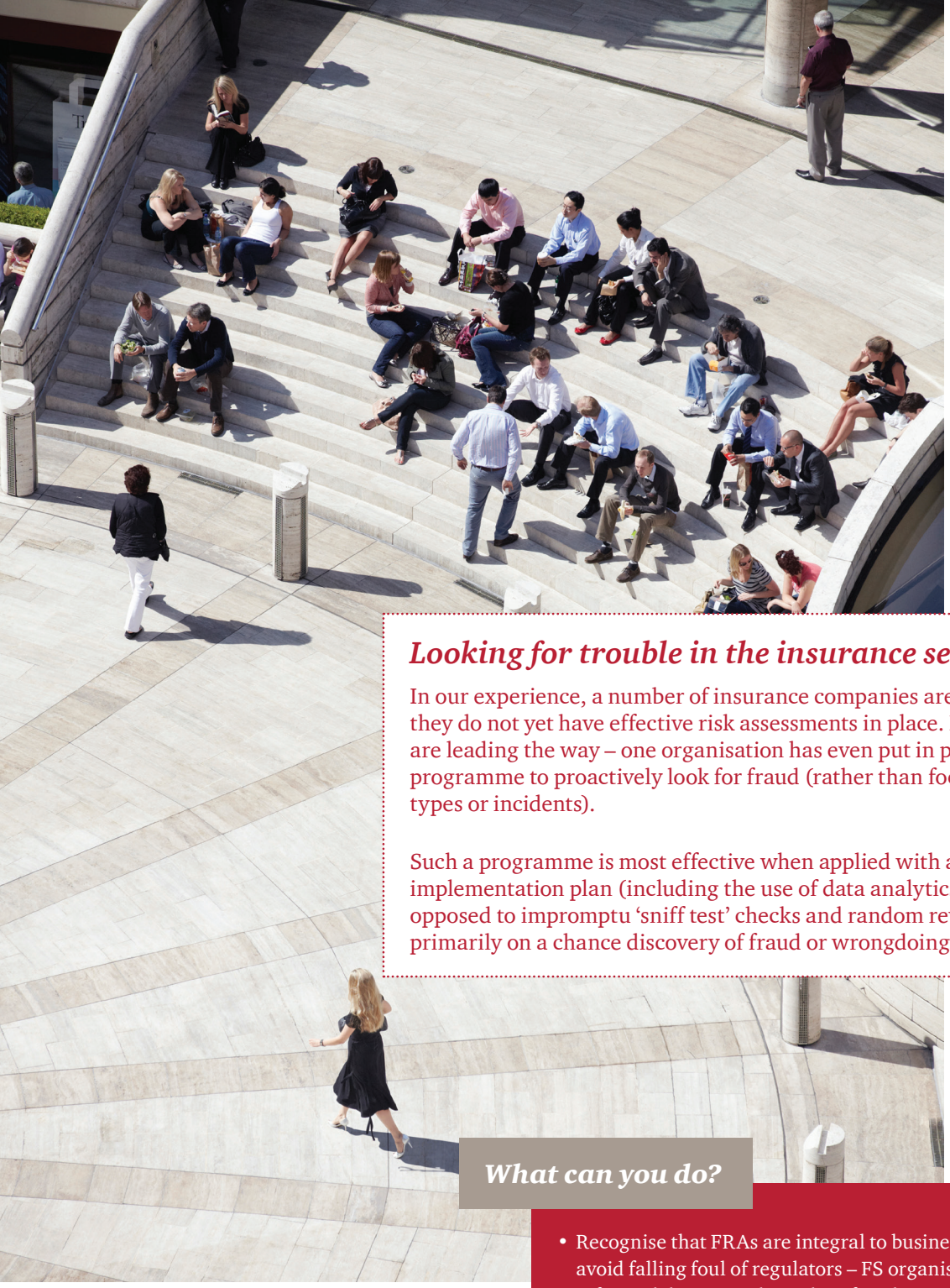
The percentage of FS respondents whose organisations did not perform annual FRAs has increased from 18% to 25%, This appears to be better than other industries (where 43% do not have annual FRAs), but is considered to be relatively high taking into account that FS regulators tend to expect or even fully require such a risk assessment in many jurisdictions.

A further 12% of FS respondents do not know whether any FRAs were performed in their organisation during the survey period. When asked why, 32% noted they did not know what an FRA involves (compared to 30% in other industries in 2014, 36% of FS respondents in 2011). Another 27% perceived a lack of value in FRAs.

It appears that over 50% of respondents from FS organisations that did not carry out any FRAs during the survey period fail to see the correlation between fraud, working conditions, organisational culture and the effectiveness of corporate controls. And yet, almost one in all 5 serious frauds was detected by Fraud Risk Management ("FRM"). FRM remains the most effective method in fraud detection (17% of serious frauds experienced by FS respondents were detected this way). Only 13% of frauds were detected through suspicious transaction reporting (compared to 19% in 2011). 6% were detected through data analytics (an option not offered in the 2011 survey) – which is likely to become a more important detection tool in the future. Surprisingly,1 in 5 FS respondents did not confirm a method of fraud detection ("Don't know") compared to only 8% in 2011.

Fig 5: Economic crime detection methods in FS organisations

% FS respondents



Looking for trouble in the insurance sector

In our experience, a number of insurance companies are starting to realise that they do not yet have effective risk assessments in place. However, some insurers are leading the way – one organisation has even put in place a fraud detection programme to proactively look for fraud (rather than focussing on specific known types or incidents).

Such a programme is most effective when applied with a clear methodology and implementation plan (including the use of data analytics if appropriate), as opposed to impromptu 'sniff test' checks and random reviews which seek to rely primarily on a chance discovery of fraud or wrongdoing.

What can you do?

- Recognise that FRAs are integral to business and often necessary to avoid falling foul of regulators – FS organisations need to be making informed decisions about their fraud prevention and detection mechanisms.
- Consider new ways of fraud detection – data analytics capabilities are helping FS organisations identify fraud based on 'outlier' criteria (e.g. unlikely transaction or payment dates).

Contacts

For more information on the Global Economic Crime Survey and the survey methodology, please refer to Economic crime: A threat to business globally at www.pwc.com/crimesurvey.

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 get in touch with your local PwC contact or the sector report team:

Contact team

Andrew Clark (Sector report lead partner)
+44 (0) 20 7804 5761
andrew.p.clark@uk.pwc.com

Tien Tien Tan (Sector report project manager)
+44 (0)20 7212 1133
tien.tien.t.tan@uk.pwc.com

Forensic Service Leaders

Chris Barbee
Partner, USA, Global Leader
+1 (267) 330 3020
chris.barbee@us.pwc.com

John Donker
Partner, Hong Kong, East Cluster Leader
+852 2289 2411
john.donker@hk.pwc.com

Andrew Palmer
Partner, United Kingdom, Central Cluster Leader
+44 (0) 20 7212 8656
andrew.palmer@uk.pwc.com

Erik Skramstad
Partner, USA, West Cluster Leader
+1 (617) 530 6156
erik.skramstad@us.pwc.com

Editorial team acknowledgements

In preparing this report, assistance was gratefully received from PwC teams in Germany, the Republic of Ireland, Israel, Lebanon, Qatar, Luxembourg, Malaysia, New Zealand, Nigeria, South Africa, the United Kingdom and the U.S.

Forensic Services

The PwC forensic services network is comprised of forensic accountants, economists, statisticians, former regulators and law enforcement, fraud examiners, forensic technologists and corporate intelligence specialists. 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.

The Design Group 21991 (02/14)