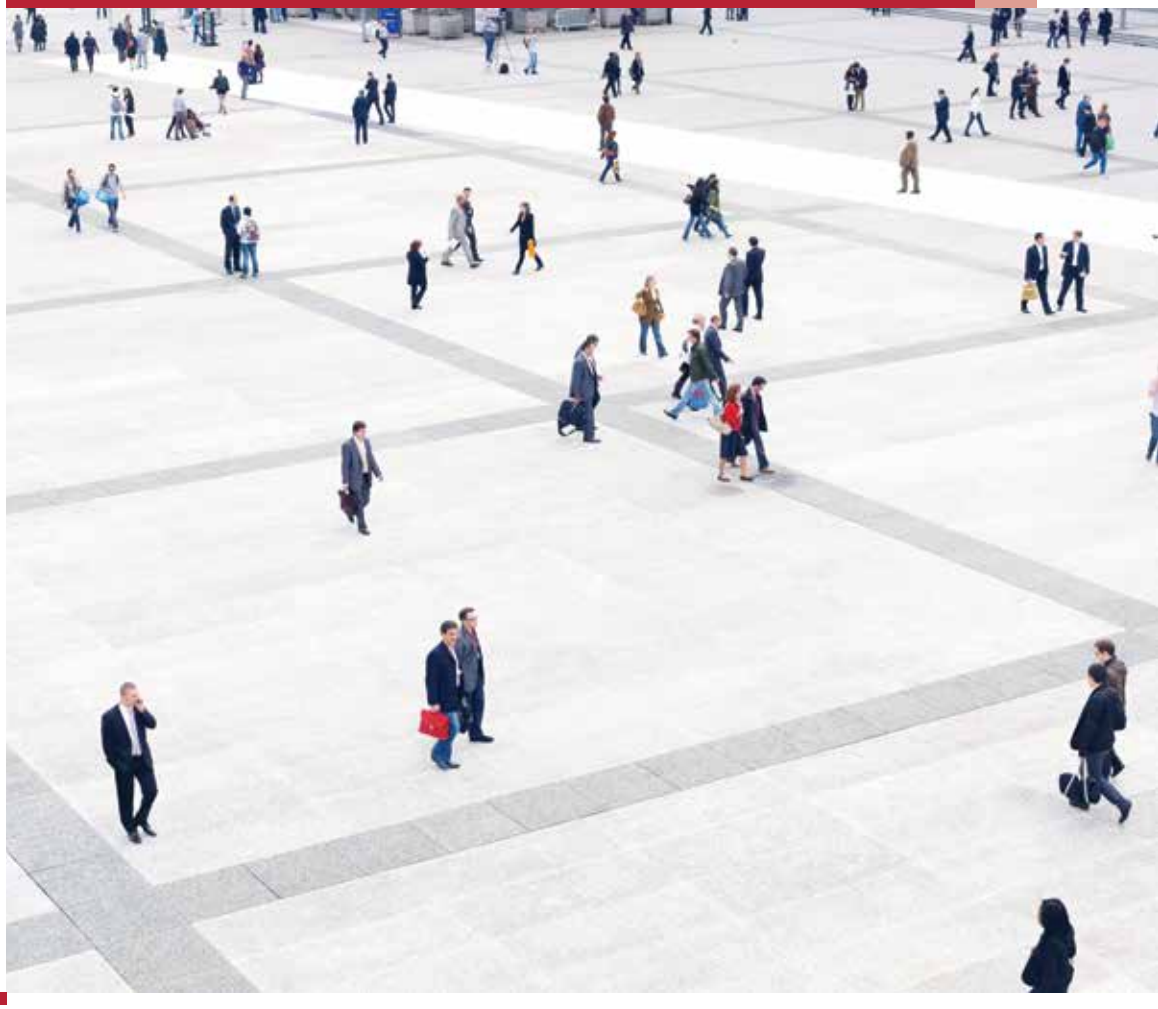
Fighting Fraud in Financial Services:

6th PwC Global Economic Crime Survey

An Australian snapshot of economic crime in the financial services sector

July 2012



pwc

Contents

Fast facts for the global financial services industry

45% Said their organisation experienced economic crime in the last 12 months, compared to 30% in other industries. Of those:

44% Said they experienced more than 10 incidents of fraud in the last 12 months.

54% Said they suffered losses in the last 12 months that were in excess of $100,000 as a result of fraud.

51% Said they think the risk of cybercrime has increased over the last 12 months.

> ***"People are highly motivated by fear of losing economic and social status relative to others. 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

Introduction

PwC is pleased to present Fighting Fraud in Financial Services which highlights, specifically in relation to financial services organisations, the challenges identified in the 6th PwC Global Economic Crime Survey 2011, one of the largest and most comprehensive surveys of its kind.

The 6th *PwC Global Economic Crime Survey 2011* was completed by 688 financial services respondents in 78 countries, and 3,877 respondents from all sectors globally. Of the total number of financial services respondents, 49% were senior executives of their respective organisations.

The uncertain economic environment has increased both the opportunity and incentive to commit economic crime. The financial services sector appears to be an industry of choice for fraudsters, where there continues to be high instances of asset misappropriation, money laundering and accounting fraud. In addition, with financial transactions increasingly technology-driven, there has been a significant increase in instances of cybercrime.

We have provided an Australian perspective by including Australian case studies from investigations we have conducted and observations by Australian regulators.

All the statistics provided in this report are taken from the results of the *PwC Global Economic Crime Survey 2011* unless otherwise stated.

PwC would like to thank everyone who participated in the survey. We hope these insights will help the financial services industry combat fraud and other economic crimes.

Malcolm Shackell
Partner, Forensic Services

Natalie Faulkner
Director, Forensic Services

Key findings

- 45% of the financial services respondents said they experienced one or more incidences of economic crime over the past year, significantly higher than the average of 30% across all industries. Of those:
- 44% said they had suffered more than 10 incidences of economic crime over the past year
- 54% reported their organisation directly lost more than $100,000 and 11% reported their organisation directly lost more than $5 million from economic crime over the past year.
- Asset misappropriation was the most common form of economic crime reported by the financial services respondents in the last 12 months (67%), followed by cybercrime (38%) and accounting fraud/money laundering (26% and 24% respectively).
- 60% of the financial services respondents said external parties committed the most serious incidences of economic crime over the past 12 months.
- The financial services respondents were asked which economic crimes they expected to occur over the next 12 months. The top three economic crimes expected were cybercrime (43%), money laundering (36%) and asset misappropriation (35%).
- 22% of the financial services sector respondents noted economic crime had a significant impact on the organisation's reputation and brand, and 23% noted a significant impact on the organisation's relations with regulators.

Cybercrime

- Cybercrime, also known as computer crime, is defined as economic crime using a computer and/or the internet as the primary tool to commit fraud.
- Cybercrime was reported by the financial services respondents as the second most common type of economic crime after asset misappropriation.
- 38% of the financial services respondents experienced cybercrime over the past 12 months compared to our last survey in 2009, where cybercrime was not statistically significant (i.e. 0%). Additionally, 43% of the financial services respondents thought it was likely they would experience cybercrime in the next 12 months.
- 51% of the financial services respondents think the risk of cybercrime is increasing.

Despite these statistics, many of the financial services respondents continue to take a reactive, instead of a proactive approach to managing cybercrime. 30% of senior executives and board members review cybercrime risks on an ad-hoc basis or not at all, and nearly a third of respondents in financial services organisations have not received any cyber security-related training.

Instances of fraud

45% of the financial services respondents experienced economic crime over the past 12 months, higher than the all industry average of 30%.

From PwC's Global Economic Crime Survey, it appears that the financial services industry is a target for economic crime, ranking as the sixth highest out of the 22 industries that reported having experienced incidences of economic crime in the last 12 months. It should be noted that the results for the insurance industry were reported separately to the financial services sector as a whole, with the insurance sector placing second and the health care sector coming at the top of the list.

In relation to the quantity of funds misappropriated, 54% of the financial services respondents reported more than $100,000 lost to economic crime in the past 12 months, compared to 43% across all industries.

In response to the economic downturn, many banks and financial services providers are cutting costs and restructuring, which may result in increased back office fraud risk where full checks and balances and segregation of duties may have been removed[1] providing the opportunity to commit fraud.

Existing controls appear to be challenged by:

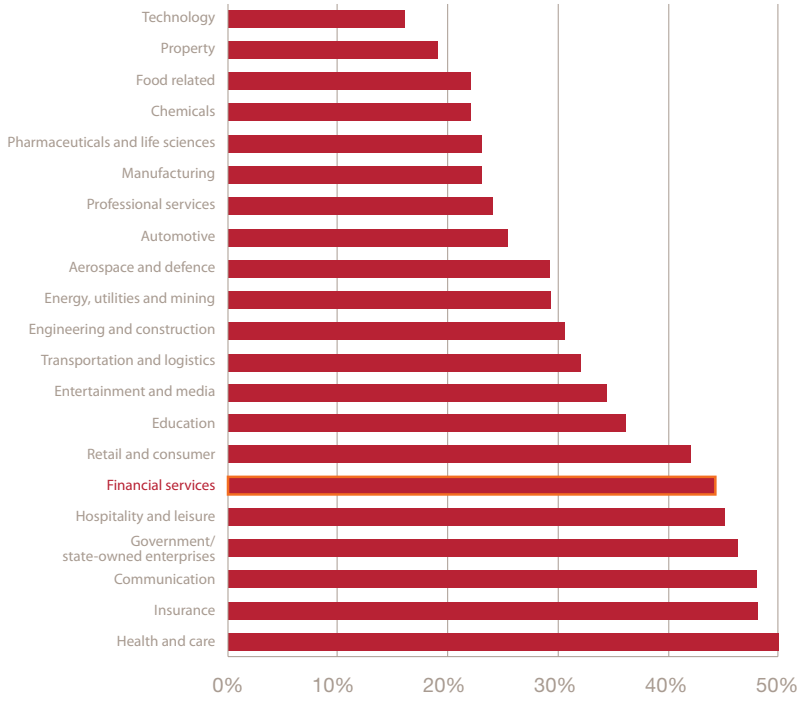
- The replacement, or upgrading of banking systems.
- Risks arising from process reorganisation in the interests of driving efficiency and cost reduction.
- The increasing complexity of products and platforms.
- Merger and acquisition activity.
- New regulations.

With organisations focused on cost reduction, reinforcing the highest levels of integrity and codes of conduct may not be prioritised, thus creating opportunities for economic crime.

In the current economic climate, there are increased incidences of reduced job security, reduced pay rises and/or reduced or eliminated bonuses. This can impact the culture of an organisation, creating a culture of 'entitlement' where employees feel they deserve more compensation than they are receiving, thus providing the incentive to commit economic crime and possibly allowing employees to justify or rationalise the act of fraud.

The increase in reported economic crime may also be due to organisations implementing better fraud detection techniques such as data analytics and continuous transaction monitoring to detect fraud. Fraud detection and prevention methods to help reduce instances of fraud are discussed later in this publication.

The % of global respondents by industry who stated they had suffered fraud in the past 12 months



1 *Banking Banana skins 2012: the system in peril*, PwC and the Centre for the study of Financial Innovation (CSFI), March 2012, p.5

Economic crimes experienced in the financial services sector

Our survey shows that there has been an increase in almost all types of fraud. When asked which types of economic crime the financial services respondents experienced over the past 12 months, the most prevalent was asset misappropriation, experienced by 67% of respondents.

Asset misappropriation

Asset misappropriation is the most prevalent type of fraud reported across all industries. Prevention is often reliant on the vigilance of employees, and traditional detective measures can easily miss fraud that is hidden within millions of transactions. An example of asset misappropriation is procurement fraud. In our experience, most procurement frauds are conducted over a period of several years and it can be hard for organisations to recoup losses related to this type of fraud. It is, however, an area where data analytics can bring real benefits in detecting fraud as early as possible to reduce the quantum of funds misappropriated.

Cybercrime

Cybercrime, previously statistically insignificant, has emerged as a growing threat and was reported as having been suffered by 38% of the financial services respondents. The level of cybercrime experienced in the last 12 months for all industries in Australia (30%) is significantly higher than global (23%) and Asia Pacific (22%) levels.

The increase in cybercrime is not unexpected, as transactions are increasingly technology-driven with customers accessing their bank, trading and superannuation accounts online rather than by entering a branch or physical location. In our experience, recent financial services cybercrimes have included:

- Phishing spam emails pretending to be from the financial services provider requesting the account holder to enter their account and password details.
- Unaurthorised access of online trading accounts.
- ATM skimming where bank account details are copied from the magnetic strip on a credit or debit card when an ATM or EFTPOS machine is used. Increasingly sophisticated skimming machines pick up key strokes and no longer require surveillance of the pin being entered.
- Overseas syndicates targeting superannuation funds posing as the account holder (having obtained identity information from post theft or electronically) and withdrawing funds claiming to be setting up a self-managed superannuation fund.

Accounting Fraud

The number of financial services respondents experiencing accounting fraud has increased from 19% in 2009 to 26% in 2011. This increase may be due to borrowers' incentive to appear credit worthy in order to secure finance, despite economic deterioration in their position.

Increase in internal accounting fraud may be due to employees being motivated to misstate performance in order to reach KPIs during difficult economic times.

Money laundering

24% of the financial services respondents reported that they detected money laundering activity in their organisation in the past 12 months. Globally, there has been an increase in awareness of the obligation to report suspicious matters, as required by regulators around the world. In addition, there is more media coverage of money laundering cases, which has also increased awareness of this type of crime.

The increased reporting of incidences of money laundering by the financial services respondents may be driven by regulatory requirements of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. Quantifying the extent of money laundering is difficult given its covert nature. The Australian Transaction Reports and Analysis Centre (AUSTRAC) estimates that more than AU$1.5 trillion of illegal funds are laundered worldwide each year, with AU$200 billion being in the Asia Pacific region.[2]

2. *Money Laundering in Australia*, 2011, Australian Transaction Reports and Analysis Centre, 2011, Canberra, AUSTRAC, p17, www.austrac.gov.au/money_laundering_in_australia_2011.html, accessed 17 April 2012

The financial services respondents have reported more cybercrime, accounting fraud, money laundering and insider trading compared to the average reported across all industries. This may be because the financial services industry is highly regulated and has extensive controls for identifying attempted fraud.

Bribery and corruption

16% of the financial services respondents reported instances of bribery and corruption in the past 12 months. Recent high profile cases of bribery and corruption involving Australian companies and increased Australian Federal Police activity both highlight the need for businesses to consider and address the risk of bribery and corruption as part of day-to-day operations. Organisations need to instill a zero tolerance culture towards bribery and corruption.

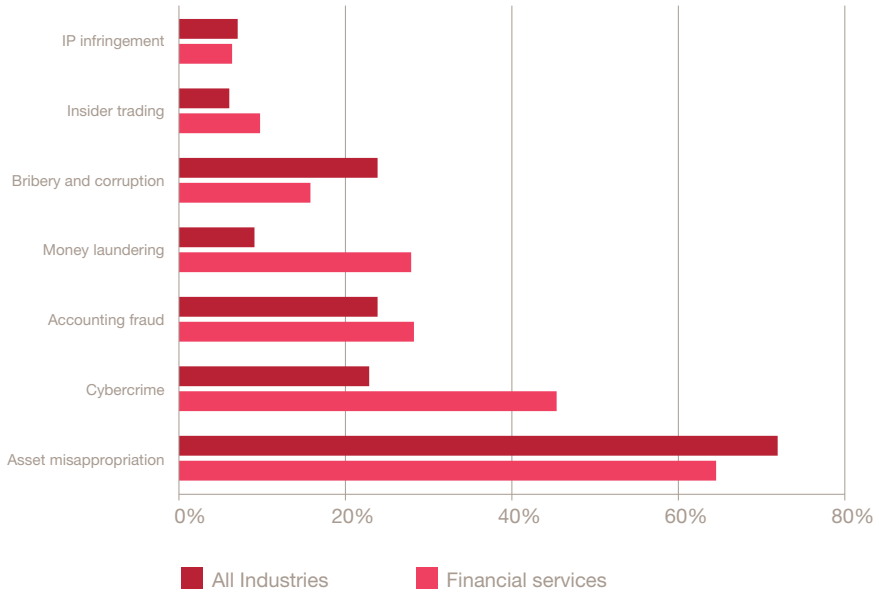
Insider trading

Insider trading was reported as having been experienced by 10% of the financial services respondents over the past 12 months. In November 2011, the Australian Securities and Investments Commission (ASIC) reported receiving almost 30,000 insider trading tip-offs and 35 cases were referred for formal investigation.[3]

"During regular surveillance of the Australian financial markets, ASIC has become aware of several stockbroking account intrusions involving unauthorised access and trading."

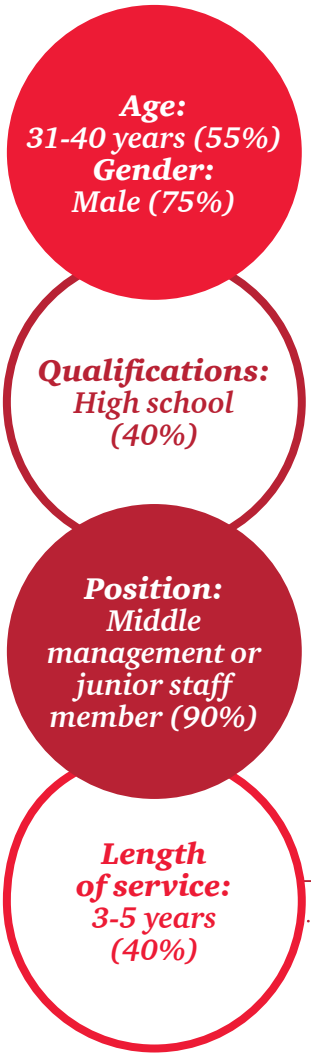
– ASIC Consumer Alert, 20 January 2012

The % of financial services respondents experiencing each type of fraud compared to respondents in other industries



3. Harper, J., *ASIC warns on insider trading*, Herald Sun, November 28, 2011, http://www.heraldsun.com.au accessed 17 April 2012

Profile of a fraudster



Profile of an average Australian fraudsters

(PwC survey results across all industries)

60% of the financial services respondents said external parties committed the most serious incidences of economic crime over the past 12 months. In other industries, the fraudster is typically reported as being on the entity's payroll.

Crime syndicates and money laundering: financial services

The higher rate of external fraudsters targeting the financial services industry is consistent with the predominance of cybercrime and money laundering in the financial services industry. These economic crimes are increasingly perpetrated by sophisticated, entrepreneurial and well organised crime syndicates.

Crime syndicates in the past typically looked to banks to launder the proceeds of crime including drug trafficking, gambling, people trafficking, theft and prostitution. More recently, banks appear to have strengthened their customer due diligence practices and money laundering controls, yet PwC's survey shows money laundering is still an ongoing threat to financial institutions.

The Australian Crime Commission estimates organised crime costs Australia from $10 billion to $15 billion per annum[4]. The Australian Crime Commission notes that an increasing number of organised crime groups in Australia are becoming involved in money laundering[6].

AUSTRAC recently published *Money Laundering in Australia 2011*[5], a consolidated picture of money laundering activity in Australia, including key vulnerabilities and emerging threats.

AUSTRAC's paper notes that the sheer size and complexity of banking systems globally offers opportunities for fraudsters to conceal illicit transactions.

Crime syndicates are also targeting money transfer businesses and alternative remittance dealers who transfer funds (or value) within and between countries. There are some 7,000 small businesses in Australia in this sector, most operating as part of a larger network, which typically conduct high volume, low value transactions. In the last financial year, AUSTRAC received international funds transfer reports from these businesses amounting to approximately $8.2 billion, a significant amount of funds for criminals and fraudsters to target.

4. *Money Laundering Fact Sheet*, 2011, The Australian Crime Commission, www.crimecommission.gov.au accessed 17 April 2012
5. *Money Laundering in Australia*, 2011, Australian Transaction Reports and Analysis Centre, 2011, Canberra, AUSTRAC, p17, www.austrac.gov.au/money_laundering_in_australia_2011.html, accessed 17 April 2012
6. *Money Laundering Fact Sheet*, 2011, The Australian Crime Commission, www.crimecommission.gov.au accessed 17 April 2012

Crime syndicates: superannuation

Crime syndicates have also been targeting Australian superannuation funds. Australian superannuation fund assets are estimated to have reached almost US$1.3 trillion, according to Towers Watson's 2011 survey[7].

In 2011, Australian superannuation assets moved up from fifth position to become the fourth largest pension asset pool in the world. The Australian Prudential Regulation Authority (APRA) has noted in its best practice guide, *How to Reduce the Risk of Fraud*[8] that projections show this figure will continue to grow significantly in the next twenty years and with it, the incentive to commit fraud.

APRA notes this trend places an increasing onus on superannuation fund trustees to ensure adequate internal controls are established within their funds to safeguard members' assets against fraud.

In our experience key fraud risks to superannuation funds include:

- Identity fraud where crime syndicates have used fake identification to set up a self-managed super fund and withdrawn customer savings.
- Risk of financial planners, investment managers, accountants or advisers diverting funds.
- False death certificates.
- Phishing scams whereby personal details are obtained and superannuation accessed.
- Associates posing as relatives, for example an estranged spouse.
- Superannuation fund employees investing in unauthorised investments, whether or not for personal gain.

Gatekeepers

In PwC's experience, economic crime is also conducted within the financial services industry by those in a position of trust, where there is a duty of care when dealing with customers' funds. ASIC's chairman, Mr Greg Medcraft, has stated that part of his focus in meeting ASIC's priorities is to hold these "gatekeepers" to the financial system accountable.

Mr Medcraft listed "gatekeepers" as including accountants, directors, advisers, custodians, product manufacturers, market operators and participants. ASIC has stated it will take action where "gatekeepers" do not meet their responsibilities[9].

Australian case study

Fraud by a financial adviser

PwC performed an investigation of an accounting practice acting as the financial adviser to a high net worth individual. Unbeknownst to the individual, the accounting firm improperly invested funds in loans to various individuals, and listed and unlisted entities, including loans to associates of the accounting firm. To do this the accountant used a fraudulent power of attorney. The high net worth individual lost over $50 million and, following years of litigation, the case was settled for an undisclosed amount.

7. *Global Pension Asset Study*, 2012, Towers Watsons, p7, www.towerswatson.com/assets/pdf/6267/Global-Pensions-Asset-Study-2012.pdf accessed 17 April 2012
8. *How to Reduce the Risk of Fraud*, 2012, The Australian Prudential Regulatory Authority (APRA), p5, www.apra.gov.au accessed 17 April 2012, http://creativecommons.org/licenses/by/3.0/au/legalcode
9. *Committee for Sydney presentation, Speaking notes for address by Greg Medcraft, Chairman*, 8 November 2011, Australian Securities and Investments Commission (ASIC), p3, www.asic.gov.au accessed 17 April 2012

Internal risk

PwC's survey shows internal parties committed 40% of the most serious economic crimes against financial services organisations in the past 12 months.

Experience has shown that financial services organisations with cultures that focus on, and reward employees for the pursuit of profit without sufficient focus on a robust control environment can be susceptible to heavy losses.

The share of economic crime incidents committed by employees for all industries in Australia was reported to have increased from 33% in 2009 to 54% in 2011. This escalation of internal fraud highlights the importance of organisations focusing on proactive fraud risk management. APRA notes that minimising opportunity is the most important element in fighting fraud. Gaps in controls, lack of segregation of duties where the same employee is responsible for processing, recording and reconciling transactions can increase the opportunity for the fraudster.

The typical internal fraud involves a long period of undiscovered deceptions, rather than a single large fraudulent incident (as is often the case with external fraud). Having fraud detection methods in place such as data analytics can result in early detection of such fraud, reducing the amount of funds taken.

Proactive fraud prevention measures will help organisations identify weaknesses in their environment and reduce opportunities for internal fraud. These may include having a robust fraud risk framework, managerial messages about intolerance of fraudulent or rogue behaviour where controls are bypassed or over-ridden, pre-employment and on-going screening and, most importantly, fostering a culture of fraud awareness.

Australian case studies

Fraud by a relationship manager at a global bank

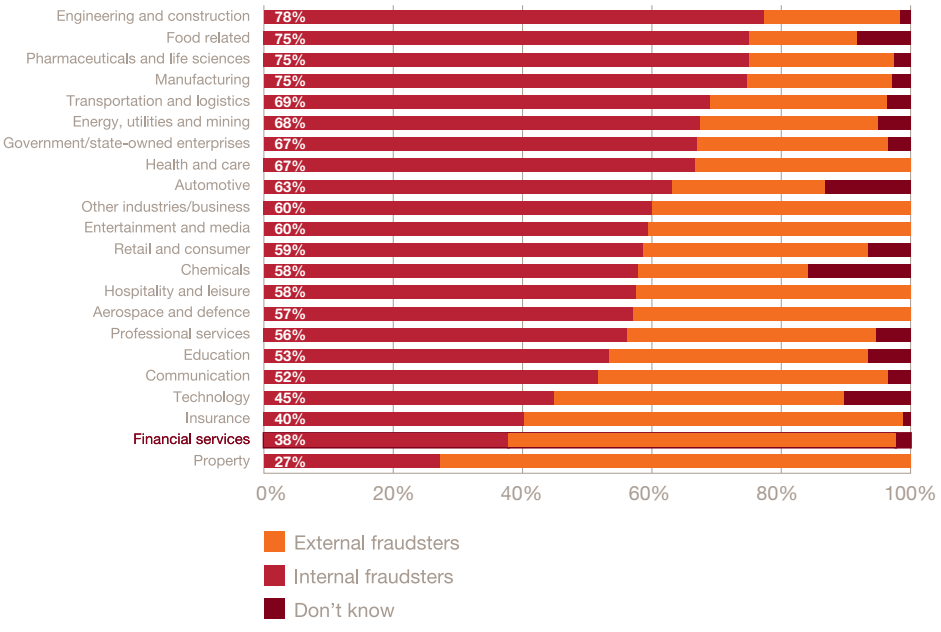
PwC performed an investigation of a relationship manager (RM) who was diverting customer funds to her personal bank account via a foreign exchange institution. She was also transferring funds between customer accounts in order to appear to be a successful foreign currency trader. The RM targeted foreign and older customers whom she believed were not vigilantly monitoring their accounts. She suppressed customer statements and communicated to the account holders that their account balances were higher than they actually were.

The estimated loss to the bank was over $3.5 million.

Mortgage fraud

An investment manager became concerned about a number of loans in their investment portfolio obtained through mortgage brokers. PwC performed an investigation and found there was a mismatch between loan applications, pay slips and tax returns. A number of the tax returns were prepared by the same tax agent and in one case, it appeared finance was obtained without the knowledge or consent of the security holders. Further, data analytics showed that a number of borrowers shared details such as addresses and contact numbers. We identified that a mortgage broker was acting in collusion with valuers to obtain mortgages for customers with insufficient security for loans.

The % of fraud committed by internal and external parties



Forward thinking: will fraud continue to rise?

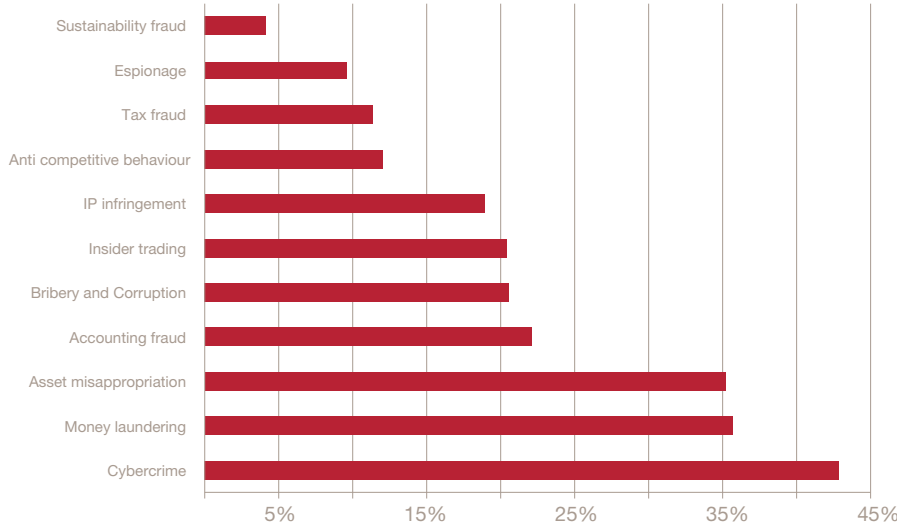
Money laundering, asset misappropriation and accounting fraud, together with bribery and corruption, remain high on the list of expected future economic crimes. However, new risks such as cybercrime and sustainability fraud are increasing rapidly.

Respondents to the PwC survey were asked which types of economic crime they expected to experience in the next 12 months (respondents were able to nominate more than one type of economic crime). Financial services respondents felt that in the next 12 months the most likely economic crimes will be cybercrime (43%), money laundering (36%) and asset misappropriation (35%).

When we compare the estimates of future fraud from previous PwC surveys, to actual fraud that occurred post survey and match expectations to occurrence, it appears that respondents have underestimated the level of economic crime they are likely to experience in the future.

In the next section, we look at how financial services respondents act to prevent and detect future economic crime.

The % of financial services respondents with types of fraud thought to most likely occur in the next 12 months



Putting the detective cap on: detecting and preventing fraud

One reason for the increased reporting of economic crime in the financial services sector may be the growing focus on fraud risk, fraud risk management processes and controls and suspicious transactions analysis, despite the pressure on resources.

Fraud risk management

There appears to be a correlation between the frequency of fraud risk assessments and the extent of reported frauds across all industries.

PwC's survey shows that the most effective detection method for financial services respondents was fraud risk management, with 21% of the respondents reporting that their most serious economic crimes were detected using this method.

67% of the financial services respondents reported conducting at least one fraud risk assessment in the last 12 months, higher than the all industry average of 59%. In an ever-changing world, fraud risk assessments can quickly become out of date, leaving an organisation vulnerable to new threats if not revisited regularly. We would suggest every 2 years or more frequently if there is a change in the business operations.

Where a fraud risk assessment was not performed, the main reported reason for not performing a fraud risk assessment was that the respondents did not know what was involved (36%). Another reported reason was that there was a perceived lack of value (34%). Our view is that, when done well, a fraud risk assessment can be a vital tool in the anti-fraud arsenal.

Suspicious transactions reporting

Increased use of technology is helping to fight fraud. Identifying suspicious transactions through the use of data mining and analysis can quickly identify anomalies to help identify fraud. If fraud is detected sooner, the damage is likely to be less.

Suspicious transaction reporting can be an effective tool to detect fraud and error in financial systems by identifying:

- Collusion between parties (employees, vendors, agents).
- Errors in processing (for example duplicate payments).
- Whether obsolete information, which a fraudster may use to mask their conduct, has been retired from the system.
- Fraudulent transactions (for example, vendor payments to an employee's bank account).

Respondents across all industries have reported an increased reliance on suspicious transaction reporting to detect fraud. When asked about the most serious economic crime experienced over the past 12 months, 14% of the respondents reported that they detected the incident using suspicious transaction reporting. This highlights the potential benefits to organisations of performing analysis of their financial systems to identify conflicts of interest and potential fraud.

Internal audit

Internal audit processes, although not directly aimed at detecting fraud, can also be a means of identifying fraud with the financial services respondents reporting that 9% of the most serious economic crimes in the last 12 months were detected by internal audit processes.

Tip offs/Whistleblower hotline

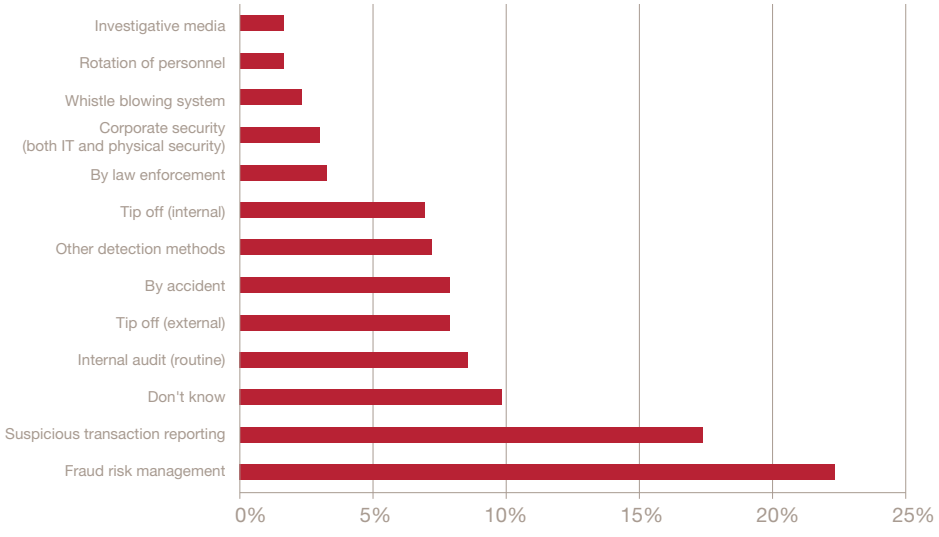
Internal and external tip offs can also help detect fraud in financial services organisations (15% of the respondents reported that they detected fraud in this way). This suggests that implementing a whistleblower policy and reporting channel is valuable in the fight against fraud. However, 45% of the financial services respondents do not employ a whistleblower mechanism and 28% said their whistleblower mechanism, was either not effective or slightly effective.

Australian case study

Data analytics – expense claim

Data analytics were used to review unusual expense claims made by staff, including senior executives, by matching expense claims to policy allowances. Several years worth of data were analysed for suspicious transactions. Expense items were then matched to supporting documentation, and 'show cause' notifications were given to staff where required. The analysis showed employees had breached policy allowances on multiple occasions. A further review was performed around the approval processes for expense claims, which found senior executives were using peer review as a way to approve claims which were outside the policy. This highlights the value in taking a combined approach to tackling fraud, including data analysis, controls and an organisational culture of compliance and zero tolerance to fraud.

Financial services methods used to detect the most serious economic crime in the last 12 months



Finger on the trigger: responding to fraud

The PwC survey shows that financial services respondents are more likely to take civil action and refer fraud matters to law enforcement authorities and regulators, for both internal and external perpetrators, than all other industries surveyed.

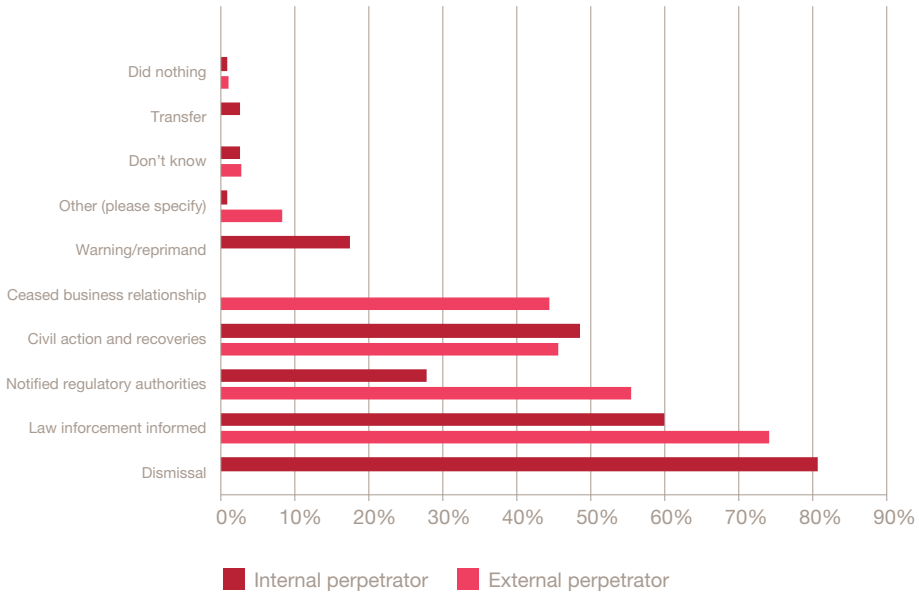
In relation to internal fraud, the relevant employee was dismissed in 81% of cases reported by the respondents.

In relation to fraud committed by external perpetrators, 74% of financial services respondents stated that they informed law enforcement authorities of the fraud, compared to 60% with respect to internal fraud. Regulators were informed by the respondents in 55% of instances for external fraud and only 28% in cases of internal fraud.

It is our view that failure to report fraud to the police and/or regulatory authorities can influence organisational culture and can send a message that staff misconduct is not taken seriously. It may also increase the risk that employees who have been disciplined but not reported by their employer may obtain employment with another organisation and continue fraudulent behaviour.

The financial services respondents reported that they ceased doing business with an external fraudster in only 45% of instances of external fraud. We believe that a significant controls review around transactions would need to be undertaken by an organisation before continuing to do business with a third party who had perpetrated fraud against the organisation.

Action taken against perpetrators by financial services respondents'



Cybercrime: the emerging economic crime

Cybercrime ranks as the second most reported economic crime for the financial services respondents. Examples of cybercrime noted by the financial services respondents include account takeovers, siphoning off of money or stealing customer data. In prior years, cybercrime was so statistically insignificant that results were combined with 'other types of fraud'. So why has cybercrime increased so markedly?

In our view, the increased awareness of cybercrime risks has occurred partly because media attention around recent high profile cases has increased organisational awareness of this threat.

Cybercrime can be defined in a number of different ways. The following definition was used in our survey: "Cybercrime, also known as computer crime, is 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 account details. It is only a cybercrime if a computer, or computers, and the internet play a central role in the crime, not an incidental one."

As with traditional economic crime, cybercrime can take many different forms.

Globally, businesses are increasing their reliance on technologies such as cloud computing, online banking and social networks. At the same time, the rate of change for new technology is increasing, for example the rapid uptake of mobile banking apps to access banking services. Organisations are finding it difficult to keep up with the risks of introducing and using new technology. To highlight this point, the number of internet-enabled devices now exceed the earth's population.

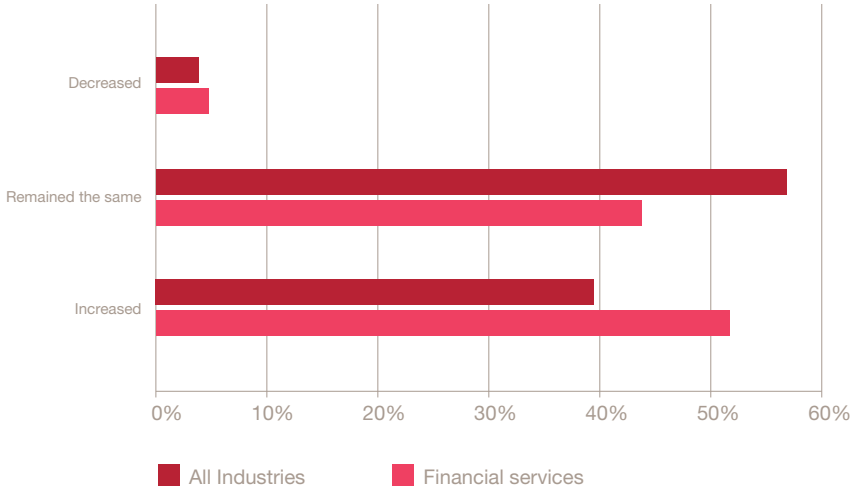
Our survey shows that organisations are aware of the growing threat, with 43% of the financial services respondents indicating they believe they are likely to suffer a cybercrime attack in the next 12 months. Further, 53% of the financial services respondents perceive the greatest risk of cybercrime to be from outside their organisation (compared to 10% who say the greatest risk of cybercrime is internal). 31% of the financial services respondents say the risk from cybercrime comes from both internal and external threats.

Cybercrime is no longer the domain of young hackers, instead it is committed by a multitude of offenders with diverse motives, including:

- Insiders who have authorised access to relevant systems and who abuse this for personal gain.
- Competitors who are seeking an advantage.
- Trans-national criminal enterprises who are stealing and extorting information to generate income.
- Moral activists (or 'hacktivists' as they are known) who are protesting company actions or policies.
- Disgruntled parties obtaining confidential information (such as bank account details, pay, bonuses and other rewards) and uses this information for personal advantage.
- Employees sharing sensitive information with friends or connections on social media, which spreads to the public domain.
- Websites are defaced or disrupted by an attack on the server of the computer network so the server does not perform properly or prevents legitimate website visitors from accessing the site.
- People are tricked into disclosing their confidential information or passwords required to access their accounts through an email requesting they click onto an authentic looking but fake website and input their personal information. It is then possible to fraudulently transfer money from an individual's account.
- An individual deliberately enters malicious software (for example viruses or trojans) into a computer network to steal information or damage the system, causing economic loss.

In relation to internal risks, 62% of the financial services respondents perceived their IT departments to represent the highest potential risk, followed by operations (48%). So the 'cyber savvy CEO' needs to consider whether all departments, including those viewed as low risk, such as HR and legal, are sufficiently protected, especially given the nature of information to which they have access.

Financial services respondents' perception of the risk of cybercrime attack in the next 12 months



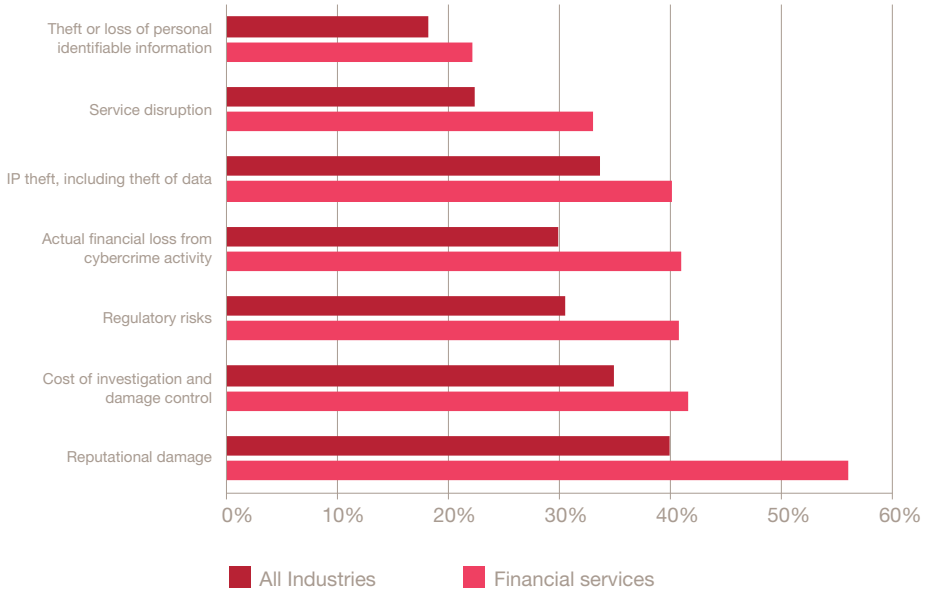
What are you most worried about?

With respect to cybercrime, the financial services respondents were most concerned about reputational damage (56%) followed by the cost of an investigation (42%). This is one of the troubling features of cybercrime – the impact of the fraud can be more extensive than the amounts the subject of the actual fraud.

Some of the characteristics that make cybercrime dangerous:

- Single event frauds – cybercrime is often a single event crime, resulting in a potentially devastating one-off financial loss.
- Low risks and high rewards – committing cybercrime is attractive to many fraudsters, with the high availability and decreasing costs of technology lowering the set up costs required to commit crime. In addition, there are fewer risks when compared with frauds that require physical presence at the target organisation.
- Anonymous perpetrators – the technical knowledge of cybercrime fraudsters means in many cases it is difficult for authorities to identify the perpetrator or even the location of the crime.
- Difficulty of recovery – cybercrime is a global business with fraudsters often located offshore. This makes it difficult to arrest and prosecute cybercriminals and, more importantly – hinders efforts to recover misappropriated funds.
- Diversity of risk – the motivation behind cyber attacks can vary greatly meaning it is difficult to know what is at risk. Attackers may be financially motivated and target payment systems or customer details. Others may be politically motivated wanting to cause disruption to operating systems, while some may be motivated to harm and interfere with defence networks and communications.
- Speed of information dissemination – once accessed, information can be disseminated within seconds meaning response plans have to be extremely agile and decisions need to be made quickly. Australian banks with IT system failures have experienced this when social media has been used to quickly disseminate and exploit weakness following a systems failure.

The % financial services respondents concerned about the impact of a cybercrime attack



Where has your USB been lately?

When working outside a secure office environment, most employees are aware of the need to protect sensitive data contained in physical documents. However with the increased portability of confidential data on smart phones, tablets and USB drives are you being careful enough? Consider the following questions:

- Where has your USB been?
- What wireless internet connections have you used for your company laptop and or smart device? Were they all in the office, or were some of them public hotspots?
- How complex are your passwords? Do you keep copies of your passwords in secure locations?
- Who else has access to your computer?
- To whom have you provided your personal information?
- Have you travelled to high risk territories where malware could have been placed on your computer?

Australian case study: targeting of executives

A recent cybercrime case which we assisted to investigate involved senior executives of a large multi-national organisation, who routinely travelled to foreign countries where the business had offshore operations. The fraudsters used sophisticated cybercrime techniques as part of their campaign. They produced a spoof email from a computer, compromised a website, distributed malicious PDF documents and other URL links and downloaded software to the victim company's network without consent. The malicious software gave the fraudsters "super user" access to the company's corporate network. Specialist forensic investigations identified evidence of continuous targeting for a significant period of time. As a result of the investigation, the infected machines were cleaned. The organisation has since put further security controls in place including forensic analysis of machines before and after overseas travel. In addition, senior executives have been educated about appropriate security practices when travelling.

On the front line with cyber security

Some of the questions that should be asked to gauge an organisation's cyber security expertise are:

- Is the threat of cybercrime on the organisation's risk register and/or considered a risk by the organisation?
- Does the organisation know the number of security incidents that have occurred in the past year?
- Are executives' electronic devices checked for tampering or malicious software pre- and post-travel to high-risk countries?
- Does the organisation have a security strategy and governance approach that is aligned with business strategy?
- Does the organisation have a tested incident response plan for cyber security issues?
- Are staff trained on risks and policies?

A failure to respond immediately to cybercrime with crisis management and cyber investigative techniques can result in significant financial losses and irreparable damage to an organisation's reputation. While critically important, forensic investigative experience is generally not a core competency of leading global organisations. Simply put, it is seldom practical for most organisations to maintain the requisite forensic investigative resources and technologies necessary to effectively conduct complex cyber investigations. Organisations should ensure that, where they have do not have this capability internally, they can draw on external resources in the event of a cyber attack.

Are you prepared?

The first few hours are critical when a cybercrime incident occurs. When asked who holds the ultimate responsibility for managing an organisation's cybercrime risks, 54% of the financial services respondents named either the chief information officer (CIO) or chief security officer (CSO). Only 18% specified the CEO or the board. In addition, 44% of financial services respondents reported the CEO and board reviewed cyber-related risks once a year or less. This indicates the current state of awareness of cybercrime at the management level remains limited.

The increasing prevalence and far reaching impact of cybercrime means it is no longer just an issue for the CIO. While it is easy to characterise cybercrime simply as 'an IT issue', senior management and boards must take a more holistic approach to understanding their exposure to and appetite for cyber risks.

More than 51% of the financial services respondents reported that they felt the risk of cybercrime was growing. But this is not reflected in the preparation for cybercrime incidents. Of the financial services respondents:

30% said their organisation did not have the in-house capability to prevent and detect cybercrime.

36% said their organisation did not monitor the use of social media sites. These sites can present significant security risks if employees and hackers abuse them.

27% said they had received no cyber security-related awareness training in the last 12 months.

37% do not have or are not aware of having emergency shut down procedures in place, which is concerning given the first few hours of a cyber attack are critical.

46% do not have or are not aware of having, a media or PR management plan in relation to cybercrime.

These results suggest that management of the risk of cybercrime continues to be reactive rather than proactive and that control improvements need to be made to protect against cybercrime.

Part of the problem is that no one owns or controls the internet. There is little governance, oversight or regulatory power over its users. What's more, organised criminals have become increasingly sophisticated in their ability to exploit flaws in the way the internet and other online channels operate. Many organisations simply do not know where or how to start preparing for these threats.

Principles of fraud risk management in protecting against cybercrime

The pace of technology means organisations are constantly undergoing business transformation to maintain a leading edge. This exposes organisations to unknown cyber threats. It is important for financial services organisations to have an overall information security strategy that sets out the approach to the three lines of defence for cybercrime: prevention, detection and response.

To protect against economic crime, particularly cybercrime, organisations may want to consider the fraud triangle of incentive, opportunity and rationalisation. The application of the "opportunity" lens from a fraudster's perspective may assist organisations to identify the control gaps in their operations and assess risk exposures to valuable assets and information.

The cyber world has led to a proliferation of opportunities for fraudsters to access organisations. The rationalisation of a crime varies depending on individual fraudsters, and is difficult for organisations to assess. There may be motivations experienced by employees that are hidden, like gambling problems, therefore this factor is difficult to control.

The following should be considered to protect an organisation against economic crime:

- Attitude of management – having a leadership team that prioritises fraud risk management and fraud awareness to all levels of employees. All staff need to be aware of the risks of the cyber world.
- Due diligence programs – to manage risks associated with staff, contractors, suppliers and agents.
- Having a robust IT security framework.
- Regular fraud risk assessments – consider what someone would value and how they would be able to commit fraud through IT systems.
- Industry and environment monitoring – to enable an organisation to proactively develop responses to current and growing cyber-risks.
- Incident response teams – set up a cyber incident response team that can act and adapt quickly – the organisation may then track, risk assess and deal with an incident as soon as it is spotted anywhere in the organisation.
- Consider your staff's skills and experience – cybercrime is a new and emerging risk and staff may need to be upskilled. Consider collaboration with other departments and industry to share risk assessments and response plans.

Conclusion

PwC's survey results show fraud continues to be a persistent threat in the financial services sector and that organisations need to be vigilant and proactive when fighting economic crime.

Asset misappropriation, cybercrime, accounting fraud and money laundering are the most common types of fraud that financial services organisations reported having fell victim to in the last 12 months. Cybercrime continues to be on the rise as a threat to all industries, likely as a result of more financial transactions occurring electronically with the industry having less 'face' time with customers.

At the same time as being alert to the external dangers of cybercrime and money laundering, our survey shows that financial services organisations cannot afford to ignore the risk of 'traditional frauds', such as asset misappropriation, committed by employees, which accounted for 40% of economic crime reported by financial services respondents in the last 12 months. The risk is where employees have access to assets, information and systems that may present a tempting opportunity to commit fraud where robust controls are not in place.

Reputation continues to be of paramount concern and the impact of negative headlines, regulatory scrutiny and collateral damage cannot be underestimated. It is vital, therefore, that financial services organisations continue to invest in fraud prevention and detection methods and that senior management sets a tone from the top that encourages and rewards ethical behaviour.

Methodology and acknowledgements

The following research techniques were used:

1. Survey of executives in the organisation. The findings in this survey come from executives' reports of their experiences of economic crimes in their organisations. Information was obtained from them on the different types of economic crime, their impact on the organisation (both the financial loss and any collateral damage), the perpetrator of these crimes, what action the organisation took and how they responded to the crime.

2. Questions relating to cybercrime. This survey takes a detailed look at the growing threat of cybercrime and how vulnerable organisations are to it. This focus enables an understanding of what cybercrime really means for organisations.

3. Analysis of trends over time. Since the survey began in 2001 PwC has asked a number of consistent core questions, as well as additional ones that are relevant from time to time, dealing with issues likely to have an impact on organisations around the world. With this historical data to hand, it is possible to identify current themes and chart developments and trends.

Table 1: Breakdown of respondents per territory

Territory	Number of respondents
Switzerland	37
Kenya	36
Middle East	30
UK	30
South Africa	26
Ukraine	26
USA	25
India	21
Romania	21
Russia	21
Indonesia	20
Australia	19
Greece	19
Malaysia	19
Denmark	18
Mexico	18
Belgium	17
New Zealand	17
Ireland	16
Norway	16
Brazil	15
Hungary	15
France	14
Poland	14
Turkey	14
Argentina	13
Italy	13
Czech Republic	12
Japan	11
Slovenia	10
Thailand	10
Netherlands	9
Hong Kong and China	8
Venezuela	8
Canada	7
Ghana	7
Bulgaria	6
Slovakia	6
Spain	6
Ecuador	5
Finland	4
Serbia	4
Bolivia	3
Sweden	3

Table 1: Continued

Territory	Number of respondents
Vietnam	3
Lithuania	3
Austria	2
Germany	2
Cyprus	2
Tunisie	2
Peru	1
Botswana	1
Montenegro	1
Namibia	1
Zambia	1
Total	**688**

Table 2: Breakdown of respondents per function

Function	Number of respondents
Finance	125
Risk management	119
Audit	104
Executive management	88
Compliance	80
Security	47
Advisory/Consultancy	30
Legal	22
Information technology	20
Operations and production	14
Customer service	11
Marketing and sales	9
Human resources	6
Other (please specify)	6
Tax	5
Research and Development	2
Total	**688**

Further information on the survey demographics and definitions of economic crime can be found online at pwc.com.au/crimesurvey

pwc.com.au/crimesurvey

For more information please contact:

New South Wales
Cassandra Michie
Partner, Sydney
+61 (2) 8266 2774
cassandra.michie@au.pwc.com

South Australia
Kim Cheater
Partner, Adelaide
+61 (8) 8218 7407
kim.cheater@au.pwc.com

New South Wales
Malcolm Shackell
Partner, Sydney
+61 (2) 8266 2993
malcolm.shackell@au.pwc.com

Victoria
Michael Cerny
Partner, Melbourne
+61 (3) 8603 6866
michael.cerny@au.pwc.com

New South Wales
Natalie Faulkner
Director, Sydney
+61 (2) 8266 4932
natalie.faulkner@au.pwc.com

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

Queensland
David Harley
Principal, Brisbane
+61 (7) 3257 8307
david.j.harley@au.pwc.com

Western Australia
Cameron Jones
Partner, Perth
+61 (8) 9238 3375
cameron.jones@au.pwc.com

© 2012 PricewaterhouseCoopers. All rights reserved.

PwC refers to the Australian member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

Liability is limited by the Accountant's Scheme under the Professional Standards Legislation.

PwC Australia helps organisations and individuals create the value they're looking for. We're a member of the PwC network of firms in 158 countries with close to 169,000 people. We're 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.au

2287729