www.psrc.pwc.com

Fighting fraud in government

A government and public sector analysis of our 2011 Global Economic Crime Survey

pwc

Contents

Introduction

Continued global economic uncertainty and public sector recession require fresh insights into tackling global economic crime.

Our 2011 survey examines the current fraud landscape, taking a closer look at who is committing fraud and what new types of economic crime are emerging.

We also turn the spotlight on the growing threat of cybercrime. In a world where most individuals and organisations rely upon the Internet and connected technologies, the risk of cyber attacks from criminals anywhere on the planet is higher than ever before. Against a background of rising incidents of data losses and theft, computer viruses and hacking, our survey scrutinised the significance and impact of this new type of economic crime and the way in which it affects organisations worldwide.

Respondents were asked a number of 'core' questions on economic crime in general to enable us to detect long term trends as well as questions specifically relating to cybercrime. We had over 180 respondents from government/state owned enterprises in 36 countries across the globe. A detailed breakdown of the respondents is set out in the appendix to this report.

Please note that some of the percentages may not add up to 100% due to rounding or respondents being able to choose multiple responses.

Experiences of fraud

Our 2009 survey looked at experiences of fraud against a backdrop of worldwide economic turmoil and private sector recession. Since then, governments around the world have been forced to take action to address their faltering economies and often these actions have had a direct impact on those who work for, and with, the public sector.

Given the challenges and pressures placed both on individuals and organisations, it is not surprising that in our 2011 survey we continue to see an increase in the number of frauds committed against the public purse.

Of the government and public sector respondents, 46% reported experiencing one or more incidents of economic crime in the last 12 months, up from 37% in 2009 **(Figure 1)**, and well above the average of 34% across all industries globally **(Figure 2)**.

Figure 1: Experience of economic crime by public sector respondents

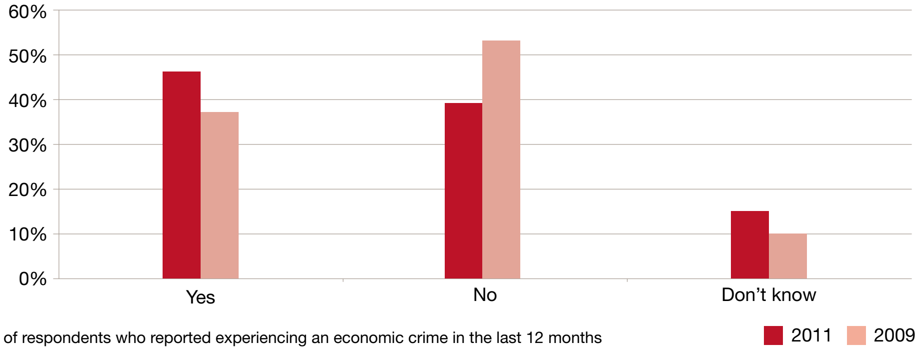
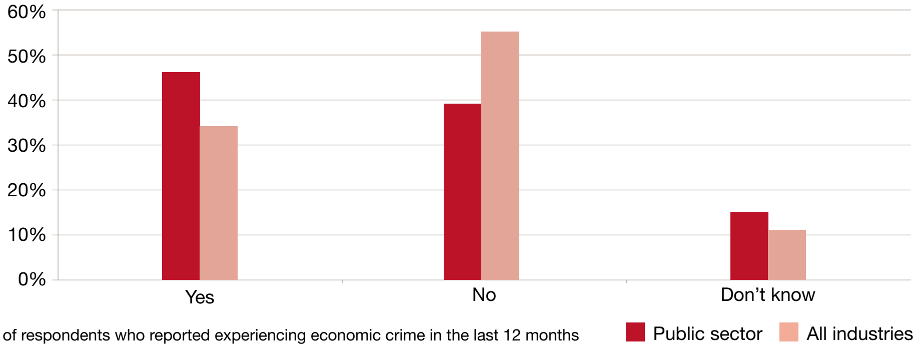


Figure 2: Experience of economic crime by public sector respondents and all industries



It also appears that organisations are suffering a higher number of incidents of fraud than in previous years. The number of respondents who reported experiencing between 11 and 100 incidents in the last twelve months has risen from 18% to 24%, whilst there has been a decrease in the number experiencing less than 10 incidents of fraud in the year from 74% to 67%.

Why is this? One possible reason may be that the impact of cost-saving measures implemented over the last two years by governments with large deficits has led to increased pressure on individuals with limited resources. It may also be that the increased use of technology, including suspicious transaction monitoring and data analytics, is helping to detect more fraud within organisations.

We have seen an increase in the number of incidents of almost all types of fraud, including the 'big three' of asset misappropriation, accounting fraud and bribery and corruption.

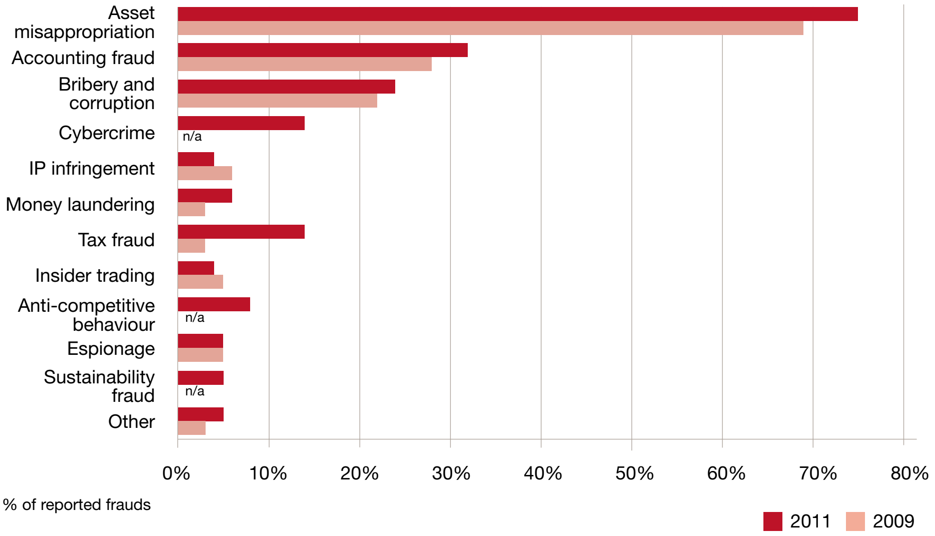
As ever, asset misappropriation is the most common type of fraud, suffered by 75% of respondents **(Figure 3)**. The number of organisations experiencing accounting fraud has risen from 28% in 2009 to 32% in 2011. This is in contrast to the number across all industries, where the number of accounting frauds has decreased in the last two years after a peak in 2009. At the time, the private sector experience seemed indicative of the struggle to survive in difficult economic circumstances, placing pressure on management and staff to meet targets and improve performance.

It seems that we are now seeing a similar pattern of behaviour in the public sector as cuts and redundancies begin to take hold. Companies responded to this growing threat by tightening up their controls and investing in fraud prevention techniques and public sector organisations must follow suit if they are to prevent the number of accounting frauds from increasing in the future.

Cybercrime, previously statistically insignificant, has also emerged as a growing threat, suffered by 14% of respondents.

Cybercrime is not as prevalent in the public sector compared to all sectors. However, the large amounts of data held by public sector organisations and recent high profile attacks on government departments, both domestically and from overseas, it is essential for public sector organisations to address this growing threat upfront.

Figure 3: Types of economic crime reported by public sector respondents



We are seeing the same levels of bribery and corruption in the public sector as across all industries **(Figure 4)**. Public sector organisations also continue to have a high awareness of the possible threat with 37% of respondents believing that their organisation is likely to suffer an incident in the next 12 months.

In recent years, the UK has been leading the charge against unethical behaviour and brought in stringent anti-bribery legislation. Despite the greater awareness of unethical behaviour and concern over the punitive punishments, 89% of public sector organisations in the UK have taken limited or no action to address the demands of the legislation.

We have seen a surprising jump in the number of organisations reporting that they have suffered tax fraud (most often tax evasion committed by external parties) to 14%. This may suggest that people are more likely to commit tax evasion in times of economic uncertainty, as it is often viewed as a victimless crime, or it might be indicative of better methods of detecting tax fraud.

Quite rightly, organisations are telling us that they are concerned not just about the financial impact of a fraud but also about the collateral damage. 35% of respondents from the public sector were very concerned about the impact that a fraudulent act would have on their reputation, compared to 19% across all industries. This highlights the fact that reputation is critical for government and public sector bodies and that building and maintaining trust is an important priority. Respondents also felt that there was a significant impact on relations with regulators (27%) and employee morale (32%) **(Figure 5)**.

Figure 4: Types of economic crime reported by public sector respondents and by all industries

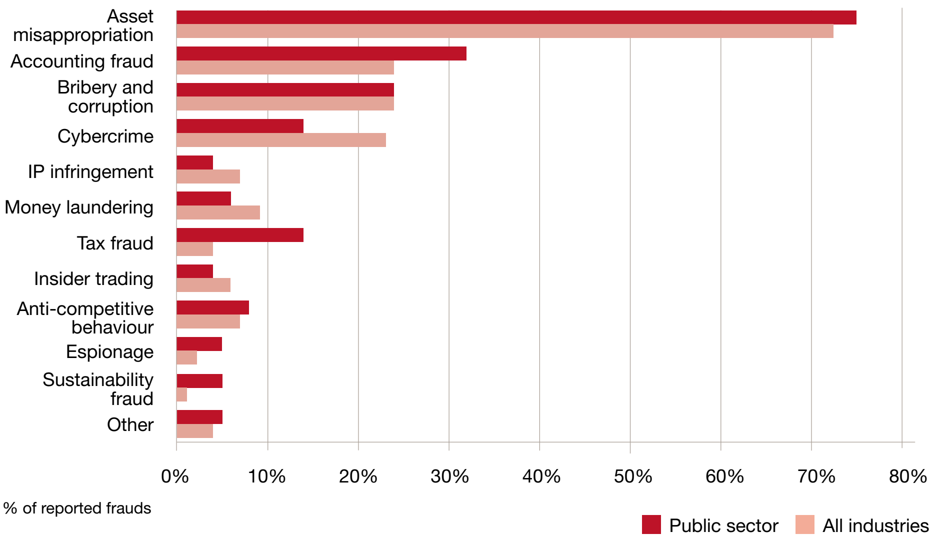
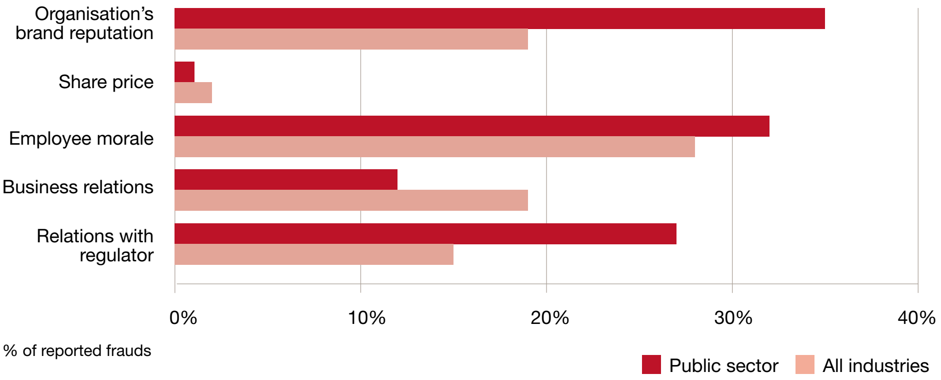


Figure 5: Collateral damage

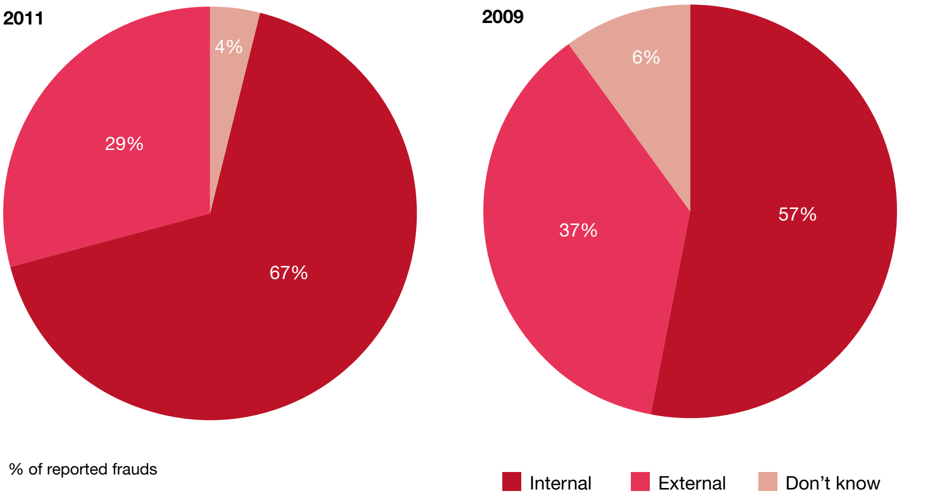


Who is committing fraud?

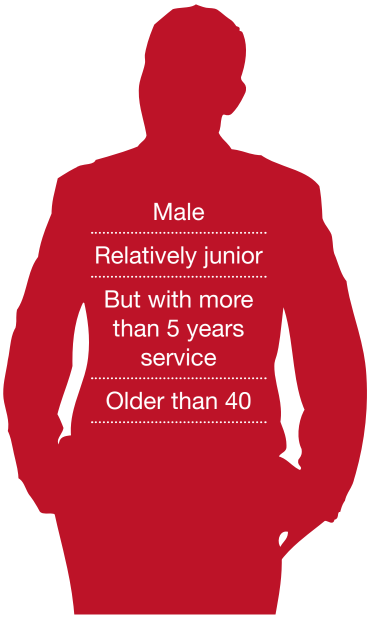
Our survey shows that there has been a big increase in the number of frauds committed by public sector staff; over two-thirds of the economic crimes experienced in the last 12 months have been committed by employees, compared to just over half in 2009 **(Figure 6)**.

Our survey also showed that public sector employers are less likely to dismiss employees for committing fraudulent acts than in other industries. It can be easy for an individual to simply transfer departments, leaving them free to commit their crimes over and over again. If public sector organisations are to adopt a zero tolerance approach to economic crime, they need to consider seriously the actions taken against fraudulent behaviour.

Figure 6: The main perpetrator of the most serious fraud



The profile of a typical internal fraudster



Whilst our survey shows that just under a third of frauds are committed by external parties in 2011, it is imperative that organisations stay alert to new threats. In the last two years, we've seen a big increase in supplier fraud, accounting for 32% of all external frauds, up from 13% in 2009 **(Figure 7)**. Although the public sector seems to have taken action to bring the number of customer and agent frauds down in line with the all industries average, it appears that public organisations are increasingly at risk from their suppliers **(Figure 8)**.

Our clients are telling us the same story – false invoicing schemes and unauthorised changes of supplier details are on the rise and, most worryingly, these types of crimes can often involve some collusion from within an organisation. One of the reasons for the increase in supplier fraud may be that public sector organisations are continuing to maintain business relationships with third parties that have defrauded them, with only a quarter terminating the relationship after the discovery of an incidence of fraud, compared to nearly half in the private sector. This may be unavoidable due to contractual relationships, but it is imperative that organisations in the public sector know with whom they are doing business.

Figure 7: **Perpetrators of external fraud**

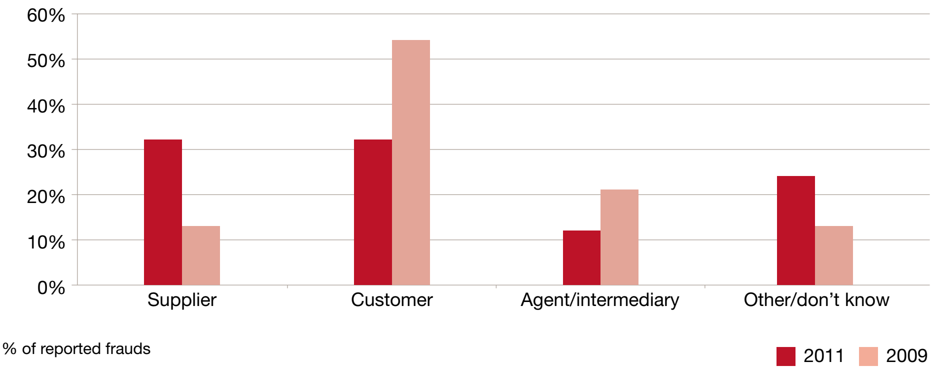
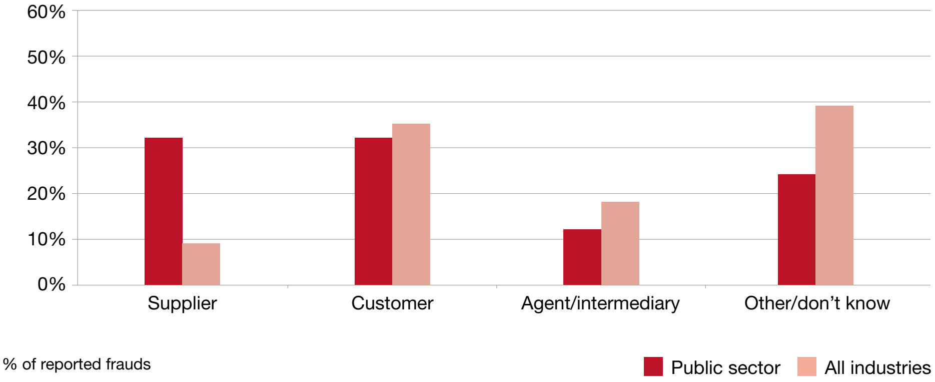


Figure 8: **Perpetrators of external fraud reported by public sector respondents and by all industries**



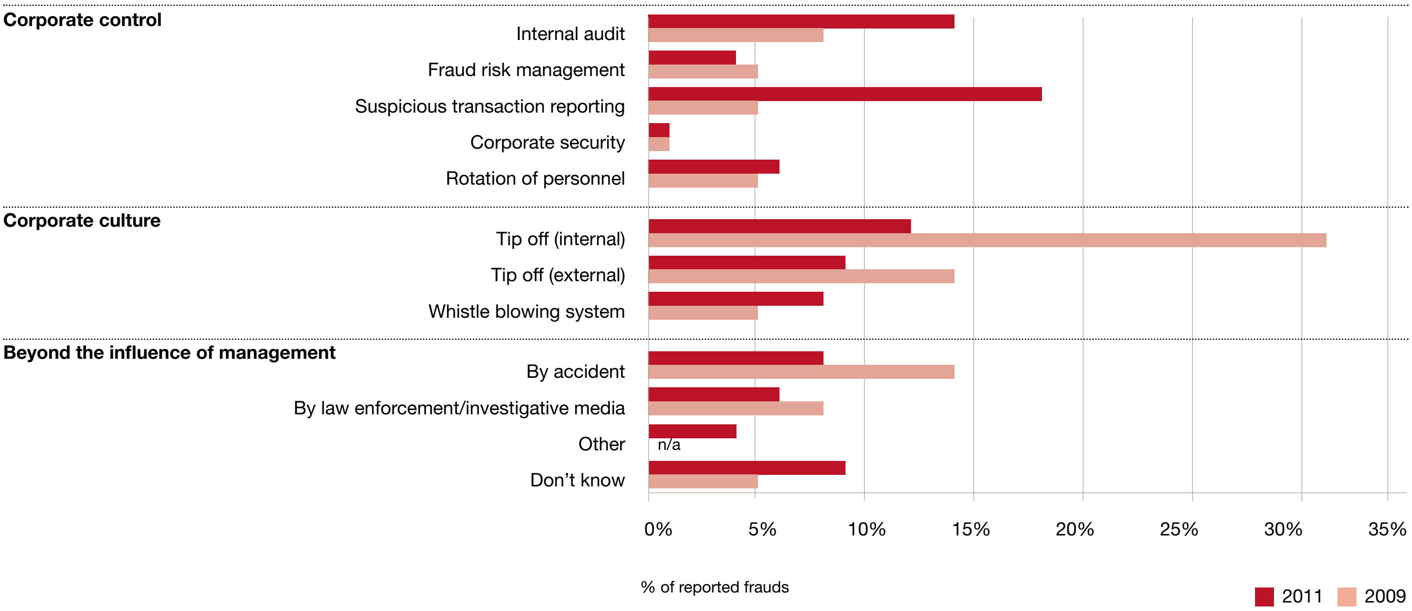
As the public service market becomes more open and suppliers more diverse with more voluntary and private sector organisations become involved in delivering public services, procurement departments will also face a whole raft of new challenges to ensure that the quality and cost-efficiency of the services being delivered are not compromised. This is a particular risk facing the UK at the moment, with the Coalition actively promoting an Open Public Services Agenda.

Supplier frauds still occur because their prevention is often reliant on the vigilance of employees and traditional detective measures can easily miss fraud that is hidden within millions of transactions and thousands of suppliers. Most procurement frauds are conducted over a period of several years and it can be hard for organisations to recoup any losses. It is, however, an area where new technologies, and, in particular, advanced data analytics, can bring real benefits in detecting fraud and identifying clusters of unusual transactions.

Detection and prevention

One reason for the increased reporting of economic crime in the public sector may be the improved performance of internal audit and suspicious transaction monitoring in detecting fraud over the last two years, despite the pressure on resources **(Figure 9)**. Detection of frauds by internal audit teams in the public sector is now on a par with their private sector counterparts.

Figure 9: Detection methods

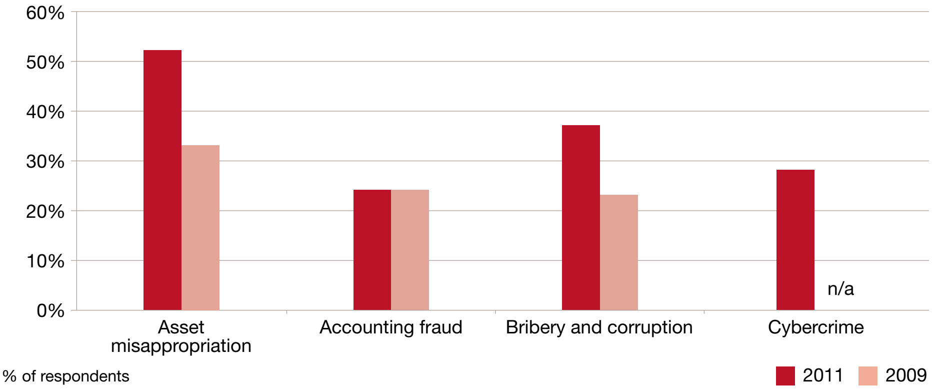


This increase in formal methods of fraud prevention and detection has been offset by a decrease in the number of frauds detected through the 'corporate culture' methods of fraud detection (such as internal and external tip offs). It may be that people are either less willing to inform on their colleagues or that different departments are not talking to each other and acting on the information that they receive. It is, however, encouraging to see a small increase in the number of frauds detected by formal whistle blowing procedures as the investment in training and awareness starts to pay off.

Fraud risk management tools continue, however, to be under utilised in the public sector, with 29% of organisations failing to perform a fraud risk assessment in the last 12 months and only 23% performing them more frequently than annually. In an ever-changing world, fraud risk assessments can quickly become out of date, leaving an organisation vulnerable to new threats. The main reason for not performing assessments is a perceived lack of value (by 43% of respondents) but, when done well, a fraud risk assessment can be a vital tool in your anti-fraud arsenal.

It is even more essential that organisations continue to invest in fraud prevention and detection tools, given that respondents to our survey felt that they were more likely to suffer a fraud in the next twelve months than they did two years ago. Over half felt that they were likely to suffer asset misappropriation and over a third felt that they were likely to suffer an incident of bribery and corruption **(Figure 10)**.

Figure 10: Trends in fraud perception



Five ways to protect your organisation against economic crime

1. Know who you are dealing with – staff, suppliers, partners and agents.
2. Align IT, internal audit and the board in the fight against economic crime.
3. Conduct regular fraud risk assessments.
4. Consider whether the actions taken against internal and external fraudsters are sufficient and if you really have a zero tolerance environment.
5. Set the tone from the top and instil a cyber risk aware culture throughout your organisation.

Cybercrime

> ***"Cybercrime – 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's only a cybercrime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one.*** [1] ***"***

In our previous global economic crime surveys, when we asked respondents if they had experienced cybercrime, the response levels were very low and statistically insignificant. Hence, in the past we have combined the results with 'other types of fraud' in our survey reports. Given the increasing concerns around cyber threats, we focussed on cybercrime this year and reintroduced it as a separate category of fraud, asking the respondents whether they had been affected by any incidents in the last 12 months.

This year, 14% of respondents from the public sector reported having experienced a cybercrime attack in the past 12 months **(see Figure 3)**. Whilst this is less than across other industries (23%), government and public sector organisations cannot ignore the risks, especially considering the large amounts of both personal and confidential data held – they are a prime target for attack.

As the threat of cybercrime grows, more and more organisations are waking up to the risks not least because of the heightened media interest in cyber attacks. Hardly a week goes by without a report in the press about people, organisations or governments coming under attack and having information stolen or their financial security compromised by criminals.

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

Our survey shows that people are aware of the growing threat, with 28% of respondents thinking that they are likely to suffer a cybercrime attack in the next 12 months and over 40% of respondents saying that they perceive the risk of cybercrime to be on the rise **(Figure 11)**.

Although cybercrime is usually thought to be perpetrated by external parties, the majority of respondents to our survey felt that the threat from inside an organisation was just as strong. It is not surprising that the IT department is perceived to pose the highest risk, closely followed by Physical Security, Operations and Finance. It is, however, important to ensure that all departments are sufficiently protected, including those viewed as low risk such as HR and Legal, especially given the confidential nature of information to which they have access.

Again, damage to an organisation's reputation and the public sector's potential loss of data are high on the agenda when it comes to the impact of cyber attacks. This is hardly surprising given recent high profile cases of data security breaches **(Figure 12)**. It is therefore vital that organisations continue to ensure they are investing in cybercrime prevention and detection.

There is no generally agreed definition of cybercrime, which can make it hard to detect and investigate cybercrimes, and a general lack of understanding may give fraudsters an opportunity to exploit gaps in control. Cybercrimes can easily be committed by a perpetrator in a different location or jurisdiction, which can make identifying and bringing them to justice far more difficult.

Figure 11: **Perception of the risk of cybercrime**

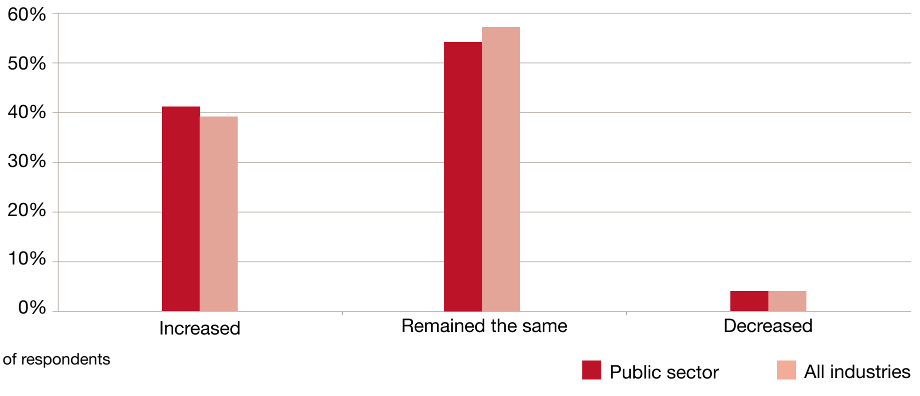
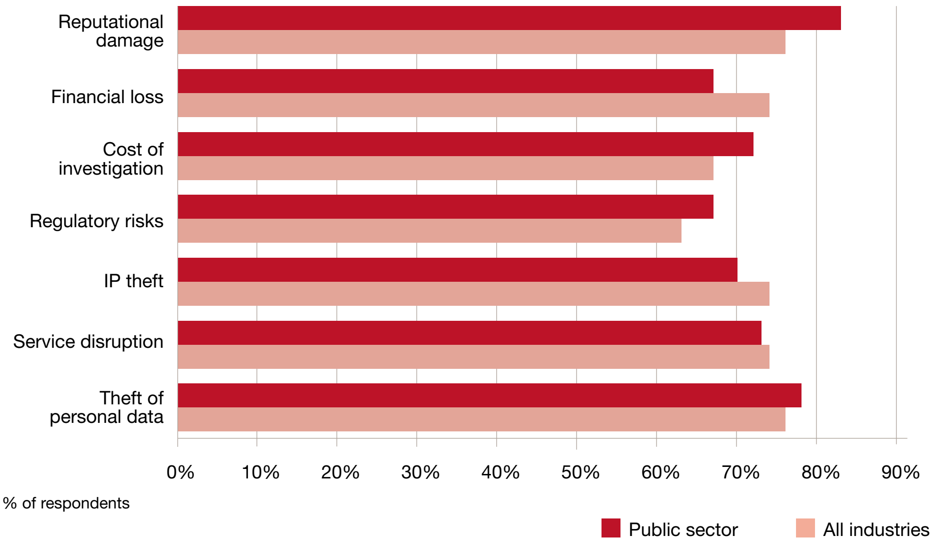


Figure 12: **Impact of cyber attacks**



Although over half of public sector organisations have in-house capabilities to detect cybercrime, most don't have the resources to investigate it and are reliant on external investigators. Nearly half of public sector organisations surveyed don't have, or are not aware of having, emergency shut down procedures in place, which is concerning given that the first few hours of a cyber attack are crucial. When it comes to safeguarding their reputation, over half of the organisations surveyed don't have, or are not aware of having, a media plan in place. Given the importance that respondents to our survey placed on their reputations and the awareness of the impact that a potential attack could have, this statistic is somewhat surprising and should be a cause for concern.

Nearly half of the respondents felt that the overall responsibility for cybercrime risks lies with the Chief Information Officer (CIO), with only a fifth believing that responsibility lies at board level. Like the overall anti-fraud programme, we expect that the CEO and the board would take ultimate ownership of the programme and it is important that cybercrime risks feature as one of the agenda items discussed with the CEO and the board on a regular basis.

The statistics indicate that the most senior people within organisations are not placing enough emphasis on the importance of managing the real threats that cybercrime frauds present to their organisations, with nearly half of boards not reviewing the threat more frequently than annually.

It is vital that executives accept more responsibility for managing and mitigating cybercrime risks and set an appropriate tone at the top. Leadership by a management team which instils a cyber risk-aware culture and ensures that all departments are aligned in the fight against fraud is key in order to succeed in today's environment.

What actions should organisations take to defend themselves against cyber attacks?

- **Get senior management involved –** senior management and the board need to be aware of the risks and opportunities of the cyber world.
- **Look at how prepared the organisation is for cybercrime –** unlike traditional economic crime, cybercrime is fast-paced and new risks emerge all the time, which means the organisation needs to adapt its procedures continually to reflect these.
- **Be aware of the current and emerging cyber environment –** only then can the organisation make well-informed decisions and do the right things at the right times.
- **Set up a cyber incident response team that can act and adapt quickly –** the organisation can then track, risk-assess and deal with an incident as soon as it is spotted anywhere in the business.
- **Recruit people with the relevant skills and experience –** they can pass this knowledge on to everyone else, helping to create a 'cyber-aware' organisation that can protect itself better.
- **Take a tougher and clearer stance on cybercrime** – the organisation should show it means business by taking legal action against cyber criminals and announcing what it's doing about threats and incidents.

For more information on dealing with cyber threats, see our report
'Delusions of safety? The Cyber Savvy CEO: Getting to grips with today's growing cyber-threats'

Conclusion

Our survey results show that fraud continues to be a persistent threat in the public sector and that organisations need to be vigilant and proactive when fighting economic crime.

Asset misappropriation, accounting fraud and bribery and corruption remain the top three frauds that our respondents suffered in the last 12 months. But 'new' types of fraud are emerging and, in particular, cybercrime. Whilst in our survey findings cybercrime is not yet as prevalent in the public sector compared to all sectors, the risk to government organisations is only going to increase with new technologies and a changing work environment.

At the same time as being alert to the dangers of cybercrime, our survey shows that organisations cannot afford to ignore the risk of 'traditional frauds'. In particular, we are seeing large numbers of frauds committed by an organisation's own employees – these are the people that organisations trust, that potentially have access to systems and to significant amounts of data.

The changing ways in which governments are doing business also present fraudsters with potential opportunities. We have seen a big rise in the number of procurement frauds in the last twelve months and our experience tells us that there are likely to be many more rogue transactions hidden in accounts payable systems.

Reputation continues to be of paramount concern to public sector organisations and the negative headlines, administrative burden and collateral damage that an incident of economic crime brings cannot be underestimated. It is vital, therefore, that organisations continue to ensure that they are investing in fraud prevention and detection methods and that senior management is setting a tone from the top that encourages, and rewards, ethical behaviour.

Appendix: Methodology and acknowledgements

About the survey

The 2011 Global Economic Crime Survey was completed by 184 respondents from the public sector from 36 countries. Of the total number of respondents, 36% were senior executives of their respective organisations.

We used the following research techniques:

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. We obtained information 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 us to understand what cybercrime really means for organisations.

3. **Analysis of trends over time.** Since we started doing these surveys in 2001, we have asked a number of core questions, and extra 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, we can see current themes, chart developments, and find trends.

Figure 13: Participating territory counts for public sector respondents

Territory	Number of respondents
Argentina	7
Australia	16
Belgium	11
Brazil	1
Bulgaria	1
Canada	1
Czech Republic	3
Denmark	6
Finland	1
Ghana	1
Greece	4
Hungary	1
Indonesia	2
Ireland	4
Italy	3
Kenya	15
Liberia	3
Malaysia	6
Middle East	10
Netherlands	1
New Zealand	19
Norway	2
Peru	1
Russia	1
Singapore	1
Slovakia	5
Slovenia	2
South Africa	12
Spain	7
Sweden	1
Switzerland	3
Thailand	1
UK	27
USA	2
Venezuela	2
Sudan	1
Total	184

Figure 14: Function (main responsibility) of public sector participants in the organisation

Function	Number of respondents
Audit	57
Advisory/Consultancy	8
Compliance	11
Customer service	1
Executive management	27
Finance	30
Human resources	4
Information technology	5
Legal	7
Marketing and sales	1
Operations and production	2
Procurement	1
Research and Development	3
Risk management	8
Security	9
Tax	2
Other	8
Total	184

Contacts

Ian Elliott
+44 20 7213 1640
ian.elliott@uk.pwc.com

Ian Elliott is a Partner in the PwC Forensic Services group and is the leader of the Forensic Services Government and Public Sector team in the UK. Ian has a broad range of forensic experience, with particular expertise in non-financial investigations and the investigation of fraud and accounting irregularities.

Tony Parton
+44 20 7213 4068
tony.d.parton@uk.pwc.com

Tony is the Leader of the firm's Global Economic Crime Survey. He is an investigations partner in the Forensic Services practice and has been involved in financial and non-financial investigations for over 30 years, with cases covering a large range of industry sectors and geographies. He was the firm's Forensic leader in Asia Pacific until 2006 when he returned to the UK.

About PwC

At PwC we focus on three things for government and the public sector: assurance, tax and advisory services. Working together with our clients, we look for answers on how to increase efficiencies while improving quality and outcomes, and help to develop solutions that add value and are practical to implement.

As well as bringing our insight and expertise to this sector, we contribute our thinking and experience to the public policy debate through our Public Sector Research Centre. To join this free online community, go to **www.psrc.pwc.com** and register today for our research and analysis.

Join the debate. www.psrc.pwc.com

The Public Sector Research Centre is PwC’s online community for insight and research into the most pressing issues and challenges facing government and public sector organisations, today and in the future.

The PSRC enables the collaborative exchange of ideas between policy makers, opinion formers, market experts, academics and practitioners internationally.

To register for this free resource please visit www.psrc.pwc.com

In this document, “PwC” refers to PricewaterhouseCoopers LLP, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity. This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

www.psrc.pwc.com