

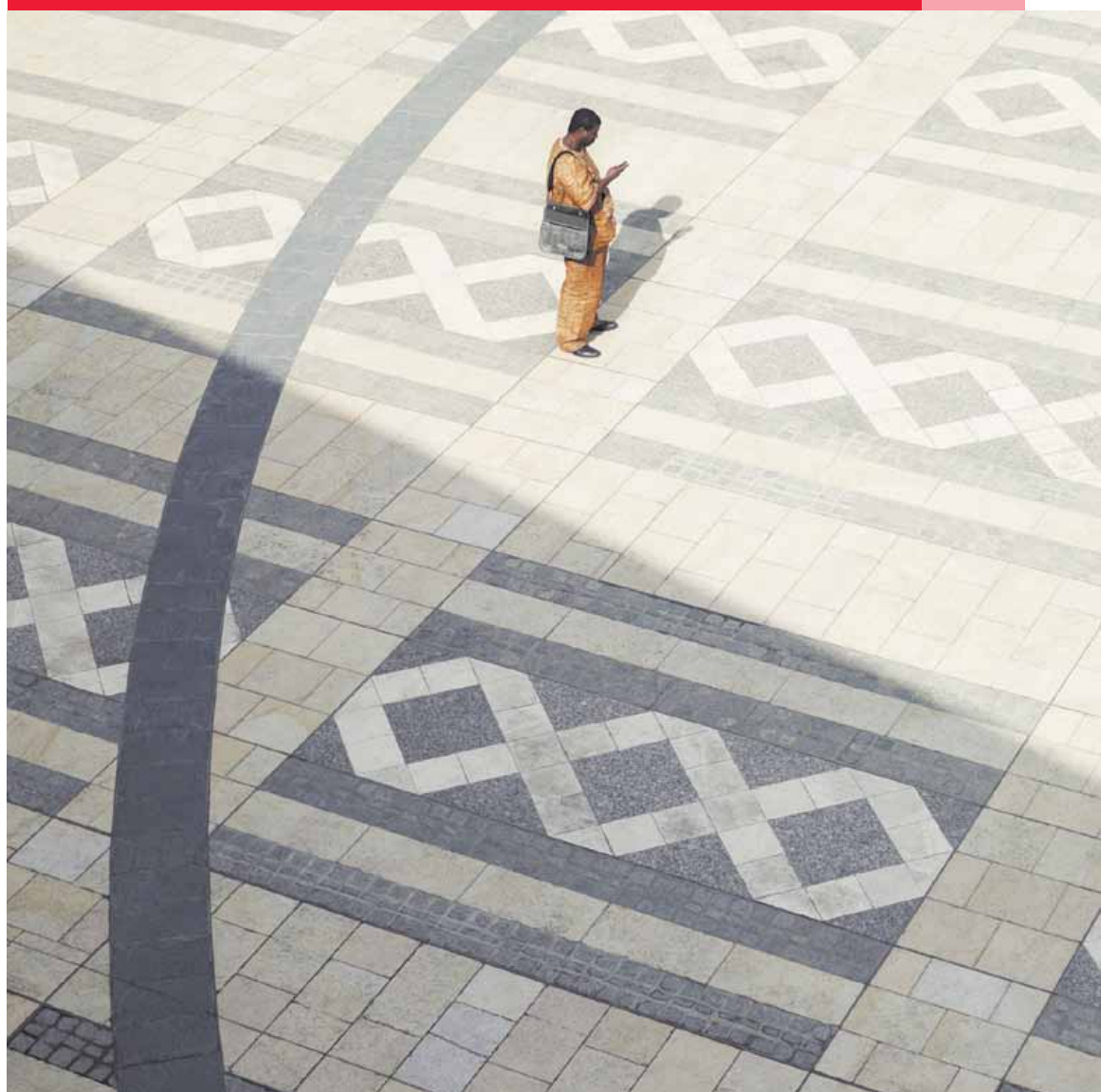
# *The Global Economic Crime Survey*

## Cybercrime in the spotlight

Canadian Supplement

*Almost 4,000 respondents  
from organizations in 78  
countries provide a global  
picture of economic crimes.*

November 2011





---

# *Contents*

Introduction	2
Cybercrime in the spotlight	3
Fraud, the fraudster and the defrauded	7
How PwC can help	15
Who to call	16

---

# Introduction

PwC's Global Economic Crime Survey 2011 continues to provide insight into the state of economic crime worldwide. Although we are slowly recovering from the global economic downturn which had a significant impact on our 2009 survey results, it is clear from the results this year that stakeholders must remain diligent about fraud risk management, as no organization or industry is immune.

*The results of our 2011 survey show that 32% of Canadian organizations surveyed reported being victims of economic crime during the previous 12 months.*

Our 2011 survey turns a spotlight on the growing threat of cybercrime in a world that relies on the internet and connected technologies, which can leave organizations susceptible to the risk of attack by criminals from across the globe. The survey looks at the significance and impact of cybercrime and the way in which it affects businesses worldwide.

The results of our 2011 survey show that 32% of Canadian organizations surveyed (34% globally) reported being victims of economic crime during the previous 12 months, which represents a decrease of 24% from our 2009 survey. Almost 1 in 4 of the organizations who experienced economic crime globally stated that they had been subject to cybercrime in the past 12 months, and 39% of global respondents noted an increasing awareness of cybercrime threats. This year's Canadian report is divided into two key sections:

- **Cybercrime** – awareness of the crime, how it impacts organizations, and what actions are taken to address the risks; and
- **Fraud, the fraudster and the defrauded** – the types of fraud committed, who is committing them, how they are detected and actions taken by organizations in response.

*Cybercrime is ranked as one of the top four economic crimes.*

## **Cybercrime in the spotlight**

For the purposes of our survey questionnaire, we defined cybercrime as:

*“An economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing<sup>1</sup> and pharming<sup>2</sup>, and stealing personal information like bank account details. It’s only cybercrime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one.”*

1 Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

2 Pharming is a hacker’s attack aiming to redirect a website’s traffic to another, bogus website.

Is cybercrime simply a means by which a fraudster commits the illegal act, or is it an economic crime in its own right? Should organizations take specific measures, over and above other fraud prevention and detection methods, to manage this risk? Our survey takes a closer look at these issues. Key objectives of the 2011 survey relating to cybercrime were to understand:

- Whether the incidence of cybercrime related fraud has become more prevalent in recent years;
- Where the risks of cybercrime related frauds are coming from; and
- What steps organizations are taking to prevent and detect this type of fraud.

### **Cybercrime: the next wave**

According to our 2011 survey, cybercrime is ranked as one of the top four economic crimes, behind asset misappropriation, accounting fraud, bribery and corruption. Some of the possible reasons that cybercrime has emerged as a top type of economic crime could be:

- Increased media attention around recent cybercrime cases leading to a heightened awareness of this type of economic crime. Organizations may have put additional controls in place to detect and report this form of economic crime; or
- Respondents may have re-classified some of the more traditional types of crime as cybercrime, since it was offered as a separate category for the first time; or
- Increased focus from regulators; or
- Advancements in technology have made it easier to commit cybercrimes.

### **Is it really just an external threat?**

In the last 12 months, 38% of Canadian organizations (39% globally) believe their perception of the risks of cybercrime to their organization have increased. This illustrates the growing significance of cybercrime around the world and the need to remain aware of new and emerging cybercrime threats.

More than half (57%) of Canadian respondents (46% globally) believe the greatest cybercrime threat to their organization is cybercrime by an external person to the organization, while 9% (13% globally) believe such threats are internal, and 19% (29% globally) believe the greatest threats are both internal and external.

## Canadian respondents indicated their greatest concern related to cybercrime was the theft or loss of personal identifiable information.

### Where does the threat come from?

Of Canadian respondents who believe the greatest cybercrime threats are external, 53% (51% globally) indicated that the threats are coming from both within and outside of their own country. The top five countries reported globally are set out in Figure 1 below.

**Figure 1: Top 5 countries reported globally as the likely home of cybercrime**

(Alphabetical order)

Hong Kong (and China)

India

Nigeria

Russia

USA

This highlights the global nature of cybercrime and the fact that traditional geographic borders do not provide protection.

Of respondents who believe the greatest cybercrime threat is internal, the area within the organization of most concern is the Information Technology (IT) department, with 53% of global respondents indicating that this area is high risk.

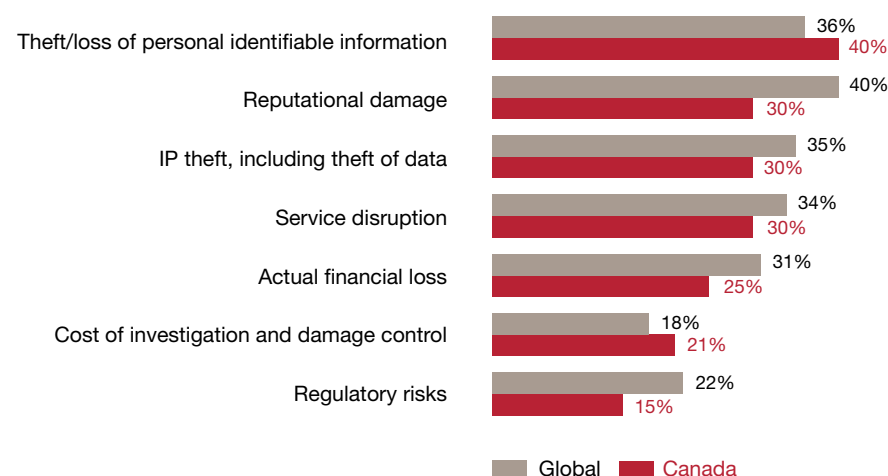
### What are organizations really worried about?

Figure 2 demonstrates that Canadian respondents indicated their greatest concerns related to cybercrime were the theft or loss of personal identifiable information followed by reputational damage, intellectual property theft and service disruption. Of least concern were regulatory risks and the cost of the investigation and damage control, which may indicate that organizations recognize the significance of protection against, and investigation of, cybercrime incidents.

### Do you know what's out there?

When it comes to preventing and detecting cybercrime, 60% of both Canadian and global respondents believe they have in house capabilities to prevent and detect cybercrime, suggesting a level of confidence in the organization's IT infrastructure. It is important that organizations remain focussed on upgrading or transforming their cybercrime prevention capabilities to deal with new risks as they emerge. However, only 36% (40% globally) of respondents believe they

**Figure 2: Concerns about cybercrime (2011)**





*70% of Canadian respondents stated that their organization does not monitor employees' use of social media sites (e.g. Facebook, Twitter).*

have in house capabilities to investigate cybercrime, and 47% (39% globally) responded that they have access to forensic technology investigators. It is vital that organizations create a cyber incident response team to establish effective response mechanisms and policies, and ensure any cybercrime threat can be dealt with effectively, whether it be in house or through the use of external experts.

In the event of a cybercrime incident, 53% (65% globally) indicated that they consult with experts who are external to the firm, and 51% of both Canadian and global respondents inform law enforcement of the incident.

Of global respondents who indicated that they consult external experts, 40% indicated that they engage experts routinely or in a proactive manner, while 48% consult experts only once an incident has occurred, or in a more reactive manner.

### **Keeping an eye on social media sites**

70% of Canadian respondents (60% globally) stated that their organization does not monitor employees' use of social media sites (e.g. Facebook, Twitter, etc.). Of respondents who are monitoring social media use, the majority are taking actions such as:

- Monitoring internal or external electronic traffic, including web-based activity;
- Ensuring that employee contracts refer to a code of conduct; and
- Initiating training programs for employees regarding appropriate internet use.

As employee use of social media grows, it is becoming increasingly important for organizations to consider:

- Reduction in employee productivity;
- Inappropriate use of the internet by employees (e.g. gambling, pornography, etc.);
- Leakage of confidential information;
- Exposure of infrastructure to cyber attacks; and
- Potential for litigation.

### **Reducing the risks**

49% percent of Canadian respondents (42% globally) indicated that they had not received cyber security related awareness training over the past 12 months. In order to address the growing threat of cybercrime, it is essential that the organization has a clear understanding of the current and emerging cyber environment, and that management understands the risks and opportunities of the cyber world. While the most common type of training was email announcements/posters/banners at 42% (40% globally), and computer based training at 17% (22% globally), the majority of respondents identified these methods as the least effective, instead ranking human based events such as presentations, team meetings and workshops as the most effective methods of training.

**49% of Canadian respondents indicated that they had not received cyber security related awareness training over the past 12 months.**

### **Who's ultimately responsible for dealing with cybercrime inside an organization?**

When asked where the ownership and overall responsibility for preventing cybercrime resides within an organization, the majority of respondents indicated that the senior members of the organization were responsible, with 43% (54% globally) of respondents indicating the Chief Information Officer, and 34% (21% globally) indicating that it resided with the Chief Executive Officer (CEO) and the board of directors.

When it comes to reviewing the risks that cybercrime presents to their organization, 21% (15% globally) of respondents indicated senior executives and board members review the risks that cybercrime presents to their organization on an annual basis, while 23% of both Canadian and global respondents review the risks on an ad-hoc basis. This finding supports the more “reactive culture” indicated in the survey results. It is critical that those charged with governance related to cybercrime take a more proactive approach to the threat of cybercrime, task it as a priority, and seek assistance to evaluate and reinforce cybercrime detection and prevention as one of the key components of their anti-fraud regime.

### **What actions should organizations take to defend themselves against cyber security attacks?**

- **Get the CEO involved** – the CEO and the board of directors need to be aware of cyber threats and understand the risks and opportunities of the cyber world.
- **Reassess** – reassess the security function and preparedness of the organization should a cybercrime occur. Unlike traditional economic crimes, cybercrime is fast paced given the advancing technology, with new risks emerging, which means an organization needs to adapt its procedures continually.
- **Build awareness** – organizations need to have a clear awareness of the current and emerging cyber environment. With this in place, well informed and prioritized decisions and actions can be taken.

- **Create a cyber incident response team** – which needs to act with speed and agility. A well-functioning cyber response team means once an incident is spotted anywhere in the business, it will be tracked, risk-assessed, escalated and triaged.
- **Educate all employees** – an organization needs to embed a ‘cyber awareness’ culture and the relevant policies, protocols and procedures must be communicated to all employees.
- **Take a more active and transparent stance towards cybercrime** – take action by pursuing cybercrime perpetrators through legal means and communicate more publicly the actions the organization is taking regarding the threats, incidents and responses.

Percent of Canadian respondents indicating the Chief Information Officer is responsible for cybercrime prevention

**43%**

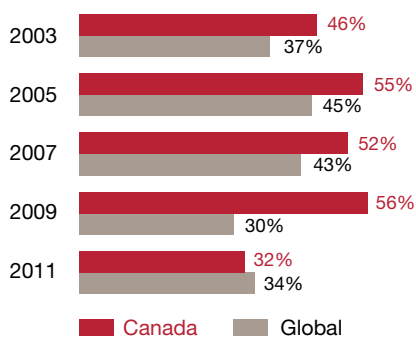
Percent of Canadian respondents indicating the Chief Executive Officer is responsible for cybercrime prevention

**34%**

Although Canada has historically reported higher instances of economic crime than our global counterparts, the 2011 results show that we are now reporting fewer instances.

## Fraud, the fraudster and the defrauded

**Figure 3: Organizations reporting fraud (2003-2011)**



Experience of economic crime in the past 12 months for 2011 and 2009, and past two years for 2007, 2005 and 2003

### Do organizations know what they're facing?

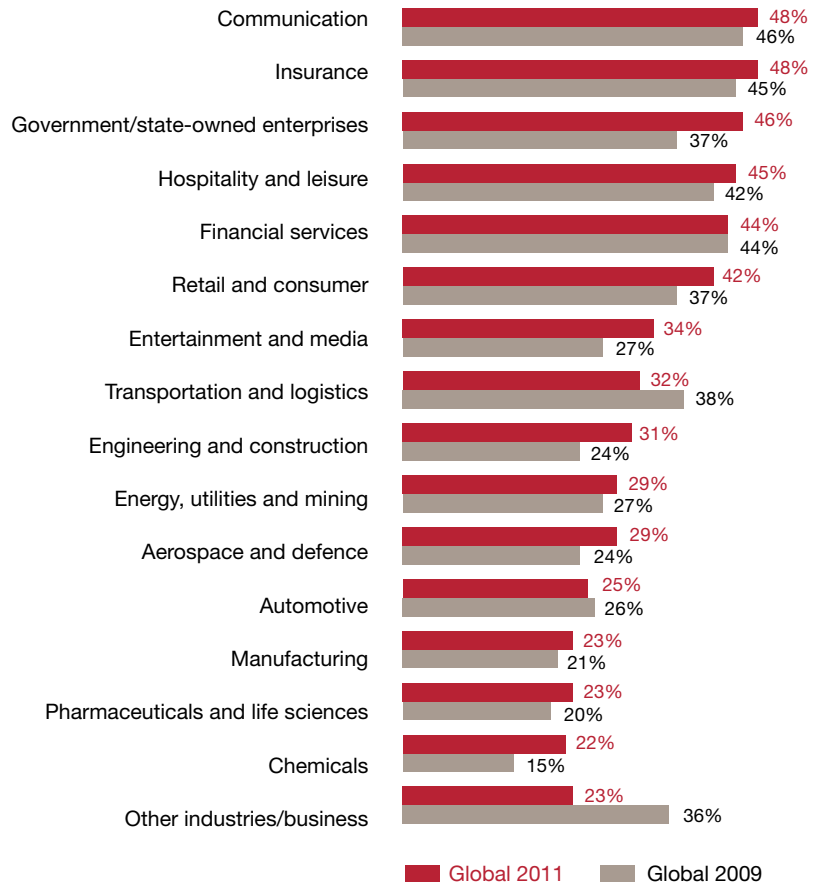
The results of our 2011 survey show that 32% of Canadian organizations (34% globally) reported being victims of economic crime during the previous 12 months. This is a decrease of 24% from the 2009 survey results. Figure 3 illustrates the percentage of companies from both a Canadian and global perspective reporting fraud from 2003 to 2011.

Although Canada has historically reported higher instances of economic crime than our global counterparts, the 2011 results show that we are now reporting fewer instances. This decrease may be due to Canadian organizations being more diligent in the

implementation of robust anti-fraud regimes, including fraud risk assessments and whistle-blowing systems, causing an increased awareness of fraud, a decrease in opportunities to commit fraud, and an increase in the organization's ability to detect fraud. The decrease in reported frauds may also be the result of the Canadian economy being stronger over the past two years compared to global counterparts, resulting in an environment with less visibility of fraud, which normally arises during a downturn. The decrease in reported instances may also indicate that sophisticated frauds, such as cybercrime or collusion between parties, are being committed, which are inherently more difficult to detect.



**Figure 4: Fraud per industry sector (% reported frauds)**



**Is any particular sector experiencing high levels of fraud?**

Economic crime is present in all sectors globally, as illustrated in the comparison with our 2009 survey results in Figure 4.

The communication and insurance sectors remain at the top of the list with respect to the number of reported fraud incidents; however, we note that fraud in the government sector has increased by 9% since our 2009 survey, making this sector one of the top five targets for economic crime.



### So what types of economic crime are we talking about?

Economic crime can take many different forms. Figure 5 shows the different types of economic crime experienced by global respondents who reported experiencing economic crime over the past 12 months.

The most common type of fraud encountered by organizations surveyed globally was asset misappropriation, which is defined as the theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit. This was followed by accounting fraud, and bribery and corruption. Asset misappropriation was identified by 72% of organizations globally that were victims of economic crime in the past 12 months, which represents a 5% increase from our 2009 survey results.

A factor that makes asset misappropriation more common than other types of fraud is that it can be relatively unsophisticated, making it easier to commit by people at many levels of authority in an organization.

24% of organizations surveyed globally experienced accounting fraud, which includes accounting manipulations, fraudulent borrowing/raising of finance, fraudulent applications for credit, and unauthorized transactions/rogue trading, which represents a 14% decrease from our 2009 survey. Factors that may have had an impact on this change include:

**Figure 5: Types of economic crime † ††**



† Note: multiple types of economic crime were experienced by many of the respondents.

†† In our previous Economic Crime Surveys, when we asked respondents if they had experienced cybercrime, the response levels were very low and statistically insignificant. Hence, we combined the results with 'other types of fraud' in our past survey reports. Given the increasing concerns around cybercrime, we focussed on cybercrime this year and reintroduced it in the types of fraud question, asking respondents whether they had experienced cybercrime in the past 12 months.

1. Organizations may have put tighter controls in place to deter the perpetrator;
2. Our 2009 survey saw a sharp rise in accounting frauds from the 2007 survey, and this could have been the result of organizations struggling to survive in difficult times and management feeling the pressure to manipulate financial statements. It may be that there is less incentive and/or pressure prevalent today.
3. Organizations might not be detecting economic crime accurately due to reductions in "fraud prevention" headcount within organizations globally since our last survey.

A quarter of those who reported economic crime globally suffered from bribery and corruption. Bribery and corruption is a form of economic crime which had consistently increased in our surveys up to 2007, however since 2009 our surveys have shown a slight decline in reported cases. Organizations may be reluctant to report this form of economic crime because of increased media attention, regulatory and criminal enforcement, including significant penalties in recent years.

Canada has publically shown a commitment to addressing bribery and corruption with the Corruption of Foreign Public Officials Act ("CFPOA"). As Canadian organizations expand into emerging markets, it is important for them to understand the CFPOA and how it governs their interactions with foreign public officials.

*13% of respondents indicated that in the last 12 months, their organization chose not to enter a new market or declined to pursue a new business opportunity due to corruption risks.*

13% of global respondents indicated that in the last 12 months, their organization chose not to enter a new market or declined to pursue a new business opportunity due to corruption risks. This finding may indicate an awareness of the implication of foreign corruption and the impact corruption could have on an organization's reputation and plans for growth and expansion. It will be interesting to see whether this reluctance to enter new markets due to corruption will persist in future surveys as organizations continue to expand globally.

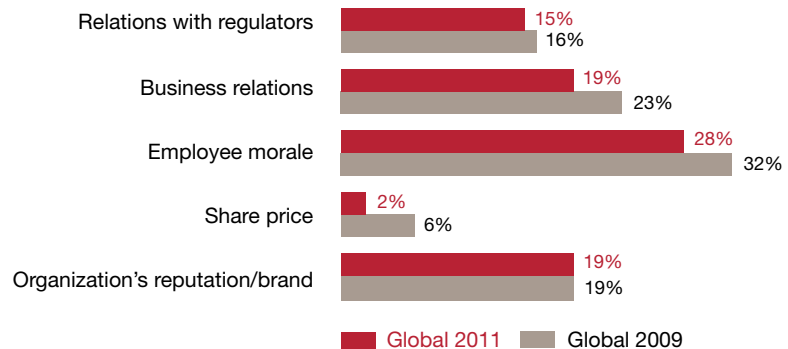
Cybercrime is a new category of economic crime which was included in the 2011 survey results. The results of our survey show that cybercrime has impacted 23% of global respondents.

#### ***How much does fraud cost, and what's the collateral damage?***

While it is difficult to quantify the financial impact of economic crime, of global respondents who had experienced economic crime in the past 12 months, almost 1 in 10 reported losses of more than US\$5 million. Almost 1 in 5 of those who suffered from bribery and corruption lost more than US\$5 million on average.

In addition to direct losses, our survey also covered collateral damage suffered by organizations with respect to brand/reputation, share price, employee morale, business relations and relations with regulators. Figure 6 provides detail on organizations reporting significant collateral damage worldwide.

**Figure 6: Collateral damage**



The impact of indirect losses related to fraud can be difficult to quantify. One example is employee morale, which was identified by 28% of global respondents as being significantly impacted as a result of an economic crime. Experience has shown that negative employee morale can result in additional losses for an organization because it can lead to reduced performance and future detrimental behaviour. The organization's reputation has been significantly affected by economic crime 19% of the time for global respondents in both 2009 and 2011. Since an organization's reputation is often closely tied to its competitive advantage, and can take years to repair once it has been damaged, the impact of collateral damage should not be underestimated.

*Of respondents who had experienced economic crime in the past 12 months, almost 1 in 10 reported losses of more than US\$5 million.*

**Who's committing fraud?**

According to our 2011 survey results, 56% of organizations globally that were victims of economic crime in the last 12 months said that the fraud was committed by an internal party (employee) of the organization and 40% identified the main perpetrator as an external party (Figure 7).

Given the increasing prevalence of internal fraudsters, there is a need for organizations to improve internal controls and demonstrate a heightened awareness around fraudster profiles. Based on the results of our 2011 global survey, the typical internal fraudster was male (77%), between 31 and 40 years old (43%), a first degree graduate (37%) and had been employed by the organization between three and five years (30%).

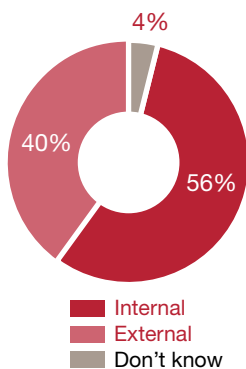
Figure 8 shows that for organizations surveyed globally in 2011 that experienced economic crime as the result of employee actions, 39% of the perpetrators were classified as junior staff, 41% as middle management, and 18% as senior management.

It is important to note that while the results of our global survey show that economic crimes committed by senior management were fewer than employees at more junior levels, these crimes tend to be more sophisticated and larger in dollar value. As sophisticated frauds are more difficult to detect, this could also be a factor as to why economic crimes committed by senior management were not identified nearly as often as those committed by middle management or junior staff.

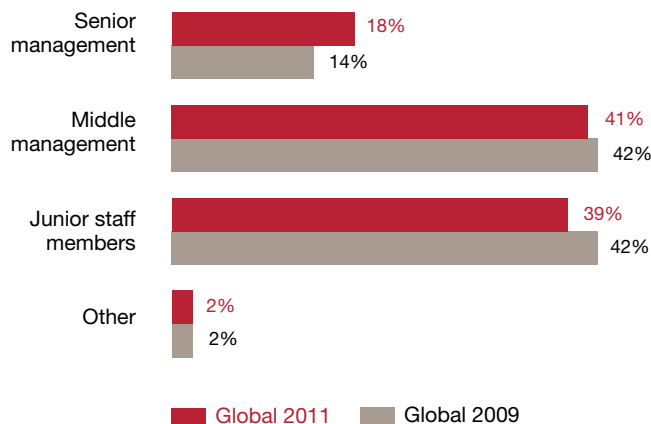
For organizations globally that experienced economic crime primarily by external parties, 35% identified customers as the most common perpetrators, 18% indicated agents or intermediaries as the perpetrators, and 17% indicated they did not know who the perpetrator was.

*56% of organizations that were victims of economic crime in the past 12 months said that the fraud was committed by an internal party.*

**Figure 7: Fraudsters' relation to the organization (Global 2011)**



**Figure 8: Profile of internal fraudsters**



**What do organizations do with the fraudster?**

The 2011 global responses for disciplinary action against internal perpetrators showed that in the majority of cases (77%) the perpetrators were dismissed. In 44% of the incidents, law enforcement was informed, while in 40% of the incidents, civil action was taken.

The need for robust and proper investigation protocols for evidence gathering is increased, and will help an organization maximize recoveries and potentially avoid future losses.

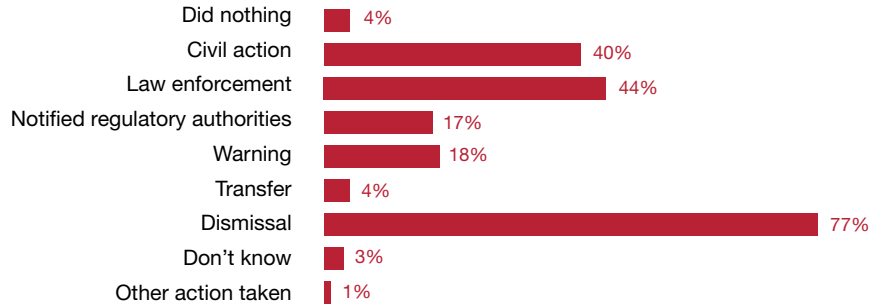
**How do organizations detect fraud?**

Fraud detection refers to the methods employed by organizations to determine if economic crime has been committed. Figure 10 sets out these various detection methods.

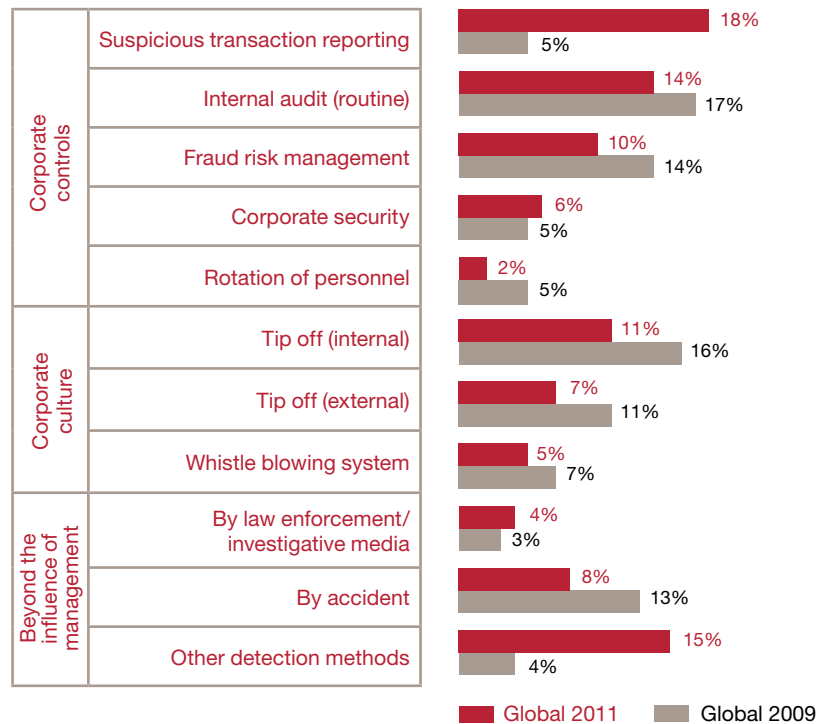
Our survey statistics show that 18% of the economic crimes reported by global respondents were detected by suspicious transaction reporting, an increase of 13% over 2009 (5%). Suspicious transaction reporting refers to the use of predictive data analytics to identify anomalies in financial data that could be caused by inappropriate activities.

In 2011, 23% of global organizations that were victims of economic crime over the past 12 months detected the fraud by a whistle-blowing system/

**Figure 9: Actions against internal perpetrator (Global 2011)**



**Figure 10: Detection methods**

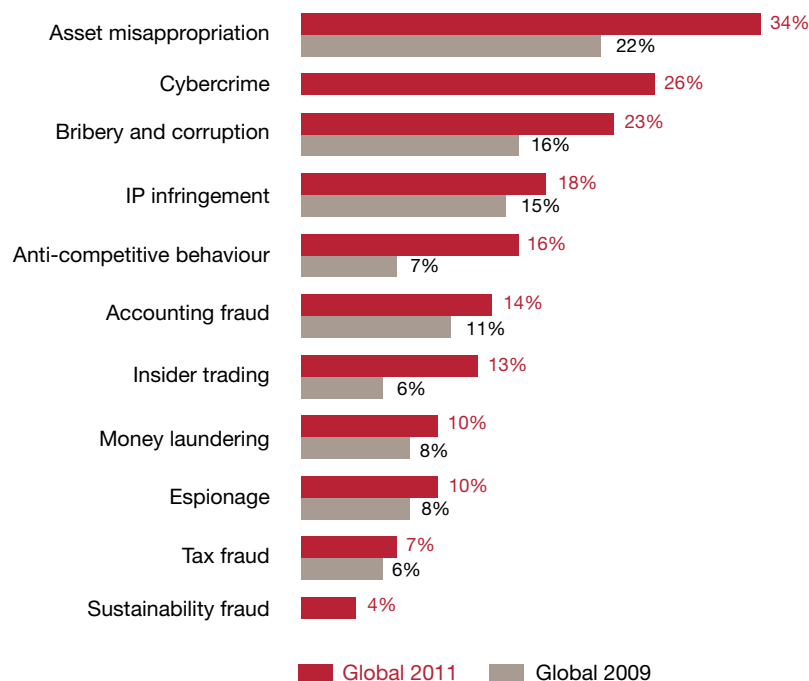


internal or external tip-off, which is a decrease of 11% from 34% in 2009. This result may suggest less economic crime, however it may also suggest people are unwilling to report their colleagues and customers, or that communication between business units is lacking and reports of irregularities are not acted upon. Organizations should ensure their employees are aware that such systems exist, provide a higher level of comfort in using the hotlines, and a greater understanding of their obligation to report economic crime—and the implications of not doing so. Organization leadership must also be seen as taking whistle-blowing seriously to ensure employees feel confident that reporting fraud through whistle-blowing mechanisms can be trusted, kept confidential and responded to appropriately.

In addition to suspicious transaction reporting and corporate culture, corporate control activities of the organizations surveyed (internal audit, fraud risk management, corporate security and rotation of personnel) accounted for 32% of the frauds detected.

The results of the 2011 survey show that the implementation of fraud risk management did not prove as effective as a method of detection as in 2009, with detection decreasing from 14% to 10% globally. The decrease in detection through fraud risk management may be caused, for example, by increased use of predictive data analytics. Organizations with a cross-organizational approach to fraud detection which encompasses a culture of ethics, strong controls and transparent communication will have a greater likelihood of detecting fraudulent behaviour—in other words, “seek and you shall find”.

**Figure 11: Perception of fraud † † †**



† Note: multiple types of economic crime were experienced by many of the respondents.

†† In our previous Economic Crime Surveys, when we asked respondents if they had experienced cybercrime, the response levels were very low and statistically insignificant. Hence, we combined the results with ‘other types of fraud’ in our past survey reports. Given the increasing concerns around cybercrime, we focussed on cybercrime this year and reintroduced it in the types of fraud question, asking respondents whether they had experienced cybercrime in the past 12 months. Sustainability fraud has been included for the first time as a fraud category in this year’s survey.

### **Organizations see more fraud ahead**

Figure 11 outlines the perceived threats of economic fraud reported in our 2009 and 2011 surveys. 34% of our global respondents believe their organization is susceptible to asset misappropriation within the next 12 months, an increase of 12% over our 2009 survey results. 26% of global respondents believe they are likely to be affected by cybercrime, which may indicate that organizations are becoming increasingly aware of the real threat of cybercrime to their organization.

Despite occurrences of fraudulent activity and the perception of increased fraud risk, 29% of global organizations stated that their respective organizations had not performed a fraud risk assessment, and 12% had no knowledge of whether one had been performed in the last 12 months. When asked the main reason their organization had not performed a fraud risk assessment in the last 12 months, global respondents stated:

- 36% indicated the perceived lack of value;
- 30% responded that they were not sure what a fraud risk assessment involved; and
- 20% did not know why a fraud risk assessment had not been performed.

When directors take an active interest in fraud within their organization, and take robust disciplinary action towards the perpetrators of fraud, the right “tone at the top” is established. The 2011 survey results demonstrate that an

organization’s ethical “tone at the top” and a strong internal control environment combine to provide the strongest deterrent to fraudulent behaviour, and increases the likelihood of detecting fraudulent activities. A corporate culture that clearly stresses the importance of integrity, where senior management is seen as “walking the talk”, and that has a well-communicated, comprehensive anti-fraud regime, is less likely to be victimized by economic crime.

### ***Implementing an effective anti-fraud regime***

When assessing and reviewing an organization’s anti-fraud regime, management should consider obtaining professional advice on effective compliance, prevention and detection programs. The organization needs to ensure that anti-fraud guidelines and practices remain current in the face of a changing economic climate, and that measures taken consider the laws and cultures of relevant operating jurisdictions within the global marketplace.

We believe that the key anti-fraud controls should include the following:

1. Governance—oversight by the audit committee and board of directors;
2. Fraud risk assessments;
3. Code of business conduct and ethics;
4. Incident reporting mechanisms;
5. Investigative protocol (including suspicious transaction reporting);
6. Remediation protocol;
7. Hiring and promotion policies and procedures; and
8. Management evaluation and testing.

*A corporate culture that clearly stresses the importance of integrity, where senior management is seen as “walking the talk”, and that has a well-communicated, comprehensive anti-fraud regime, is less likely to be victimized by economic crime.*



---

## *How PwC can help*

PwC can help deal with all types of economic crime and financial investigations with speed, sensitivity and discretion. Economic crime poses a real and substantial threat to the stability of any business. Dealing with fraud and financial impropriety requires more than simple know-how: it requires speed, sensitivity and discretion. We appreciate the need to minimize illegal activity while safeguarding your organization's assets and reputation, avoiding recurrences and arriving at a resolution with as little disruption as possible to the regular flow of business. Our services include:

- Fraud investigation;
- Forensic accounting;
- Fraud risk management;
- Cybercrime investigation and digital forensics;
- E-discovery;
- Data analytics;
- Background checking and corporate research;
- Money laundering investigations; and
- Asset recovery services.

PwC's international network of Forensic Services professionals possess a wide variety of expertise and academic backgrounds, including investigation, forensic accounting, digital forensics, information security, regulatory, legal and law enforcement. We have the technical skills, knowledge and hands-on experience necessary to investigate white collar crime and advise on managing and mitigating risk—including ways to identify and analyze vulnerabilities.

The firms of the PwC network provide industry-focused assurance, tax and advisory services to enhance value for clients. More than 161,000 people in 154 countries in PwC firms across the PwC network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

Our diverse background and skill-sets will benefit you in your investigations and forensic undertakings, regardless of how big or small the project.

For more information see [www.pwc.com/ca/forensics](http://www.pwc.com/ca/forensics)

# Who to call

## National Forensic Services Team



**Steven Henderson**

National Forensic  
Services Leader  
416 941 8328  
steven.p.henderson@  
ca.pwc.com



**Peter Vakof**

National Forensic  
Technology Services  
Leader  
416 814 5841  
peter.vakof@ca.pwc.com



**Kas Rehman**

National Public Sector  
Forensic Services Leader  
613 755 4328  
514 205 5171  
kas.rehman@ca.pwc.com



**Paul Bradley**

Associate Partner,  
Forensic Services  
902 491 7436  
paul.f.bradley@  
ca.pwc.com



**Jason Armstrong**

Director, Forensic  
Services  
613 755 8743  
jason.r.armstrong@  
ca.pwc.com



**Harm Atwal**

Director, Forensic  
Technology Services  
416 869 2330  
harm.k.atwal@  
ca.pwc.com



**Marie-Chantal Dréau**

Vice President,  
Forensic Services  
514 205 5407  
marie-chantal.dreau@  
ca.pwc.com



**Chris Gray**

Vice President,  
Forensic Services  
519 640 8011  
chris.gray@ca.pwc.com



**Ray Haywood**

GTA Forensic Services  
Leader  
416 814 5801  
h.ray.haywood@  
ca.pwc.com



**Dave Johnson**

Vice President,  
Forensic Services  
204 926 2423  
dave.a.johnson@  
ca.pwc.com



**Kyla Kramps**

Vice President,  
Forensic Services  
204 926 2434  
kyla.kramps@ca.pwc.com



**Sarah MacGregor**

Director, Forensic  
Services  
416 814 5763  
sarah.e.macgregor@  
ca.pwc.com



**Steven Malette**

Vice President,  
Forensic Services  
613 755 5979  
steven.m.malette@  
ca.pwc.com



**Krista Mooney**

Director, Forensic  
Services  
416 941 8290  
krista.a.mooney@  
ca.pwc.com



**James Pomeroy**

Vice President,  
Forensic Services  
902 491 7416  
james.a.pomeroy@  
ca.pwc.com



**Nikki Robar**

Vice President,  
Forensic Services  
902 491 7453  
nikki.l.robar@ca.pwc.com



**Lloyd Wilks**

Director, Forensic  
Technology Services  
416 687 8115  
lloyd.wilks@ca.pwc.com

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

© 2011 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.

